ITERATED SUMSETS AND SUBSEQUENCE SUMS

DAVID J. GRYNKIEWICZ

ABSTRACT. Let $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$ be a finite abelian group with $m_1 \mid \ldots \mid m_r = \exp(G)$. The Kemperman Structure Theorem characterizes all subsets $A, B \subseteq G$ satisfying $|A+B| < |A|+|B|$ and has been extended to cover the case when $|A+B| \le |A|+|B|$. Utilizing these results, we provide a precise structural description of all finite subsets $A \subseteq G$ with $|nA| \le (|A|+1)n-3$ when $n \ge 3$ (also when G is infinite), in which case many of the pathological possibilities from the case $n=2$ vanish, particularly for large $n \ge \exp(G)-1$. The structural description is combined with other arguments to generalize a subsequence sum result of Olson asserting that a sequence S of terms from G having length $|S| \ge 2|G|-1$ must either have every element of G representable as a sum of $|G|$-terms from S or else have all but $|G/H|-2$ of its terms lying in a common H-coset for some $H \le G$. We show that the much weaker hypothesis $|S| \ge |G|+\exp(G)$ suffices to obtain a nearly identical conclusion, where for the case H is trivial we must allow all but $|G/H|-1$ terms of S to be from the same H-coset. The bound on $|S|$ is improved for several classes of groups G, yielding optimal lower bounds for $|S|$. We also generalize Olson's result for $|G|$-term subsums to an analogous one for n-term subsums when $n \ge \exp(G)$, with the bound likewise improved for several special classes of groups. This improves previous generalizations of Olson's result, with the bounds for n optimal.

1. Notation and Overview

Let G be an abelian group and let $A, B \subseteq G$ be finite and nonempty subsets. Their sumset is defined as $A+B = \{a+b : \ a \in A, b \in B\}$. For $x \in G$, we let $\mathsf{r}_{A+B}(x) = |(x-B) \cap A| = |(x-A) \cap B)|$ denote the number of ways to represent $x = a+b$ as an element in the sumset $A+B$, where $(a,b) \in A \times B$. When $\mathsf{r}_{A+B}(x) = 1$, we say that x is a *unique expression* element in $A+B$. Note $A+B = \{x \in G : \ \mathsf{r}_{A+B}(x) \ge 1\}$. Multiple summand sumsets are defined analogously: $\sum_{i=1}^{n} A_i = \{\sum_{i=1}^{n} a_i : \ a_i \in A_i\}$ for subsets $A_1, \ldots, A_n \subseteq G$. For an integer $n \ge 0$, we use the abbreviation $nA = \underbrace{A+\ldots+A}_{n}$, where $0A := \{0\}$, for the n-fold iterated sumset.

The *stabilizer* of $A \subseteq G$ is the subgroup $\mathsf{H}(A) = \{x \in G : \ x+A = A\} \le G$. It is the maximal subgroup H such that A is a union of H-cosets. When $\mathsf{H}(A)$ is trivial, A is called *aperiodic*, and when $\mathsf{H}(A)$ is nontrivial, A is called *periodic*. More generally, if A is a union of H-cosets for some subgroup $H \le G$ (necessarily with $H \le \mathsf{H}(A)$), then A is called *H-periodic*.

2010 *Mathematics Subject Classification.* 11B75, 11P70.

Key words and phrases. zero-sum, sumset, subsequence sum, subsum, Partition Theorem, DeVos-Goddyn-Mohar Theorem, Kneser's Theorem, Kemperman Structure Theorem, n-fold sumset, iterated sumset, Olson, complete sequence.

If $H \le G$ is a subgroup, then we let $\phi_H : G \to G/H$ denote the natural homomorphism. Note, if $H = \mathsf{H}(A)$, then $\phi_H(A)$ is aperiodic. We use $H < G$ to indicate that H is proper, and

$$\langle A\rangle_* := \langle A - A\rangle = \langle -x + A\rangle \quad \text{for any } x \in A$$

denotes the subgroup generated affinely by A, which is the smallest subgroup H such that A is contained in an H-coset. The relative complement of A is defined as

$$\overline{A}^{\,H} := (H + A) \setminus A.$$

When the subgroup H is implicit, it will usually be dropped from the notation.

Regarding sequences and subsequence sums, we follow the standardized notation from Factorization Theory [4] [6] [11]. The key parts are summarized here. Let $G_0 \subseteq G$ be a subset. A *sequence* S of terms from G_0 is viewed formally as an element of the free abelian monoid with basis G_0, denoted $\mathcal{F}(G_0)$. Thus a sequence $S \in \mathcal{F}(G_0)$ is written as a finite multiplicative string of terms, using the bold dot operation $\boldsymbol{\cdot}$ to concatenate terms, and with the order irrelevant:

$$S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$$

with $g_i \in G_0$ the terms of S and $|S| := \ell \ge 0$ the *length* of S. Given $g \in G_0$ and $s \ge 0$, we let $g^{[s]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{s}$ denote the sequence consisting of the element g repeated s times. We let

$$\mathsf{v}_g(S) = |\{i \in [1, \ell] :\ g_i = g\}| \ge 0$$

denote the multiplicity of the term $g \in G_0$ in the sequence S. If S, $T \in \mathcal{F}(G_0)$ are sequences, then $S \boldsymbol{\cdot} T \in \mathcal{F}(G_0)$ is the sequence obtained by concatenating the terms of T after those of S. A sequence S may also be defined by listing its terms as a product: $S = \prod^{\bullet}_{g\in G_0} g^{[\mathsf{v}_g(S)]}$. We use $T \mid S$ to indicate that T is a subsequence of S and let $T^{[-1]} \boldsymbol{\cdot} S$ or $S \boldsymbol{\cdot} T^{[-1]}$ denote the sequence obtained by removing the terms of T from S. Then

$$\begin{aligned}
&\mathsf{h}(S) = \max\{\mathsf{v}_g(S) :\ g \in G_0\} \quad \text{is the } \textit{maximum multiplicity} \text{ of } S,\\
&\mathrm{Supp}(S) = \{g \in G_0 :\ \mathsf{v}_g(S) > 0\} \subseteq G \quad \text{is the } \textit{support} \text{ of } S,\\
&\sigma(S) = \sum_{i=1}^{\ell} g_i = \sum_{g\in G_0} \mathsf{v}_g(S)g \in G \quad \text{is the } \textit{sum} \text{ of } S,\\
&\Sigma_n(S) = \{\sigma(T) :\ T \mid S, |T| = n\} \subseteq G \quad \text{are the } n\text{-term } \textit{sub(sequence)-sums} \text{ of } S.
\end{aligned}$$

Given a map $\varphi\colon G_0 \to G_0'$, we let $\varphi(S) = \varphi(g_1) \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} \varphi(g_\ell) \in \mathcal{F}(G_0')$. The sequence S is called *zero-sum* if $\sigma(S) = 0$. A *setpartition* $\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n$ over G_0 is a sequence of *finite*, *nonempty* subsets $A_i \subseteq G_0$. A setpartition naturally partitions its underlying sequence

$$\mathsf{S}(\mathcal{A}) := \prod\nolimits^{\bullet}_{i\in[1,n]} \prod\nolimits^{\bullet}_{g\in A_i} g \in \mathcal{F}(G_0)$$

into n sets, so $\mathsf{S}(\mathcal{A})$ is the sequence obtained by concatenating the elements from every A_i. We let $\mathcal{S}(G_0)$ denote the set of all setpartitions over G_0, and refer to a setpartition of length $|\mathcal{A}| = n$ as an *n-setpartition.*

Intervals are discrete, so $[a, b] = \{x \in \mathbb{Z} : \ a \le x \le b\}$ for a, $b \in \mathbb{R}$, as are variables introduced with inequalities. For $m \ge 1$, we let $C_m \cong \mathbb{Z}/m\mathbb{Z}$ denote a cyclic group of order m. If G is finite, then $G \cong C_{m_1} \times \ldots \times C_{m_r}$ for some $m_1 \mid \ldots \mid m_r$ with $m_r = \exp(G)$ the *exponent* of G. For G cyclic, an affine transformation is a map $\varphi : G \to G$ of the form $\varphi(x) = sx + y$ for $x \in G$, where $y \in G$, $s \in \mathbb{Z}$ and $\gcd(s, |G|) = 1$. The *Davenport Constant*, denoted $\mathsf{D}(G)$, is the least integer such that a sequence of terms from G with length $|S| \ge \mathsf{D}(G)$ must always contain a nontrivial zero-sum subsequence. In general, $\mathsf{D}^*(G) \le \mathsf{D}(G) \le |G|$, where $\mathsf{D}^*(G) := 1 + \sum_{i=1}^{r} (m_i - 1)$, though both inequalities may fail (see [6, Propositions 5.1.4 and 5.1.8, pp. 341], or [19] for related results regarding the strong Davenport constant).

Inverse structure theorems for sumsets, describing the structure of the summands A and B when $|A + B|$ is small in comparison to the size of $|A|$ and $|B|$, are among the most fundamental questions in Additive Combinatorics. The texts [5] [6] [11] [17] [20] provide some overview. While there are many such results approximating the structure of A and B, particularly in special groups, there are very few that fully characterize the possibilities, especially for an unrestricted abelian group G. One such result is due to Kemperman [11, Chapter 9] [13] [14], who gave a full characterization of when $|A + B| < |A| + |B|$. This was later extended to a characterization of when $|A + B| \le |A| + |B|$ in [9], generalizing partial work achieved in [12]. They include some unwieldy possibilities, particularly when $|A + B|$ is large in comparison to $|G|$, leading us to defer the relevant details until Section 2. Our first goal in this paper is to extend the symmetric case in these results to n-fold iterated sumsets, giving the following precise characterization applicable when $|nA| < n|A + H| + (n - 3)|H|$, where $H = \mathsf{H}(nA)$, by applying it to $n\phi_H(A)$. The definitions used to describe the possible structures in Theorem 1.1 are explained in detail in Section 2.

Theorem 1.1. *Let G be a nontrivial abelian group, let $A \subseteq G$ be a finite subset with $\langle A \rangle_* = G$, and let $n \ge 3$ be an integer. Suppose nA is aperiodic and*

$$|nA| < (|A| + 1)n - 3.$$

If $|A| = 3$, then A is given by one of the possibilities listed in Lemma 3.1. Otherwise, one of the following must hold.

(i) *There is an arithmetic progression $P \subseteq G$ such that $A \subseteq P$ and $|P| \le |A| + 1$, in which case $|nA| = (|A| - 1)n + 1$, $|nA| = |A|n$, $|nA| = |A|n + 1$ or $|nA| = |A|n - 1 = |G| - 1$.*

(ii) *(A, A) is an elementary pair of type (VIII) with $|A| \ge 4$, in which case $|nA| = |A|n$ or $|nA| = |A|n - 1 = |G| - 1$.*

(iii) *There is an H-coset progression decomposition $A = A_0 \cup A_1 \cup \ldots \cup A_r$ with $H < G$ a finite, nontrivial, proper subgroup, $r \geq 1$ and $\sum_{i=1}^{r} |A_i| = r|H| - \epsilon$ with $\epsilon \in \{0, 1\}$. Moreover, nA_0 is an aperiodic subset with $|nA_0| < \min\{|K|, (|A_0| + 1 - \epsilon)n - 3\}$ or $|A_0| = 1$, where $K = \langle A_0 \rangle_* \leq H$, and one of the following also holds.*

- (a) *$nA = (nA \setminus nA_0) \cup nA_0$ is an H-quasi-periodic decomposition and $|nA| - |A|n = |nA_0| - |A_0|n + \epsilon n$.*
- (b) *$|H| = 2$, $|A_0| = |A_r| = 1$ and $r \geq 2$, in which case $|nA| = |A|n$ or $|nA| = |A|n - 1 = |G| - 1$.*
- (c) *$|A_0| = 1$ and $|A_1| = |H| - 1$, in which case $|nA| = |A|n$ or $|nA| = |A|n - 1 = |G| - 1$.*

When G is finite and n is large, many of the possibilities given in Theorem 1.1 are no longer possible. Requiring $|nA| < |A|n$ or knowing that $|A|$ is large can also further simplify the list of structures. We give two such corollaries (Corollaries 3.2 and 3.3) at the end of Section 3, though many more would be possible, varying according to the specific limitations imposed on n, A and G.

Our second goal is to utilize the structural characterization given in Theorem 1.1 to help improve some classical results regarding n-term subsequence sums and zero-sums. One inception for the study of subsequence sums is the Erdős-Ginzburg-Ziv Theorem [2] [5, Corollary 4.2.8] [6, Corollary 5.7.5] [11, Theorem 10.1].

Theorem A (Erdős-Ginzburg-Ziv Theorem)**.** *Let G be a finite abelian group and let $S \in \mathcal{F}(G)$ be a sequence of terms from G of length $|S| \geq 2|G| - 1$. Then $0 \in \Sigma_{|G|}(S)$.*

If one is interested in knowing whether an element $g \in G$ other than 0 can be represented as a subsum, there is a natural obstruction: S could consist of a single element repeated with high multiplicity or, more generally, most of the terms of S could lie in a coset of a proper subgroup. Olson [18], generalizing previous work of Mann [16], showed this to be the only barrier. We refer to the hypothesis in Theorem B that, for every $H < G$ and $\alpha \in G$, there are at least $|G/H| - 1$ terms of S lying outside the coset $\alpha + H$, as the *coset condition*.

Theorem B. [18] *Let G be a finite abelian group and let $S \in \mathcal{F}(G)$ be a sequence of terms from G of length $|S| \geq 2|G| - 1$. Suppose, for every $H < G$ and $\alpha \in G$, there are at least $|G/H| - 1$ terms of S lying outside the coset $\alpha + H$. Then $\Sigma_{|G|}(S) = G$.*

There are several natural approaches to generalizing the above result of Olson. First, one could ask whether the bound $|S| \geq 2|G| - 1$ is tight. Second, one could attempt to replace $\Sigma_{|G|}(S)$ with $\Sigma_n(S)$ for a more general integer $n \geq 1$. Third, one could ask whether the bound $|G/H| - 1$ is tight. Towards this end, there are results addressing the first two approaches.

For instance, Gao [3] showed that the hypothesis $|S| \geq 2|G| - 1$ in Theorem B could be replaced by $|S| \geq |G| + \mathsf{D}(G) - 1$, and the theorem remained true. A basic argument [11, Theorem 10.2] shows $\mathsf{D}(G) \leq |G|$, while $\mathsf{D}(G)$ is generally much smaller than $|G|$ (see [6, Theorem 5.5.5] [11,

Theorem 17.1]). Thus the result of Gao provided a strong generalization of Olson's result. However, the bound $|S| \ge |G| + \mathsf{D}(G) - 1$ is not optimal. It was later shown in [10] that the hypothesis $|S| \ge |G|+\mathsf{D}(G)-1$ could be replaced by $|S| \ge |G|+\mathsf{D}^*(G)-1$. Since $\mathsf{D}^*(G) \le \mathsf{D}(G)$ is the basic lower bound for the Davenport constant, known to be strictly tight in many instances (see [6, pp. 341]), this was an improvement on the bound given by Gao. It naturally raises the question, what is the minimal integer n_G such that $|S| \ge |G|+n_G$ implies $\Sigma_{|G|}(S) = G$, assuming the coset condition given in Theorem B holds? Note the coset condition failing for a coset of the subgroup $K < G$ implies that $|S| \le \mathsf{h}(S)|K| + |G/K| - 2$, which will be useful for showing that the coset condition holds in the following examples.

Example A.1. If $G = \langle g\rangle$ is cyclic of composite order with p the smallest prime divisor of $|G|$ and $H \le G$ the subgroup of order p, then the sequence $S = g^{[\frac{1}{p}|G|-1]} \cdot \prod_{h\in H}^{\bullet} h^{[\frac{1}{p}|G|]}$ has $|S| = |G| + \frac{1}{p}|G| - 1$, satisfies the coset condition, and yet $\Sigma_{|G|}(S) = \sigma(S) - \Sigma_{|G|/p-1}(S) \ne G$. This shows that we can do no better than $n_G \ge |G|/p$ when G is cyclic.

Example A.2. If G is non-cyclic, then $G = H \oplus \langle g\rangle \cong H \oplus C_{\exp(G)}$ for some nontrivial subgroup $H < G$. In this case, the sequence $S = g^{[\exp(G)-1]} \cdot \prod_{h\in H}^{\bullet} h^{[\exp(G)]}$ has $|S| = |G| + \exp(G) - 1$, satisfies the coset condition, and yet $\Sigma_{|G|}(S) = \sigma(S) - \Sigma_{\exp(G)-1}(S) \ne G$. Thus we can do no better than $n_G \ge \exp(G)$ when G is non-cyclic.

Example A.3. If G is neither cyclic nor isomorphic to C_2^2 and $G = H \oplus \langle g\rangle \cong H \oplus C_{\exp(G)}$ with $|H| \ge \exp(G)$, then the sequence $S' = \prod_{h\in H\setminus\{0\}\cup\{g\}}^{\bullet} h^{[\exp(G)+1]}$ has $|S'| = |G| + |H| \ge |G| + \exp(G)$ and $\Sigma_{\exp(G)}(S') \ne G$. Thus, any subsequence $S \mid S'$ with $|S| = |G| + \exp(G)$ will have $\Sigma_{|G|}(S) = \sigma(S) - \Sigma_{\exp(G)}(S) \subseteq \sigma(S) - \Sigma_{\exp(G)}(S') \ne G$. If we choose S such that $\mathsf{v}_h(S) \ge \exp(G)$ for all $h \in \mathrm{Supp}(S')$, then S will also satisfy the coset condition (since $G \ncong C_2^2$), showing we can do no better than $n_G \ge \exp(G) + 1$ when $|G| \ge \max\{5, \exp(G)^2\}$.

In all the above examples, we have made use of the general fact that $\Sigma_n(S) = \sigma(S)-\Sigma_{|S|-n}(S)$, which follows in view of the one-to-one correspondence between a subsequence $T \mid S$ of length $|T| = n$ and its complementary sequence $S \cdot T^{[-1]}$. If one is interested in studying the set of n-term subsums $\Sigma_n(S)$, then having a term with multiplicity greater than n is no better than having the same term with multiplicity equal to n. In other words, $\Sigma_n(S) = \Sigma_n(S')$, where $S' \mid S$ is the subsequence with $\mathsf{v}_x(S') = \min\{\mathsf{v}_x(S), n\}$ for all $x \in \mathrm{Supp}(S)$. In light of this basic observation, it generally makes little sense to consider $\Sigma_n(S)$ without the additional assumption limiting the maximal multiplicity to $\mathsf{h}(S) \le n$. To a lesser extent, this also means that when studying $|\Sigma_{|G|}(S)|$, terms with multiplicity greater than $|S| - |G|$ are also redundant. Note, the coset condition for S with the trivial subgroup is equivalent to $\mathsf{h}(S) \le |S| - |G| + 1$, so this is nearly achieved as part of the hypotheses of Theorem B. When $|S| \ge 2|G|-1$, there can only be one term $x \in \mathrm{Supp}(S)$ with $\mathsf{v}_x(S) = |S| - |G| + 1$, meaning at most one term in S is redundant, which proves to be negligible loss. However, the examples given above make use of much more non-negligible loss when $|S| = n + |G|$ with n much smaller than $|G| - 1$. If we disallow such

redundant terms by imposing the slightly stronger hypothesis $\mathsf h(S) \le |S| - |G|$, then we can obtain a result with optimal bounds for the size of $|S|$. The optimality of the bounds for n can be seen by Examples B.1–B.3.

Theorem 1.2. *Let G be a finite abelian group, let $n \ge 1$, and let $S \in \mathcal F(G)$ be a sequence of terms from G with $|S| = |G| + n$ and $\mathsf h(S) \le n$. Suppose, for every $H < G$ and $\alpha \in G$, there are at least $|G/H| - 1$ terms of S lying outside the coset $\alpha + H$. Then $\Sigma_{|G|}(S) = G$ whenever*

1. *$n \ge \exp(G)$, or*
2. *$n \ge \exp(G) - 1$ and $G \cong H \oplus C_{\exp(G)}$ with $|H|$ or $\exp(G)$ prime, or*
3. *$n \ge \frac{|G|}{p} - 1$ and G is cyclic, where p is the smallest prime divisor of $|G|$, or*
4. *$n \ge 1$ and either $\exp(G) \le 3$, or $|G| < 12$, or $\exp(G) = 4$ with $|G| = 16$.*

Example B.1. Suppose $G = \langle g\rangle$ is cyclic of composite order $|G| \ge 10$ with p the smallest prime divisor of $|G|$ and $H < G$ the subgroup of order p. Then the sequence $S' = \prod^\bullet_{x\in H\cup(g+H)} x^{[\frac 1p|G|-2]}$ has $|S'| = 2|G| - 4p \ge |G| + \frac 1p|G| - 3$ with the inequality strict for $|G| > 10$, $\mathsf h(S') \le \frac 1p|G| - 2$, and $\Sigma_{\frac 1p|G|-2}(S') \ne G$. If $S \mid S'$ is any subsequence with $|S| = |G| + \frac 1p|G| - 2$, then $\mathsf h(S) \le \frac 1p|G| - 2$ and $\Sigma_{|G|}(S) = \sigma(S) - \Sigma_{\frac 1p|G|-2}(S) \subseteq \sigma(S) - \Sigma_{\frac 1p|G|-2}(S') \ne G$. If we choose S so that $\mathsf v_h(S) = \frac 1p|G| - 2$ for all $h \in H \cup \{g\}$, then S (and also S') satisfies the coset condition. This shows the bound $n \ge \frac 1p|G| - 1$ is tight in Theorem 1.2.3 and in Theorem 1.3.3 below.

Example B.2. Suppose $G = H \oplus \langle g\rangle \cong H \oplus C_{\exp(G)}$ with H nontrivial and $\exp(G) \ge 5$. In this case, the sequence $S' = \prod^\bullet_{x\in H\cup(g+H)} x^{[\exp(G)-2]}$ has $|S'| = 2|G| - 4|H| \ge |G| + \exp(G) - 2$ and $\Sigma_{\exp(G)-2}(S') \ne G$. If $S \mid S'$ is any subsequence with $|S| = |G| + \exp(G) - 2$, then $\mathsf h(S) \le \exp(G) - 2$ and $\Sigma_{|G|}(S) = \sigma(S) - \Sigma_{\exp(G)-2}(S) \subseteq \sigma(S) - \Sigma_{\exp(G)-2}(S') \ne G$. If we choose S so that $\mathsf v_x(S) = \exp(G) - 2$ for all $x \in H \cup \{g\}$, then S (and also S') satisfies the coset condition. This shows the bound $n \ge \exp(G) - 1$ is tight in Theorem 1.2.2 and in Theorem 1.3.2 below.

Example B.3. Suppose $G = H \oplus \langle g\rangle \cong H \oplus C_{\exp(G)}$ with $|H|$ and $\exp(G)$ composite, which implies $|G| \ge 16$. Let $K < H$ be a subgroup of order $|K| = \frac 1p|H|$ where p is the smallest prime divisor of $|H|$. The sequence $S = \prod^\bullet_{x\in H\cup(g+K)} x^{[\exp(G)-1]}$ has $|S'| = \frac{(p+1)}{p}|H|(\exp(G) - 1) = |G| + \frac{m-p-1}{pm}|G|$, where $m = \exp(G)$, and $\Sigma_{\exp(G)-1}(S') \ne G$. Note $|G| = m|H| \ge mp^2$ since $|H|$ is composite, while $m = \exp(G) \ge 2p$ since $\exp(G)$ is composite. Thus, if $m - 2 \ge \frac{m-p-1}{pm}|G|$, then $m - 2 \ge (m - p - 1)p$, implying $p^2 - 3p + 2 \le 0$, in turn implying $p = 2$. Moreover, $\frac{m-p-1}{pm}|G| \ge m - 2$. When $p = 2$, we further obtain $m - 2 \ge (m - p - 1)p = 2m - 6$, implying $\exp(G) = m \le 4$, which is only possible if $m = \exp(G) = 4$ (since $\exp(G)$ is composite). Hence $m - 2 \ge \frac{m-p-1}{pm}|G|$ implies equality holds with $|G| \le 16$ and $\exp(G) = 4$. However, since $|H|$ is composite, this is only possible if $|G| = 16$. Therefore, we conclude that $|S'| \ge |G| + \exp(G) - 2$ and $|S'| \ge |G| + \exp(G) - 1$ when $|G| \ne 16$. In the latter case, letting $S \mid S'$ be a subsequence of length $|S| = |G| + \exp(G) - 1$, we find that $\mathsf h(S) \le \exp(G) - 1$

and $\Sigma_{|G|}(S) = \sigma(S) - \Sigma_{\exp(G)-1}(S) \subseteq \sigma(S) - \Sigma_{\exp(G)-1}(S') \neq G$. If we choose S so that $\mathsf{v}_x(S) = \exp(G) - 1$ for all $x \in H \cup \{g\}$, then S also satisfies the coset condition. This shows the bound $n \geq \exp(G)$ is tight in Theorem 1.2.1. Since S' also satisfies the coset condition with $|S'| \geq |G| + \exp(G) - 2$, the bound $n \geq \exp(G)$ is also tight in Theorem 1.3.1 below.

The second approach to generalizing Theorem 1.2 is to replace $\Sigma_{|G|}(S)$ with $\Sigma_n(S)$ under the hypothesis that $\mathsf{h}(S) \leq n$. In this direction, there are results related to an analog of Kneser's Theorem for subsequence sums obtained either via the DeVos-Goddyn-Mohar Theorem [1] [11, Theorem 13.1] or the Partition Theorem [11, Theorem 14.1]. Let us begin by stating the original theorem of Kneser for sumsets [5, Theorem 4.1.1] [6, Theorem 5.2.6] [11, Theorem 6.1] [15] [17, Theorem 4.1] [20, Theorem 5.5].

Theorem C (Kneser's Theorem)**.** *Let G be an abelian group and let $A_1, \ldots, A_n \subseteq G$ be finite, nonempty subsets. Then*

$$|\sum_{i=1}^{n} A_i| \geq \sum_{i=1}^{n} |A_i + H| - (n-1)|H| = \sum_{i=1}^{n} |A_i| - (n-1)|H| + \rho,$$

where $H = \mathsf{H}(\sum_{i=1}^{n} A_i)$ and $\rho := \sum_{i=1}^{n} |(A_i + H) \setminus A_i|$.

Note $\sum_{i=1}^{n} A_i = \sum_{i=1}^{n} (A_i + H)$, and ρ measures the number of "holes" in the sets A_i relative to the sets $A_i + H$. The version of Kneser's Theorem valid for n-term subsums is the following (see the discussion in [11, pp. 181–182]).

Theorem D (Subsum Kneser's Theorem)**.** *Let G be an abelian group, let $n \geq 1$, let $S \in \mathcal{F}(G)$ be a sequence with $\mathsf{h}(S) \leq n \leq |S|$, let $H = \mathsf{H}(\Sigma_n(S))$, let $X \subseteq G/H$ be the subset of all $x \in G/H$ for which x has multiplicity at least n in $\phi_H(S)$, and let e be the number of terms from S not contained in $\phi_H^{-1}(X)$. Then*

$$\begin{aligned} |\Sigma_n(S)| &\geq (|S| - n + 1) - (n - e - 1)(|H| - 1) + \rho, \\ &= |S| - (n-1)|H| + e(|H| - 1) + \rho, \end{aligned}$$

where $\rho = |X||H|n + e - |S| \geq 0$.

A short calculation shows that the bound given in Theorem D is equal to $((N-1)n+e+1)|H| = (\sum_{x \in G/H} \min\{n, \mathsf{v}_x(\phi_H(S))\} - n + 1)|H|$, where $N = |X|$, which is how the bound is stated in [11] and [1]. The form given above is perhaps easier to apply in practice and highlights the connection with the bound from Kneser's Theorem better. If we define S^* to be the sequence obtained from S (as given in Theorem D) by taking each term $x \in \phi_H^{-1}(X)$ and changing its multiplicity from $\mathsf{v}_x(S)$ to $\mathsf{v}_x(S^*) = n$, then $S \mid S^*$, $|S^*| = |S| + \rho$ and $\Sigma_n(S) = \Sigma_n(S^*)$ with ρ measuring the number of "holes" in the sequence S relative to S^*. The sequence S^* plays the

same role in Theorem D as the sets $A_i + H$ in the bound $|\sum_{i=1}^{n} A_i| \ge \sum_{i=1}^{n} |A_i + H| - (n-1)|H|$ obtained from Kneser's Theorem. As mentioned above, Theorem D can be obtained either from the DeVos-Goddyn-Mohar Theorem or the Partition Theorem. The Partition Theorem first appeared (in some form) in [7], with the variation allowing $S' \mid S$ appearing in [8]. The more general form given below, which subtlety refines and strengthens the Subsum Kneser's Theorem, may be found in [11, Theorem 14.1], slightly reworded here.

Theorem E (Partition Theorem)**.** *Let G be an abelian group, let $n \ge 1$, let $S \in \mathcal{F}(G)$ be a sequence, let $S' \mid S$ be a subsequence with $\mathsf{h}(S') \le n \le |S'|$, let $H = \mathsf{H}(\Sigma_n(S))$, let $X \subseteq G/H$ be the subset of all $x \in G/H$ for which x has multiplicity at least n in $\phi_H(S)$, and let e be the number of terms from S not contained in $\phi_H^{-1}(X)$. Then there exists a setpartition $\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n \in \mathcal{S}(G)$ with $\mathsf{S}(\mathcal{A}) \mid S$ and $|\mathsf{S}(\mathcal{A})| = |S'|$ such that either*

1. *$|\Sigma_n(S)| \ge |\sum_{i=1}^{n} A_i| \ge \sum_{i=1}^{n} |A_i| - n + 1 = |S'| - n + 1$, or*
2. *$|\Sigma_n(S)| = |\sum_{i=1}^{n} A_i| \ge \sum_{i=1}^{n} |A_i + H| - (n-1)|H| = |S'| - (n-1)|H| + e(|H| - 1) + \rho$, where $\rho = |X||H|n + e - |S'| \ge 0$, while $\mathrm{Supp}(\mathsf{S}(\mathcal{A})^{[-1]} \cdot S) \subseteq \phi_H^{-1}(X) \subseteq A_i + H$ and $|A_i \setminus \phi_H^{-1}(X)| \le 1$ for all $i \in [1, n]$.*

If $|\Sigma_n(S)| < |S| - n + 1$, then combining this bound with the lower bound from Theorem D implies that there are a small number of H-cosets, namely $N = |X| \ge 1$, containing most of the terms from S, namely all but e terms. For large n, say $n \ge \frac{1}{p}|G| - 1$ where p is the smallest prime divisor of $\exp(G)$, comparing these lower and upper bounds forces $N = 1$, leading to the coset condition holding for S, giving a version of Olson's Theorem valid for n-sums. However, it is actually possible to force the coset condition to hold for much smaller n. For instance, such a result was achieved for $n \ge \mathsf{D}^*(G) - 1$ in [10]. The Partition Theorem yields the bound given in Theorem D but also shows that there is an actual setpartition $\mathcal{A} = A_1 \cdot \ldots \cdot A_n$ with either $|\Sigma_n(S)| \ge |\sum_{i=1}^{n} A_i| \ge |S'| - n + 1$ or $\Sigma_n(S) = \sum_{i=1}^{n} A_i$. We will use this realization of $\Sigma_n(S)$ as a sumset together with the results from Section 3 to reduce even further the necessary lower bound for n, and thereby obtain a generalization of Olson's Theorem B from $|G|$-term to n-term subsums with optimal bounds for how large n must be. The optimality follows in view of Examples B.1–B.3.

Theorem 1.3. *Let G be a finite abelian group, let $n \ge 1$, and let $S \in \mathcal{F}(G)$ be a sequence of terms from G with $|S| \ge n + |G| - 1$ and $\mathsf{h}(S) \le n$. Suppose, for every $H < G$ and $\alpha \in G$, there are at least $|G/H| - 1$ terms of S lying outside the coset $\alpha + H$. Then $\Sigma_n(G) = G$ whenever*

1. *$n \ge \exp(G)$, or*
2. *$n \ge \exp(G) - 1$ and $G \cong H \oplus C_{\exp(G)}$ with $|H|$ or $\exp(G)$ prime, or*
3. *$n \ge \frac{1}{p}|G| - 1$ and G is cyclic, where p is the smallest prime divisor of $|G|$, or*
4. *$n \ge 1$ and either $\exp(G) \le 3$ or $|G| < 10$.*

2. Critical Pair Theory

We review the portions of Kemperman's Critical Pair Theory needed for the paper. We begin with the following simple consequence of the Pigeonhole Principle [11, Theorem 5.1]. Note, if A and B are each subsets of an H-coset with $|A|+|B| \geq |H|+1$, then Theorem F (applied to A and B translated so that they are subsets of the subgroup H) ensures that $A+B$ is an H-coset.

Theorem F (Pigeonhole Bound)**.** *Let G be an abelian group and let A, $B \subseteq G$ be finite subsets. If $|A|+|B| \geq |G|+r$ with $r \geq 1$ an integer, then $A+B = G$ with $\mathsf{r}_{A+B}(x) \geq r$ for every $x \in G$.*

Given a subgroup $H \leq G$, subset $A \subseteq G$ and $x \in A$, we call the subset $(x+H) \cap A \neq \emptyset$ an *H-coset slice* of A. The set A naturally decomposes into the disjoint union of it's H-coset slices, $A = A_1 \cup \ldots \cup A_d$ with each $A_i = (x_i + H) \cap A$ for some $x_i \in A$. We call such a decomposition the *H-coset decomposition* of A. Thus $\phi_H(A) = \{\phi_H(x_1), \ldots, \phi_H(x_d)\}$ with the elements $\phi_H(x_i)$ distinct. If $\phi_H(x_{i+1}) - \phi_H(x_i)$ is constant for $i = 1, \ldots, d-1$, so $\phi_H(A) = \{\phi_H(x_1), \ldots, \phi_H(x_d)\}$ is an arithmetic progression with the indices chosen to reflect the order of terms in the progression, then we say $A = A_1 \cup \ldots \cup A_d$ is an *H-coset progression decomposition* of A. If $A = (A \setminus A_\emptyset) \cup A_\emptyset$ with $A_\emptyset$ a nonempty subset of an H-coset and $A \setminus A_\emptyset$ H-periodic, then we call $A = (A \setminus A_\emptyset) \cup A_\emptyset$ an *H-quasi-periodic decomposition* of A. Note this means (after re-indexing the terms in its H-coset decomposition) that $A_i = x_i + H$ for $i \in [2, d]$ and $A_1 = A_\emptyset$.

Let X, $Y \subseteq G$ be finite and nonempty subsets with $H = \langle X+Y \rangle_*$. We say that the pair (X, Y) is *elementary of type* (I), (II), ..., (VII) or (VIII) if there are x, $y \in G$ such that $X = x + A$ and $Y = y + B$ for a pair of subsets A, $B \subseteq H$ satisfying the corresponding requirement below (with all complements relative to the subgroup H, so $\overline{A} = (H + A) \setminus A = H \setminus A$):

- (I) $|A| = 1$ or $|B| = 1$
- (II) A and B are arithmetic progressions of common difference $d \in H$ with $|A|$, $|B| \geq 2$ and $\mathrm{ord}(d) \geq |A| + |B| - 1 \geq 3$
- (III) $|A| + |B| = |H| + 1$ and there is precisely one unique expression element in the sumset $A + B$; in particular, $A + B = H$
- (IV) $B = -\overline{A}$ and the sumset $A+B$ is aperiodic and contains no unique expression elements; in particular, $A + B = A - \overline{A} = H \setminus \{0\}$
- (V) $|A| = 2$ or $|B| = 2$, and $|A + B| = |A| + |B|$
- (VI) $|A| = |B| = 3$, $A = B$ and $|A + B| = |A| + |B| = 6$
- (VII) either $|A| = 3$, $|2A| = 6$, $B = -\overline{2A}$ and $A = -\overline{A + B}$, or else $|B| = 3$, $|2B| = 6$, $A = -\overline{2B}$ and $B = -\overline{A + B}$; in particular, $|A + B| = |A| + |B| = |H| - 3$
- (VIII) there exist subgroups K_1, K_2, $K \leq H$, with $K_1 \cong K_2 \cong \mathbb{Z}/2\mathbb{Z}$ and $K = K_1 \oplus K_2$, and K-coset progression decompositions $A = A_1 \cup \ldots \cup A_r$ and $B = B_1 \cup \ldots \cup B_s$ such that $(\phi_K(A), \phi_K(B))$ is of type (II), A_1 and B_1 are each a K_1-coset, A_r and B_s are each a K_2-coset, and all other A_i and B_j, for $i \in [2, r-1]$ and $j \in [2, s-1]$, are full K-cosets; in particular, $|A + B| = |A| + |B|$.

As is easily observed, $|A+B| = |A|+|B|-1$ when (A,B) is an elementary pair of type (I), (II), (III) or (IV), and $|A+B| = |A|+|B|$ when (A,B) is an elementary pair of type (V), (VI), (VII) or (VIII). These elementary pairs are the basic building blocks of all sumsets $A+B$ with $|A+B| \le |A|+|B|$.

In view of Kneser's Theorem, the study of sumsets with $|A+B| \le |A|+|B|$ reduces to the aperiodic case. This structure is fully characterized in [9, Theorem 4.1, Corollary 4.2]. Combining this result with the "dual" formulation of the Kemperman Structure Theorem [11, Theorem 9.2], which characterizes the case when $|A+B| \le |A|+|B|-1$, we can now summarize the relevant structural information we will need.

Theorem G. *Let G be a nontrivial abelian group and let $A, B \subseteq G$ be finite and nonempty subsets with $\langle A+B\rangle_* = G$. Suppose $|A+B| \le |A|+|B|$ and $A+B$ is aperiodic. Then one of the following holds.*

(i) *(A,B) is an elementary pair of some type (I)–(II) or (IV)–(VIII).*

(ii) *$|A+B| = |A|+|B| \ge |G|-2$.*

(iii) *There are arithmetic progressions P_A, $P_B \subseteq G$ of common difference such that $A \subseteq P_A$, $B \subseteq P_B$, and $|P_A \setminus A|$, $|P_B \setminus B| \le 1$.*

(iv) *There exists a proper, finite and nontrivial subgroup $H < G$ and nonempty subsets $A_\emptyset = (\alpha+H)\cap A$ and $B_\emptyset = (\beta+H)\cap B$, for some α, $\beta \in G$, such that*

  (a) *$(\phi_H(A), \phi_H(B))$ is an elementary pair of some type (I)–(III),*

  (b) *$\phi_H(A_\emptyset)+\phi_H(B_\emptyset)$ is a unique expression element in $\phi_H(A)+\phi_H(B)$,*

  (c) *$|A\setminus A_\emptyset| \ge |H+(A\setminus A_\emptyset)|-1$ and $|B\setminus B_\emptyset| \ge |H+(B\setminus B_\emptyset)|-1$, with equality in either only possible when $|A+B| = |A|+|B|$,*

  (d) *$A_\emptyset + B_\emptyset$ is aperiodic and $-1 \le |A_\emptyset+B_\emptyset| - |A_\emptyset| - |B_\emptyset| \le |A+B|-|A|-|B|$, and*

  (e) *either $A+B = \Big((A+B)\setminus(A_\emptyset+B_\emptyset)\Big)\cup(A_\emptyset+B_\emptyset)$ is an H-quasi-periodic decomposition, or else $|A_\emptyset| = |B_\emptyset| = 1$, $\phi_H(A)$ and $\phi_H(B)$ are both arithmetic progressions of common difference with $\phi_H(A_\emptyset)$ and $\phi_H(B_\emptyset)$ the respective first terms, equality holds in both estimates from (c), say with $\{x\} = \overline{A\setminus A_\emptyset}^{\,H}$ and $\{y\} = \overline{B\setminus B_\emptyset}^{\,H}$, and either $\phi_H(x)$ and $\phi_H(y)$ are the respective second terms in $\phi_H(A)$ and $\phi_H(B)$, or $|H| = 2$ and $\phi_H(x)$ and $\phi_H(y)$ are the respective last terms.*

3. Iterated Sumsets

The goal of this section is to derive improved structural information when $\langle A\rangle_* = G$ and $|nA| < \min\{|G|, (|A|+1)n-3\}$ with $n \ge 3$. The behaviour of nA when $|A| \le 2$ is rather straightforward, since in this case A is an arithmetic progression. We begin with the first nontrivial case: $|A| = 3$.

Lemma 3.1. *Let G be an abelian group, let $A \subseteq G$ be a subset with $\langle A\rangle_* = G$ and $|A| = 3$, and let $n \geq 3$ be an integer. Suppose*

$$|nA| < \min\{|G|, (|A|+1)n - 3\} = \min\{|G|, 4n-3\}. \tag{1}$$

Then nA is aperiodic and one of the following holds.

(i) *There is an arithmetic progression $P \subseteq G$ such that $A \subseteq P$ and $3 \leq |P| \leq 4$, in which case $|nA| = 2n+1$, $|nA| = 3n$ or $|nA| = 3n-1 = |G|-1$.*

(ii) *There is an H-coset decomposition $A = A_1 \cup A_0$ with $\langle A_1\rangle_* = H \leq G$ a subgroup such that $2 \leq |H| \leq 3$, in which case $|nA| = 2n+1$, $|nA| = 3n$ or $|nA| = 3n-1 = |G|-1$.*

(iii) *There is an H-coset decomposition $A = A_1 \cup A_0$ with $\langle A_0\rangle_* = H \leq G$ a subgroup such that either $|H| = 4$ and $|nA| = 4n-5 = |G|-1$, or else $|H| = |G/H| = 5$ and $|nA| = 4n-4 = |G|-1 = 24$.*

(iv) *$G \cong C_2 \oplus C_{\exp(G)}$ with $4 \mid \exp(G)$ and there is an H-coset decomposition $A = \{x,z\} \cup \{y\}$ with $\langle x-z\rangle = H$ such that $|G/H| = 2$, $2(y+z) = 4x$ and $|nA| = 4n-5 = |G|-1$.*

(v) *There is an arithmetic progression $P \subseteq G$ with $A \subseteq P$ such that either $|P| = 5$ and $|nA| = 4n-5 = |G|-1$ or $|nA| = 4n-4 = |G|-1$, or else $|P| = 6$, $|G| = 21$ and $|nA| = 4n-4 = |G|-1 = 20$.*

(vi) *G is cyclic, $8 \nmid |G|$, $|nA| = 4n-5 = |G|-1$ and $A = \{0, 1, \frac{m}{2} - 1\}$ up to affine transformation.*

Proof. Suppose nA is periodic, say with $H = \mathsf{H}(nA)$ nontrivial. Since $|nA| < |G|$, H must be a proper subgroup. Thus, since $\langle A\rangle_* = G$, we have $2 \leq |\phi_H(A)| \leq 3$. Kneser's Theorem ensures that $|nA| \geq (n|\phi_H(A)| - n + 1)|H|$. Thus, if $|\phi_H(A)| = 3$, then the bound becomes $|nA| \geq (2n+1)|H| \geq 4n+2$, contrary to hypothesis. Therefore $|\phi_H(A)| = 2$, implying we have an H-quasi-periodic decomposition $A = A_1 \cup A_0$ with $|A_0| = 1$. Thus, since $\phi_H(A)$ is an arithmetic progression of size 2 and $\langle \phi_H(A)\rangle_* = G/H$, the only way nA can be H-periodic is if $n \geq |G/H| - 1$, in which case $|nA| \geq (n|\phi_H(A)| - n + 1)|H| = (n+1)|H| \geq |G|$, contradicting that $H < G$ is proper. So we instead conclude that nA is aperiodic.

We may assume by contradiction that neither (i) nor (ii) hold for A. Consequently, Theorem G and $|nA| < |G|$ ensure that $|kA| \geq |(k-1)A| + |A| = |(k-1)A| + 3$ for $k \in [2,n]$ unless $((k-1)A, A)$ is elementary of type (IV), in which case $|kA| = |(k-1)A| + |A| - 1 = |(k-1)A| + 2 = |G| - 1$. As a result, Theorem F and $|nA| < |G|$ ensure this is only possible for $k = n \geq 3$. In particular, $|2A| = 2|A| = 6$ (since $|2A| \leq \frac{1}{2}|A|(|A|+1)$ is a trivial upper bound).

Given the structural restrictions for A established above, we can now conclude from Theorem G that $|kA| \geq |(k-1)A| + |A| + 1 = |(k-1)A| + 4$ for $k \in [2,n]$ except when $((k-1)A, A)$ is elementary of type (IV), (VI) or (VII), or when $|(k-1)A + A| = |(k-1)A| + |A| \geq |G| - 2$. The second is only possible for $k = 2$. In view of Theorem F and $|nA| < |G|$, the first and fourth possibility can only occur for $k = n$, while the third is only possible for $k \in [n-1, n]$ and implies $|kA| = |G| - 3$.

For $k \ge 2$, let ϵ_k be the integer such that $|kA| = |(k-1)A| + 4 + \epsilon_k$. Thus

$$|nA| = 4n - 1 + \sum_{i=2}^{n} \epsilon_i. \tag{2}$$

In view of the above work, we have

$$\epsilon_2 = -1, \quad \epsilon_k \ge 0 \text{ for all } k \in [3, n-2], \quad \epsilon_{n-1} \ge -1, \qquad \text{and} \qquad \epsilon_n \ge -2. \tag{3}$$

Moreover, $\epsilon_n = -2$ is only possible if $|nA| = |G| - 1$; and $\epsilon_{n-1} = -1$ with $n - 1 > 2$ is only possible if $|(n-1)A| = |G| - 3$, in which case $|nA| = |G| - 1$ with $\epsilon_n = -2$ necessarily following in view of $|nA| < |G|$. It is now clear that the hypothesis $|nA| < 4n - 3$ is only possible if $|G|$ is finite with $\epsilon_n = -2$ and $|nA| = |G| - 1$, which we now assume. Moreover, we must either have $|nA| = 4n - 4 = |G| - 1$ or $n|A| = 4n - 5 = |G| - 1$, ensuring that

$$|G| \equiv 0 \text{ or } 1 \mod 4.$$

Suppose there is an H-coset decomposition $A = A_1 \cup A_0$. Then w.l.o.g $|A_1| = 2$ and $|A_0| = 1$. Moreover, $A = A_1 \cup A_0$ is also a $\langle A_1 \rangle_*$-coset decomposition, so we may w.l.o.g. assume $H = \langle A_1 \rangle_*$. Since (ii) is assumed not to hold, we must have $|H| \ge 4$. Suppose $|H| = 4$. If $|G/H| = 2$, then $|G| = 2|H| = 8$ and $|2A| = 6 = |G| - 2$, in which case $|3A| = |G|$ in view of Theorem F, contrary to hypothesis. Therefore we may assume $|G/H| \ge 3$. But now it is clear that $|kA| = |(k-1)A| + 4$ when $3 \le k \le \frac{1}{4}|G| - 1$, that $|kA| = |(k-1)A| + 3 = |G| - 3$ for $k = \frac{1}{4}|G|$, and that $|kA| = |(k-1)A| + 2 = |G| - 1$ for $k = \frac{1}{4}|G| + 1$, and thus (iii) follows. So we may assume $|H| \ge 5$. If we also have $|G/H| \ge 5$, then $\epsilon_2 = -1$, $\epsilon_3 = 0$ and $\epsilon_4 = 1$. Moreover, $\epsilon_5 \ge 1$ unless $|G/H| = |H| = 5$. However, if $|G/H| = |H| = 5$, then we instead have $|G| = |G/H||H| = 25$, $\epsilon_5 = 0$, $\epsilon_6 = -1$, and $\epsilon_7 = -2$ with $|7A| = |G| - 1$. In this case, (iii) follows in view of (2). On the other hand, if we instead have $\epsilon_5 \ge 1$, then (2) and (3) ensure that $|nA| \ge 4n - 3$, contrary to hypothesis. So we now conclude that if there is an H-coset decomposition $A = A_1 \cup A_0$, then $|H| \ge 5$ and $|G/H| \le 4$. In particular, considering $H = \langle a - b \rangle$ with $a, b \in A$ gives (note $\langle a - b \rangle = \langle A \rangle_* = G$ if $c \in \langle a - b \rangle_* + b$)

$$\text{ord}(a - b) \ge \max\{5, |G|/4\} \quad \text{for all distinct } a, b \in A. \tag{4}$$

Suppose there is an H-coset decomposition $A = \{x, z\} \cup \{y\}$ with $\langle x - z \rangle = H \le G$ a subgroup such that $|G/H| = 2$ and $2(y + z) = 4x$. By translating by $-z$, we can w.l.o.g. assume $A = \{x, 0\} \cup \{y\}$ with $2y = 4x$. Since $|G/H| = 2$, we must have $|G|$ even, whence $|nA| = 4n - 5 = |G| - 1$ as noted above, ensuring that $|G|$ is divisible by 4. If G were cyclic, then $2y = 4x$ combined with $|G| \equiv 0 \mod 4$ and $|G/H| = 2$ ensures that $y \in \langle x \rangle = H$, in which case $\langle A \rangle_* = \langle 0, y, x \rangle = \langle x \rangle = H < G$, contradicting the hypothesis $\langle A \rangle_* = G$. Therefore, since $\langle x \rangle = H$ is an index 2 subgroup, we must have $G \cong C_2 \times C_{\exp(G)}$. It remains to show $4 \mid \exp(G)$, which in view of $4(n-1) = |G| = 2\exp(G)$ is equivalent to n being odd, and then (iv) will

follow. To see this, we have only to note that

$$kA = \{0, x, \dots, (2k-1)x\} \cup y + \{0, x, \dots, (2k-4)x, (2k-2)x\} \qquad \text{for } k \geq 3 \text{ odd and}$$
$$kA = \{0, x, \dots, (2k-2)x, (2k)x\} \cup y + \{0, x, \dots, (2k-3)x\} \qquad \text{for } k \geq 2 \text{ even.}$$

Consequently, since $|nA| = |G| - 1$, we must either have n odd with $2n - 2 = |H| = \frac{1}{2}|G|$ (note $|H| = \frac{1}{2}|G|$ is even since 4 divides $|G|$) or else n is even with $2n = |H| = \frac{1}{2}|G|$. Since $|nA| = 4n - 5 = |G| - 1$, only the former is possible, and (iv) follows. So we can now assume no such H-coset decomposition exists.

By translating A appropriately, we can w.l.o.g. assume $0 \in A$, in which case $\langle A \rangle = \langle A \rangle_* = G$ ensures that G is generated by the two non-zero elements of $A = \{0, a, b\}$. Thus G has rank at most 2. Let us next dispense with the case when G is non-cyclic, say $G \cong \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with $m' \mid m$ and $m' \geq 2$. Suppose both nonzero elements $a, b \in A$ have order less than $\exp(G) = m$. Then $\mathrm{ord}(a), \mathrm{ord}(b) \leq \frac{|G|}{2m'}$, and we conclude that $m' = 2$ and $\mathrm{ord}(a) = \mathrm{ord}(b) = |G|/4 = m/2$ in view of (4). However, since any element of order $m/2$ in $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ must have an even second coordinate, this contradicts that $\langle a, b \rangle = \langle A \rangle = G$. So we can instead assume some element in A has order equal to $\exp(G) = m$. Any element $g \in G$ with $\mathrm{ord}(g) = \exp(G)$ generates a subgroup which is a direct summand in G. Thus we can w.l.o.g. assume $A = \{(0,0), (0,1), (1,x)\}$ with $0 \leq x \leq \frac{1}{2}m$. In view of (4) applied with $a = (0,1)$ and $b = (0,0)$, we conclude that $m = \exp(G) \geq 5$ and $m' \leq 4$. Thus $m \geq 6$ (since $m' \mid m$ with $m' \in [2,4]$ and $m \geq 5$), and since $|G| \equiv 0$ or 1 modulo 4, we conclude that either m is even, or else $m \equiv -1 \mod 4$ with $m' = 3$. In view of (4) applied with $a = (1,x)$ and $b = (0,0)$, we conclude that $\mathrm{ord}((1,x)) = m$ or $\frac{m}{2}$, with $\mathrm{ord}((1,x)) = \frac{m}{2}$ only possible if $m' = 2$. Likewise applying (4) with $a = (1,x)$ and $b = (0,1)$, we conclude that $\mathrm{ord}((1,x-1)) = m$ or $\frac{m}{2}$, with the latter only possible when $m' = 2$.

Now $A \subseteq 2A \subseteq 3A \subseteq 4A$ with

$$4A = \{(0,0), (0,1), (0,2), (0,3), (0,4)\} \cup \{(1,x), (1,x+1), (1,x+2), (1,x+3)\} \cup$$
$$\{(2,2x), (2,2x+1), (2,2x+2)\} \cup \{(3,3x), (3,3x+1)\} \cup \{(4,4x)\}.$$

Thus $|4A| \leq 15$, and in view of $m \geq 6$, it follows that the five groupings of elements above each consist of distinct elements. Consequently, if $|3A| < 15$, then we must have $2x \equiv -2, -1, 0, 1, 2, 3$ or $4 \mod m$ with $m' = 2$, or $3x \equiv -1, 0, 1, 2, 3$ or $4 \mod m$ with $m' = 3$, or $4x \equiv 0, 1, 2, 3$ or $4 \mod m$ with $m' = 4$ or 2. Since $m' \mid m$ and $0 \leq x \leq \frac{m}{2}$, it follows that either $x = 0, 1, 2, \frac{m}{2}, \frac{m}{2} - 1, \frac{m}{4}, \frac{m}{4} + 1$ or $\frac{m+2}{4}$ with $m' = 2$, or $x = 0, 1, \frac{m}{3}, \frac{m}{3} + 1$ with $m' = 3$, or $x = 0, \frac{m}{4}, \frac{m}{2}, 1$ or $\frac{m}{4} + 1$ with $m' = 4$. When $m' = 4$, $x = 0, \frac{m}{4}$ or $\frac{m}{2}$ implies $\mathrm{ord}((1,x)) \leq 4 < m$, while $x = 1$ or $\frac{m}{4} + 1$ implies $\mathrm{ord}((1,x-1)) \leq 4 < m$, both contradictions to what was shown above. When $m' = 3$, $x = 0$ or $\frac{m}{3}$ implies $\mathrm{ord}((1,x)) = 3 < m$, while $x = 1$ or $\frac{m}{3} + 1$ implies $\mathrm{ord}((1,x-1)) = 3 < m$, both contradictions to what was shown above. When $m' = 2$, $x = 0$ or $\frac{m}{2}$ implies $\mathrm{ord}((1,x)) = 2 < 3 \leq \frac{m}{2}$; $x = 1$ implies $\mathrm{ord}((1,x-1)) = 2 < 3 \leq \frac{m}{2}$; $x = \frac{m}{4}$

implies either $x = 2$ or else $m \ge 12$ and $\mathrm{ord}((1, x)) = 4 < 6 \le \frac{m}{2}$; and $x = \frac{m}{4} + 1$ implies either $x = \frac{m}{2} - 1$ or else $m \ge 12$ and $\mathrm{ord}((1, x-1)) = 4 < 6 \le \frac{m}{2}$. Thus we obtain contradictions in all cases except for $m' = 2$ with $x = 2, \frac{m}{2} - 1$ or $\frac{m+2}{4}$. If $x = \frac{m+2}{4}$, then we find that

$$kA = \{(0,0),(0,1),\dots,(0,k)\} \cup \{(0,\frac{m}{2}+1),\dots,(0,\frac{m}{2}+k-1)\} \cup$$
$$\{(1,\frac{m+2}{4}),\dots,(1,\frac{m+2}{4}+k-1)\} \cup \{(1,\frac{3m+6}{4}),\dots,(1,\frac{3m+6}{4}+k-3)\}$$

for $k \ge 3$. Thus $|kA| = 4k-2$ for $k \in [3, \frac{m}{2}]$, while $kA = G$ for $k = \frac{m}{2}+1$, contrary to (1). If $x = 2$, then $2(1,x) = (0,4) = 4(0,1)$. Likewise, if $x = \frac{m}{2}-1$, then translating all terms by $(0,-1)$ yields $A = \{(0,0),(0,-1),(1,\frac{m}{2}-2)\}$ with $2(1,\frac{m}{2}-2) = (0,-4) = 4(0,-1)$. Thus A has an H-coset decomposition satisfying the requirements of (iv), yielding the full conclusion contained in (iv) as shown earlier. So we can now assume $|4A| = 15$, and thus also that $|2A| = 6$ and $|3A| = 10$, since $2A \subseteq 3A \subseteq 4A$ with $4A$ only able to achieve its maximal value 15 if $|2A|$ and $|3A|$ also achieve their maximal values. It follows that $\epsilon_2 = -1$, $\epsilon_3 = 0$ and $\epsilon_4 = 1$. In consequence, in view of (2) and (3), we find that we must have $n \ge 6$ with $|nA| = 4n-4 = |G|-1$, forcing $m' = 3$. Moreover, we must have $n_5 \le 0$, as otherwise (2) and (3) ensure that $|nA| \ge 4n-3$, contrary to hypothesis.

Since $n_5 \le 0$ with $|4A| = 15$, we conclude that $|5A| \le 19$. Now

$$5A = \{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5)\} \cup \{(1,x),(1,x+1),(1,x+2),(1,x+3),(1,x+4)\}$$
$$\cup \{(2,2x),(2,2x+1),(2,2x+2),(2,2x+3)\}$$
$$\cup \{(3,3x),(3,3x+1),(3,3x+2)\} \cup \{(4,4x),(4,4x+1)\} \cup \{(5,5x)\}.$$

If all the elements listed above are distinct, then $|5A| = 21$, contrary to what we concluded above. Thus, in view of $m = \exp(G) \ge 6$ and $m' = 3$, we must have $3x \equiv -2,-1,0,1,2,3,4$ or $5 \mod m$. Since $3 = m' \mid m$, this is only possible if $3x \equiv 0$ or $3 \mod m$, both of which would contradict that $|4A| = 15$. This completes the case when G is non-cyclic. So we now assume w.l.o.g. that $G = \mathbb{Z}/m\mathbb{Z}$ with $m = |G| \equiv 0$ or $1 \mod 4$ and $6 = |2A| \le |G| - 3 = m - 3$ (the upper bound follows else Theorem F implies that $3A = G$), ensuring that $m \ge 9$.

Suppose next that there is some generating element for G contained in $A - A$. Then, by applying an appropriate affine transformation, we can w.l.o.g. assume $A = \{0, 1, y\}$ with $2 \le y \le \frac{m}{2}$ (if $y = \frac{m+1}{2}$, then m is odd and the affine transformation $x \mapsto 2x$ yields $A = \{0,1,2\}$; otherwise, apply the affine transformation $x \mapsto -x+1$ when $y \ge \frac{m}{2}+1$). Moreover, since we have assumed (i) does not hold, we must have $4 \le y \le \frac{m}{2}$. Now $A \subseteq 2A \subseteq 3A \subseteq 4A$ with

$$4A = [0,4] \cup (y + [0,3]) \cup (2y + [0,2]) \cup (3y + [0,1]) \cup \{4y\}.$$

Thus $|4A| \le 15$, and in view of $m \ge 9$, it follows that the five groupings of elements above each consist of distinct elements. Consequently, if $|4A| < 15$, then we must have $y \equiv t \mod m$ for some $t \in [-3,4]$, or $2y \equiv t \mod m$ for some $t \in [-2,4]$, or $3y \equiv t \mod m$ for some $t \in [-1,4]$, or $4y \equiv t \mod m$ for some $t \in [0,4]$. Hence, since $m \equiv 0$ or $1 \mod 4$ with $4 \le y \le \frac{m}{2}$ and $m \ge 9$,

we conclude that $y \in \{4, \frac{m}{2}-1, \frac{m-1}{2}, \frac{m}{2}, \frac{m-1}{3}, \frac{m}{3}, \frac{m+1}{3}, \frac{m+2}{3}, \frac{m}{3}+1, \frac{m+4}{3}, \frac{m}{4}, \frac{m+3}{4}, \frac{m}{4}+1\}$. If $y = 4$, then $P = \{0, 1, 2, 3, 4\}$ show that (v) holds; if $y = \frac{m-1}{2}$, then (i) holds with $P = \{\frac{m-1}{2}, 0, \frac{m+1}{2}, 1\}$; if $y = \frac{m}{2}$, then $A = \{0, \frac{m}{2}\} \cup \{1\}$ is an H-coset decomposition satisfying (ii); if $y = \frac{m-1}{3}$, then $P = \{\frac{m-1}{3}, 0, \frac{2m+1}{3}, \frac{m+2}{3}, 1\}$ shows that (v) holds; if $y = \frac{m}{3}$, then $A = \{0, \frac{m}{3}\} \cup \{1\}$ is an H-coset decomposition satisfying (ii); if $y = \frac{m+1}{3}$, then $P = \{0, \frac{m+1}{3}, \frac{2m+2}{3}, 1\}$ shows that (i) holds; if $y = \frac{m+2}{3}$, then $P = \{1, \frac{m+2}{3}, \frac{2m+1}{3}, 0\}$ shows that (i) holds; if $y = \frac{m}{3}+1$, then $A = \{1, \frac{m}{3}+1\} \cup \{0\}$ is an H-coset decomposition satisfying (ii); if $y = \frac{m+4}{3}$, then $P = \{0, \frac{m+1}{3}, \frac{2m+2}{3}, 1, \frac{m+4}{3}\}$ shows that (v) holds; if $y = \frac{m}{4}$, then $A = \{0, \frac{m}{4}\} \cup \{1\}$ is an H-coset decomposition satisfying (iii); if $y = \frac{m+3}{4}$, then $P = \{1, \frac{m+3}{4}, \frac{m+1}{2}, \frac{3m+1}{4}, 0\}$ shows that (v) holds; and if $y = \frac{m}{4} + 1$, then $A = \{1, \frac{m}{4} + 1\} \cup \{0\}$ is an H-coset decomposition satisfying (iii). Thus, in all cases except $y = \frac{m}{2} - 1$, one of our desired conclusions follows. However, if $y = \frac{m}{2} - 1$, then $m = |G|$ is even and $|nA| = 4n - 5 = |G| - 1 = m - 1$, whence $n = \frac{m}{4} + 1$. In this case,

$$kA = \{-k\} \cup [-k+2, k] \cup [\frac{m}{2} - k + 1, \frac{m}{2} + k - 2] \mod m \qquad \text{for } k \geq 2 \text{ even, and}$$

$$kA = [-k+1, k] \cup \{\frac{m}{2} - k\} \cup [\frac{m}{2} - k + 2, \frac{m}{2} + k - 2] \mod m \qquad \text{for } k \geq 3 \text{ odd.}$$

Consequently, $nA = G$ if $n = \frac{m}{4} + 1$ is odd, contrary to hypothesis, while if $n = \frac{m}{4} + 1$ is even, then $8 \nmid m = |G|$ and (vi) follows. So we can instead assume $|4A| = 15$, and thus also $|2A| = 6$ and $|3A| = 10$. It follows that $\epsilon_2 = -1$, $\epsilon_3 = 0$ and $\epsilon_4 = 1$. In consequence, in view of (2) and (3), we find that we must have $n \geq 6$ with $|nA| = 4n - 4 = |G| - 1 = m - 1$, forcing $m \equiv 1 \mod 4$ and $m = |G| \geq 21$. Moreover, we must have $n_5 \leq 0$, as otherwise (2) and (3) ensure that $|nA| \geq 4n - 3$, contrary to hypothesis.

Since $n_5 \leq 0$ with $|4A| = 15$, we conclude that $|5A| \leq 19$. Now

$$5A = [0, 5] \cup (y + [0, 4]) \cup (2y + [0, 3]) \cup (3y + [0, 2]) \cup \{4y + [0, 1]\} \cup \{5y\}.$$

If all the elements listed above are distinct apart from possibly $5y$, then $|5A| \geq 20$, contrary to what we concluded above. Thus, in view of $m \geq 21$, we must have $y \equiv t \mod m$ for some $t \in [-4, 5]$, or $2y \equiv t \mod m$ for some $t \in [-3, 5]$, or $3y \equiv t \mod m$ for some $t \in [-2, 5]$, or $4y \equiv t \mod m$ for some $t \in [-1, 5]$. However, since $|4A| = 15$, we can eliminate all the possibilities for t considered in the previous paragraph, leaving only the following: $y \equiv t \mod m$ for some $t \in \{-4\} \cup \{5\}$, or $2y \equiv t \mod m$ for some $t \in \{-3\} \cup \{5\}$, or $3y \equiv t \mod m$ for some $t \in \{-2\} \cup \{5\}$, or $4y \equiv t \mod m$ for some $t \in \{-1\} \cup \{5\}$. Consequently, since $m \equiv 1 \mod 4$ with $4 \leq y \leq \frac{m}{2}$ and $m \geq 21$, we conclude that $y \in \{5, \frac{m-3}{2}, \frac{m-2}{3}, \frac{m+5}{3}, \frac{m-1}{4}\}$. If $y = 5$, then $5A = [0, 13] \cup [15, 17] \cup [20, 21] \cup \{25\}$, in which case $|5A| = 20$, contrary to assumption, unless $m \leq 25$ with $m \equiv 1 \mod 4$. If, in addition, $m = 25$, then (iii) holds, while if in addition $m = 21$, then (v) holds. If $y = \frac{m-3}{2}$, then applying the affine transformation $z \mapsto 2z + 3$, we can assume $A = \{0, 3, 5\}$, in which case $5A = \{0, 3, 5, 6\} \cup [8, 20] \cup \{21, 23, 25\}$. Thus $|5A| = 20$, contrary to assumption, unless $m \leq 25$ with $m \equiv 1 \mod 4$. If, in addition, $m = 25$, then (iii) holds, while if in addition $m = 21$, then (v) holds. If $y = \frac{m-2}{3}$, then applying the affine

transformation $z \mapsto -3z+3$, we can assume $A = \{0, 3, 5\}$, and the argument is identical to the previous case when $y = \frac{m-3}{2}$. If $y = \frac{m+5}{3}$, then applying the affine transformation $z \mapsto 3z$, we can assume $A = \{0, 3, 5\}$, and the argument is identical to the previous case once more. Finally, if $y = \frac{m-1}{4}$, then applying the affine transformation $z \mapsto 4z+1$, we can assume $A = \{0, 1, 5\}$, in which the case the argument is identical to the case when $y = 5$. So we can now assume that $A - A$ contains no generating element for $G = \mathbb{Z}/m\mathbb{Z}$.

Let $A = \{0, x, y\}$ with x, $y \in [1, m-1]$. Since $A-A$ contains no generating element, it follows that $\gcd(x, m) \ge 2$, $\gcd(y, m) \ge 2$, $\gcd(x-y, m) \ge 2$. Since $\langle A\rangle = G$, we have $\gcd(x, y, m) = 1$. Since every H-coset decomposition $A = A_1 \cup A_0$ has $|H| \ge 5$ and $|G/H| \le 4$, we must have $\gcd(x, m) \le 4$, $\gcd(y, m) \le 4$ and $\gcd(x-y, m) \le 4$. Thus $\gcd(x, m)$, $\gcd(y, m)$, $\gcd(x-y, m) \in [2, 4]$. If both $\gcd(x, m) \in [2, 4]$ and $\gcd(y, m) \in [2, 4]$ are even or are both equal to 3, then this contradicts that $\gcd(x, y, m) = 1$. Thus $6 \mid m$ and we may w.l.o.g. assume $\gcd(y, m) = 3$ and $\gcd(x, m) \in \{2, 4\}$. Let $x = 2^s r$ with r odd, $s \ge 1$ and $\gcd(r, m) = 1$, and let $y = 3t$ with $\gcd(t, \frac{m}{3}) = 1$. Then $x - y = 2^s r - 3t$ is neither divisible by 2 nor 3, contradicting that $\gcd(x - y, m) \in [2, 4]$, which completes the proof. □

We note that most of the possibilities for A given by Lemma 3.1 require G to be finite with $\gcd(|G|, 30) \ne 1$, the only exceptions being those in which $A \subseteq P$ with P a short length arithmetic progression (in which case G is cyclic). Also, if $|nA| \le 4n-6$, then $|nA| \le 3n$, showing there is a gap in the possible cardinalities for $|nA|$. Indeed, we always have

$$\frac{|nA|}{n} \in \{2, 3, 4\} + \{-1/n, 0, 1/n, -4/n, -5/n\}$$

when $|A| < 4n-3$. Conditions (iii)–(vi) each require both $|nA| = |G| - 1$ and $|nA| \ge 4n-5$. Thus, if (1) is weakened to either $|nA| < \min\{|G| - 1, 4n-3\}$ or to $|nA| < \min\{|G|, 4n-5\}$, then only conclusions (i) or (ii) can hold. Conclusions (iii)–(vi) also all require $|G| \equiv 0$ or $1 \mod 4$, and can be eliminated for G infinite or with $|G| \equiv 2$ or $3 \mod 4$.

Proof of Theorem 1.1. Since G is nontrivial with $\langle A\rangle_* = G$, we have $|A| \ge 2$. If $|A| = 2$, then (i) holds with $|P| = |A| = 2$. If $|A| = 3$, then Lemma 3.1 completes the proof. Therefore we may assume $|A| \ge 4$ and w.l.o.g. (by translation) that $0 \in A$. Since nA is aperiodic, Kneser's Theorem implies that $|nA| \ge |(n-1)A| + |A| - 1$. If $|kA| \ge |(k-1)A| + |A| + 1$ for all $k \in [2, n-1]$, then $|(n-1)A| \ge (n-1)|A| + (n-2)$ follows by iterating these bounds, and then $|nA| \ge |(n-1)A| + |A| - 1 \ge |A|n + n - 3$ follows, contrary to hypothesis. Therefore there is some $k \in [2, n-1]$ such that $|kA| \le |(k-1)A| + |A|$, and we can apply Theorem G to $(k-1)A + A$.

If $|kA| \ge |G| - 3$, then $|A| \ge 4$ combined with Theorem F ensures that $(k+1)A = G$, whence $nA = G$ in view of $k < n$, contradicting that nA is aperiodic with G nontrivial. Therefore we can assume $|nA| \le |G| - 4$. Since $|A| \ge 4$ and $|nA| \le |G| - 4$, $((k-1)A, A)$ cannot be elementary of type (I), (IV), (V), (VI) nor (VII). If $((k-1)A, A)$ is elementary of type (II), then (i) follows. If $((k-1)A, A)$ is elementary of type (III), then kA is periodic, and thus also nA (as $k \le n$),

contrary to hypothesis. If $((k-1)A, A)$ is elementary of type (VIII), then (ii) follows. Therefore we can assume $((k-1)A, A)$ is not an elementary pair. If there is an arithmetic progression $P \subseteq G$ such that $A \subseteq P$ with $|P| \le |A|+1$, then (i) follows. Thus Theorem G(iv) must hold.

Let $H < G$ be a finite, nontrivial, proper subgroup such that Theorem G(iv) holds with $A_\emptyset = (x_0+H)\cap A$ and $B_\emptyset = (y_0+H)\cap B$, where $B = (k-1)A$. If $(\phi_H(A), \phi_H(B))$ is elementary of type (I), then this implies that A is contained in an H-coset (since $A \subseteq (k-1)A = B$). However, in view of the hypothesis $\langle A\rangle_* = G$, this is only possible if $H = G$, contradicting that $H < G$ is proper. If $(\phi_H(A), \phi_H(B))$ is elementary of type (III), them $\phi_H(kA) = G/H$ and Theorem G(iv)(e) ensures that $A + B = \Big((A+B) \setminus (A_\emptyset + B_\emptyset)\Big) \cup (A_\emptyset + B_\emptyset)$ is an H-quasi-periodic decomposition. In consequence, since $|\phi_H(A)| \ge 2$, it follows that $(k+1)A = G$, and thus $nA = G$ follows in view of $k < n$, contradicting that nA is aperiodic with G nontrivial. Therefore we must have $(\phi_H(A), \phi_H(B))$ elementary of type (II). As a result, since Theorem G(iv)(b) ensures that $\phi_H(A_\emptyset) + \phi_H(B_\emptyset)$ is a unique expression element in $\phi_H(A) + \phi_H(B)$, we conclude that there is an H-coset progression decomposition $A = A_0 \cup \ldots \cup A_r$ with $A_0 = A_\emptyset$. In view of Theorem G(iv)(c), we have $\sum_{i=1}^{r} |A_i| = r|H| - \epsilon \ge r|H| - 1$ with $\epsilon \in \{0, 1\}$. Since H is proper and $\langle A\rangle_* = G$, we must have $r \ge 1$. In view of Theorem G(iv)(e), we see that either (a) or (b) holds, or else $\Big((A+B) \setminus (A_\emptyset + B_\emptyset)\Big) \cup (A_\emptyset + B_\emptyset)$ is an H-quasi-periodic decomposition. We w.l.o.g. assume the latter is the case (else the proof is complete, as all other parts of (iii) are trivial when $|A_0| = 1$). Since $\phi_H(A)$ is an arithmetic progression with $\phi_H(A_0)$ an end-term, it is now clear that $(hA \setminus hA_0) \cup hA_0$ is an H-quasi-periodic decomposition for any $h \ge k$. In particular, $(nA \setminus nA_0) \cup nA_0$ is an H-quasi-periodic decomposition and

$$|nA| = |H|(|n\phi_H(A)| - 1) + |nA_0| = |H|(n|\phi_H(A)| - n) + |nA_0| = n(|A| - |A_0| + \epsilon) + |nA_0|,$$

implying $|nA| - |A|n = |nA_0| - |A_0|n + \epsilon n$. Thus (a) holds. Moreover, since $(nA \setminus nA_0) \cup nA_0$ is an H-quasi-periodic decomposition with nA aperiodic, we must have nA_0 aperiodic. In particular, $|nA_0| < |K|$ or $|A_0| = 1$, where $K = \langle A_0\rangle_*$. Finally, since $n(|A| - |A_0| + \epsilon) + |nA_0| = |nA| < (|A|+1)n - 3$, it follows that $|nA_0| < (|A_0|+1-\epsilon)n - 3$, and (iii) holds, completing the proof. □

For large n, most of the possibilities given by Theorem 1.1 are not possible, leading to the following non-recursive description.

Corollary 3.2. *Let G be a finite abelian group, let $A \subseteq G$ be a nonempty subset with $\langle A\rangle_* = G$, let $n \ge 3$ be an integer, and let $K = \mathsf{H}(nA)$. If $n \ge \exp(G) + 3$, then*

$$|nA| \ge \min\{|G|, (|A|+1)n - 3\}.$$

If $n \ge \exp(G) - 1$ and $|nA| < \min\{|G|, (|A|+1)n - 3\}$, then one of the following holds.

1. *$n = \exp(G) + 2 = 7$, $G \cong C_5^2$, $|K| = 1$, $|A| = 3$ and $|G| - 1 = |nA| = (|A|+1)n - 4$ with A given by Lemma 3.1(iii).*
2. *$n = \exp(G) + 1$, $4 \mid \exp(G)$ and either*

(a) $n = 5$, $G \cong K \times C_4^2$, $|A|n \le \frac{15}{16}|G|$ *and* $|G| - |K| = |nA| \ge |A + K|n$ *with* $\phi_K(A)$ *given by Lemma 3.1(iii), or*

(b) $n = \frac{1}{4}|G| + 1 \ge 9$, $G \cong C_4 \times C_{\exp(G)}$, $|K| = 1$, $|A|n = 3n = \frac{3}{4}|G| + 3 < |G|$, *and* $|G| - 1 = |nA| = (|A| + 1)n - 5$ *with* A *given by Lemma 3.1(iii).*

3. $n = \exp(G)$, $G \cong H \times C_{\exp(G)}$ *with* $K < H$, $|A|n \le |G|$, $|G| - |K| = |nA| \ge |A + K|n - |K|$, $|\phi_H(A)| = 2$ *and either*

(a) $H/K \cong C_2^2$ *and* $(\phi_K(A), \phi_K(A))$ *is elementary of type (VIII) with* $|\phi_K(A)| = 4$, *or*

(b) $|H/K| \ge 3$ *and* $z + A + K = (H \setminus K) \cup (x + K)$ *for some* $z \in G$ *and* $x \in G \setminus H$.

4. $n = \exp(G) - 1$, $G \cong H \times C_{\exp(G)}$ *with* $K < H$ *proper,* $|\phi_H(A)| = 2$, *and either*

(a) $|A|n \le \frac{\exp(G)-1}{\exp(G)}|G|$, $|G| - |H| = |nA| \ge |A + K|n$, *and 3(a) or 3(b) holds,*

(b) $z + A + K = H \setminus K \cup (A_0 + K)$ *for some* $z \in G$ *with* $A_0 = A \setminus H \ne \emptyset$, $|A|n \le |G| - 2|K|$, *and* $|G| - |H| + |n(A_0 + K)| = |nA| \ge |A + K|n + |K|$,

(c) $z + A + K = H \cup (A_0 + K)$ *for some* $z \in G$ *with* $A_0 = A \setminus H \ne \emptyset$, $|A|n \le |G|$, *and* $|nA| = |G| - |H| + |n(A_0 + K)|$, *or*

(d) $G = H_0 \oplus H_1 \oplus \ldots \oplus H_r$ *with* $K < H_0$ *proper,* $r \ge 1$ *and* $H_i = \langle x_i \rangle \cong C_{\exp(G)}$ *for all* $i \in [1, r]$, $z + A + K = \bigcup_{j=0}^{r} \big(K + \sum_{i=0}^{j-1} H_i + \sum_{i=j+1}^{r} x_i\big)$ *for some* $z \in G$, $|A|n \le |G| - |H_0| + (\exp(G) - 1)|K| \le \frac{p \exp(G)^r + \exp(G) - p - 1}{p \exp(G)^r}|G|$, *where* p *is the smallest prime divisor of* $\exp(H_0)$, *and* $|nA| = |G| - |H_0| + |K|$.

Proof. We may assume

$$n \ge \max\{3, \exp(G) - 1\},$$

as the corollary only applies in these cases. Let $K = \mathsf{H}(nA)$, let $X = \phi_K(A)$ and suppose $|nA| < \min\{|G|, (|A| + 1)n - 3\}$. If $|X| = |\phi_K(A)| = 1$, then $nA = \langle A \rangle_* = G = K$, contrary to assumption. Therefore we can assume $|X| = |\phi_K(A)| \ge 2$. In particular, G/K is nontrivial. Observe that $|nA| = |nX||K|$. Thus, if $|nX| \ge x|X| + y$ for some integers $x \ge 0$ and y, then $|nA| \ge x|A| + y|K|$ as well. In particular, we have $|nX| < \min\{|G/K|, (|X| + 1)n - 3\}$ and can apply Theorem 1.1 to nX. We proceed to go through the possibilities for X given by Theorem 1.1 one by one.

Case A. Suppose there is an arithmetic progression $P \subseteq G/K$ with $X \subseteq P$. Then $\langle P \rangle_* = \langle X \rangle_* = G/K$ is cyclic with $|G/K| \le \exp(G)$. If $|P| = |X|$, then, since $nX \ne G/K$ and $|X| \ge 2$, it follows that $n \le |G/K| - 2 \le \exp(G) - 2$. If $|P| = |X| + 1$, then $|X| \ge 3$ and $|nX| \ge |X|n - 1 \ge 3n - 1$, forcing $n \le \frac{1}{3}|G/K| \le |G/K| - 2 \le \exp(G) - 2$. If $|X| = 3$, $|P| = 5$ and either $|nX| = 4n - 5 = |G/K| - 1$ or $|nX| = 4n - 4 = |G/K| - 1$, then $n \le \frac{1}{4}|G/K| + 1 \le |G/K| - 2 \le \exp(G) - 2$. If $|P| = 6$, $|G/K| = 21$ and $|nX| = 4n - 4 = |G/K| - 1 = 20$, then $n = 6 < 19 = |G/K| - 2 \le \exp(G) - 2$. In all cases, we obtain the contradiction $n \le \exp(G) - 2$, thus handling all possibilities when X is contained in a short length arithmetic progression. In

particular, the theorem is now established for $G \cong C_p$ with p prime, allowing us to proceed by induction on $|G|$.

Case B. Suppose (X, X) is an elementary pair of type (VIII) with $|X| \geq 4$. Then there exists some $H/K \leq G/K$ with $H/K \cong C_2^2$ and G/H cyclic. Thus $|G/H| \leq \exp(G)$. Indeed, $|G/H|$ divides $\exp(G)$, in which case either $|G/H| = \exp(G)$ or $|G/H| \leq \frac{1}{2}\exp(G)$. Since $nX \neq G/K$, we must have $3 \leq n \leq |G/H| \leq \exp(G)$. If the latter bound is strict, we obtain the contradiction $3 \leq n \leq \frac{1}{2}\exp(G) \leq \exp(G) - 2$. As a result, we must have $|G/H| = \exp(G)$, whence $G \cong H \times C_{\exp(G)}$, in which case $\exp(G)$ must be even (as H contains a subgroup isomorphic to C_2^2). We also have either $|nX| = |X|n \leq |G/K| - 1$ or else $|nX| = |X|n - 1 = |G/K| - 1$. Thus $n \leq \frac{|G/K|}{|X|} \leq \frac{1}{4}|G/K| = |G/H| = \exp(G)$. If $|X| > 4$, then $|X| \geq 8$ and we can improve the bound to $3 \leq n \leq \frac{1}{2}\exp(G) \leq \exp(G) - 2$, contrary to assumption. Therefore $|X| = 4$ and $|\phi_H(A)| = 2$. If $n = \exp(G) - 1$, then $|A|n \leq |X||K|n = 4|K|(\exp(G) - 1) = |G| - |H| = \frac{\exp(G)-1}{\exp(G)}|G|$ and $|G| - |H| = |nA| = |A + K|n$, whence 4(a) holds. If $n = \exp(G)$, then $|G| - |K| = |nA| = |A + K|n - |K|$ and $|A|n \leq |X||K|n = 4n|K| = 4\exp(G)|K| = |G|$, whence 3(a) holds.

Case C. Suppose there is a finite, nontrivial, proper subgroup $H/K < G/K$ and H/K-coset progression decomposition $X = X_0 \cup \ldots \cup X_t$ such that Theorem 1.1(iii) holds. Then $t \geq 1$, G/H is cyclic and generated by $\phi_H(X_1) - \phi_H(X_0)$, $|G/H| \leq \exp(G)$, $\sum_{i=1}^{t} |X_i| = t|H/K| - \epsilon$ with $\epsilon \in \{0, 1\}$, and nX_0 is aperiodic. As in the previous case, $|G/H|$ divides $\exp(G)$, and thus $|G/H| < \exp(G)$ implies that $|G/H| \leq \frac{1}{2}\exp(G)$.

If Theorem 1.1(iii)(b) holds, then $t \geq 2$. Moreover, since $nX \neq G/K$ is aperiodic, we must have $2n + 1 \leq tn + 1 = |\phi_H(X)|n - n + 1 \leq |G/H| + 1$, implying $3 \leq n \leq \frac{1}{2}|G/H| \leq \frac{1}{2}\exp(G) \leq \exp(G) - 2$, contrary to assumption.

If Theorem 1.1(iii)(c) holds, then $nX \neq G/K$ aperiodic again forces $tn + 1 = |\phi_H(X)|n - n + 1 \leq |G/H| + 1$. Thus we obtain a contradiction as in the previous case unless $t = 1$ and $n \leq |G/H| = \exp(G)$. In consequence, $|\phi_H(A)| = t+1 = 2$, $|X| = |H/K|$, and $G \cong H \times C_{\exp(G)}$. Since $|X| = |H/K|$, we must have $|H/K| \geq 3$, for otherwise X is arithmetic progression, which was handled during Case A. If $n = \exp(G) - 1$, then $|G/K| - |H/K| = |nX| = |X|n$, $|G| - |H| = |nA| = |nX||K| = |A + K|n$ and $|A|n \leq n|X||K| = (\exp(G) - 1)|H| = |G| - |H| = \frac{\exp(G)-1}{\exp(G)}|G|$, whence 4(a) holds. If $n = \exp(G)$, then $|G/K| - 1 = |nX| = |X|n - 1$, $|G| - |K| = |nA| = |A + K|n - |K|$, and $|A|n \leq |X||K|n = |H|\exp(G) = |G|$. Thus 3(b) holds.

If Theorem 1.1(iii)(a) holds, then $nX \neq G/K$ implies that $tn + 1 = n|\phi_H(A)| - n + 1 \leq |G/H| \leq \exp(G)$. Consequently, if $|G/H| \leq \frac{1}{2}\exp(G)$ or $t \geq 2$, then we obtain the contradiction $3 \leq n \leq \frac{\exp(G)-1}{2} \leq \exp(G) - 2$. Therefore we must have $t = 1$ and $|G/H| = \exp(G)$, in which case $|\phi_H(A)| = 2$, $G \cong H \times C_{\exp(G)}$ and $n + 1 \leq \exp(G)$, in turn implying $n = \exp(G) - 1$. Since Theorem 1.1(iii)(a) holds with $n = \exp(G) - 1$, we have $nA = \big(G \setminus (H + nA_0)\big) \cup nA_0$. In

particular, $\overline{nA_0\,^H} = \overline{nA\,^G}$,

$$(5)\quad |nA| = |G| - |H| + |n(A_0+K)| \qquad \text{and} \qquad \mathsf{H}(nA_0) = \mathsf{H}(\overline{nA_0\,^H}) = \mathsf{H}(\overline{nA\,^G}) = \mathsf{H}(nA) = K.$$

In particular, $\mathsf{H}(nA_0) = K$ implies that $nA_0 = n(A_0+K)$.

If $\epsilon = 1$, then $z + A + K = (H \setminus K) \cup (A_0 + K)$ for some $z \in G$ with $A_0 = A \setminus H \neq \emptyset$ and $\phi_K(A_0) = X_0$. Moreover, $nA = nA'$ (since Theorem 1.1(iii)(a) holds), where $A' = H \cup (A_0 + K)$. Since $K = \mathsf{H}(nA) = \mathsf{H}(nA')$, Kneser's Theorem implies

$$(6)\qquad |nA| = |nA'| \geq n|A' + K| - (n-1)|K| = n|A+K| + |K|.$$

Since $\mathsf{H}(nA_0) = K < H$ by (5), we have $|nA_0| = |n(A_0+K)| \leq |H| - |K|$, which combined with (6) and (5) implies $|A|n \leq |A+K|n \leq |nA| - |K| \leq |G| - 2|K|$. Thus 4(b) holds.

If $\epsilon = 0$, then, by w.l.o.g. replacing A with an appropriate translate, we have $A + K = H \cup (A_0+K)$ with $A_0 = A\setminus H \neq \emptyset$ and $\phi_K(A_0) = X_0$. Letting $H' = \langle A_0\rangle_* \leq H$, we have $K \leq H' \leq H$ in view of (5). If $|X_0| = 1$, then $|nA_0| = |n(A_0+K)| = |K|$, $|A| \leq |X||K| = |H| + |K|$ and $|K| \leq \frac{1}{p}|H|$, where p is the smallest prime divisor of $\exp(H)$ (since $K < H$ is a proper subgroup in view of H/K being nontrivial). Thus

$$\begin{aligned} |A|n &\leq (|H|+|K|)(\exp(G)-1) = |G| - |H| + (\exp(G)-1)|K| \\ &\leq \frac{p+1}{p}(|G|-|H|) = \frac{p\exp(G) + \exp(G) - p - 1}{p\exp(G)}|G|, \end{aligned}$$

in which case 4(d) holds with $H_0 = H$ and $r = 1$. Therefore we may now assume $|X_0| > 1$, whence $K < H'$ is a proper subgroup and H'/K is nontrivial. In particular, since nX_0 is aperiodic, we must have $|nX_0| < |H'/K| \leq |H/K|$. Thus, if $|nX_0| \geq |X_0|n$, then we have $|X_0|n \leq |nX_0| \leq |H/K| - 1$, whence $|A|n \leq |H|n + |X_0||K|n \leq |G| - |K|$, meaning 4(c) holds. Therefore we may instead assume

$$(7)\qquad |nX_0| < \min\{|H'/K|, |X_0|n\} \qquad \text{and} \qquad |nA_0| < \min\{|H'|, |A_0+K|n\},$$

where the second inequality follows by multiplying the first by $|K|$. Since $3 \leq n = \exp(G)-1$, we have $\exp(G) \geq 4$. If $\exp(H'/K) < \exp(G)$, then $\exp(H'/K) \leq \frac{1}{2}\exp(G)$ and $n = \exp(G) - 1 \geq \frac{1}{2}\exp(G) + 1 \geq \exp(H'/K) + 1$. Consequently, applying the induction hypothesis to nX_0 yields $|nX_0| \geq |X_0|n$, contrary to (7). Therefore we instead conclude that $\exp(H'/K) = \exp(H') = \exp(H) = \exp(G)$. But now (7) and (5) combined with an application of the induction hypothesis to $n(A_0 - y)$, where $y \in A_0$ is any element, imply either $|A_0|n \leq |H'| \leq |H|$ or else that 4(d) holds for $n(A_0 - y)$. In the former case, we have $|A|n \leq |H|n + |A_0|n = |G| - |H| + |A_0|n \leq |G|$, whence 4(c) holds. On the other hand, in the latter case, we have $H' = H_0 \oplus H_1 \oplus \ldots \oplus H_{r-1}$ with $K < H_0$ proper, $r - 1 \geq 1$, $H_i = \langle x_i\rangle \cong C_{\exp(H')} \cong C_{\exp(G)}$ for all $i \in [1, r-1]$,

$$(8)\qquad z + A_0 - y + K = \bigcup_{j=0}^{r-1} \big(K + \sum_{i=0}^{j-1} H_i + \sum_{i=j+1}^{r-1} x_i\big)$$

for some $z \in H'$,

$$|A_0|n \le |H'| - |H_0| + (\exp(G)-1)|K| \le \frac{p\exp(G)^{r-1} + \exp(G) - p - 1}{p\exp(G)^{r-1}}|H'|, \tag{9}$$

where p is the smallest prime divisor of $\exp(H_0)$, and

$$|nA_0| = |H'| - |H_0| + |K|. \tag{10}$$

If $H' \neq H$, then $|H'| \le \frac{1}{2}|H|$, in which case (9) implies $|A_0|n < |H|$ and $|A| \le |H|n + |A_0|n < |H|(n+1) = |G|$, whence 4(c) holds. Therefore we may assume $H' = H$. Since $y \in A_0$ and since $\langle \phi_H(A_0)\rangle = \langle \phi_H(A)\rangle = G/H$ (recall $A + K = H \cup (A_0 + K)$) with $|G/H| = \exp(G)$, we have $G = H \oplus \langle y\rangle$. Thus, letting $x_r = y$ and $H_r = \langle x_r\rangle = \langle y\rangle \cong C_{\exp(G)}$, we find that $G = H \oplus H_r = H' \oplus H_r = H_0 \oplus H_1 \oplus \ldots \oplus H_r$. In view of (8), $z \in H' = H$ and $K < H_0$, we have $z + A + K = (z+H) \cup (z + A_0 + K) = H \cup (z + A_0 + K) = \bigcup_{j=0}^{r} \big(K + \sum_{i=0}^{j-1} H_i + \sum_{i=j+1}^{r} x_i\big)$. In view of (9) and $H' = H$, we have $|A|n \le |H|n + |A_0|n = |G| - |H| + |A_0|n \le |G| - |H_0| + (\exp(G)-1)|K| \le |G| - |H_0| + (\exp(G)-1)\frac{|H_0|}{p} = \frac{p\exp(G)^r + \exp(G) - p - 1}{p\exp(G)^r}|G|$, where p is the smallest prime divisor of $\exp(H_0)$ (since $K < H_0$ is proper). In view of (10), (5) and $H' = H$, we have $|nA| = |G| - |H| + |nA_0| = |G| - |H_0| + |K|$. Thus 4(d) holds.

Case D. Suppose that $|X| = 3$ and there is an H/K-coset decomposition $X = X_1 \cup X_0$ with $|X_1| = 2$, $|X_0| = 1$ and $\langle X_1\rangle_* = H/K$ cyclic. Then G/H is generated by a non-zero difference from $\phi_H(X_1 - X_0)$, ensuring that G/H is cyclic, whence $|G/H| \le \exp(G)$ with $|G/H| \le \frac{1}{2}\exp(G)$ when equality fails (as in previous cases).

If $2 \le |H/K| \le 3$, then Theorem 1.1(iii)(a) or (iii)(c) holds, which was handled in Case C. If $|H/K| = 4$ and $|nX| = 4n - 5 = |G/K| - 1$, then $4 \mid \exp(G)$ (as H/K is cyclic of order 4),

$$|nA| = |G| - |K|$$

and $3 \le n = \frac{1}{4}|G/K| + 1 = |G/H| + 1 \le \exp(G) + 1$. If the latter inequality is strict, we obtain the contradiction $3 \le n = |G/H| + 1 \le \frac{1}{2}\exp(G) + 1 \le \exp(G) - 2$ unless $\exp(G) = 4$, $|G/H| = \frac{1}{2}\exp(G) = 2$ and $n = 3 = \frac{1}{4}|G/K| + 1$. In this case, since $nX \neq G/K$, Theorem F implies that $|2X| \le |G/K| - 3 = 5$. Translating as necessary, we can w.l.o.g. assume $X_1 = \{0, x\}$ and $X_0 = \{y\}$. Thus $2X = \{0, x, 2x\} \cup \{y, y+x\} \cup \{2y\}$. Since $|2X| \le 5$ and $|H/K| = 4$, we must have $2y \in \{0, x, 2x\}$. If $2y = x$, then $X = \{0, y, 2y = x\}$ is an arithmetic progression, which was handled in Case A. If $2y = 2x$, then $\mathrm{ord}(x - y) = 2$ and $X = \{x, y\} \cup \{0\}$ is an H'/K-coset decomposition with $|H'/K| = 2$. Thus Theorem 1.1(iii)(a) holds, which was handled in Case C. Finally, if $2y = 0$, then $\mathrm{ord}(y) = 2$ and $X = \{0, y\} \cup \{x\}$ is an H'/K-coset decomposition with $|H'/K| = 2$, in which case Theorem 1.1(iii)(a) again holds, which was handled in Case C. Thus we can instead assume $|G/H| = \exp(G)$ and $n = |G/H| + 1 = \exp(G) + 1 \ge 5$. In particular, $G \cong H \times C_{\exp(G)}$. We also have

$$|A + K|n + (n-5)|K| = (4n-5)|K| = |nX||K| = |nA| \le |A|n + n - 4 \le 3n|K| + n - 4,$$

which (in view of $n \ge 5$) implies either $|K| = 1$ or $n \le 6$. Since $n = \exp(G) + 1$ with $4 \mid \exp(G)$, we conclude that $n = 6$ is not possible. If $n = 5$, then $|G/H| = \exp(G) = 4$ and $|A|n \le 15|K| \le \frac{15}{16}|G|$. Moreover, since H/K is a cyclic group of order $4 = \exp(G)$ with $G \cong H \times C_4$, it follows that $\exp(H) = \exp(G) = 4$ with $H \cong K \times C_4$. Thus 2(a) holds. On the other hand, if $n > 5$, then $|K| = 1$, $|H| = 4$, $\frac{1}{4}|G| + 1 = |G/H| + 1 = n \ge 9$, and $|A|n = 3n = 3\exp(G) + 3 = 3|G/H| + 3 = \frac{3}{4}|G| + 3 < |G|$. Moreover, since $H/K = H$ is a cyclic group of order 4, we have $G \cong H \times C_{\exp(G)} \cong C_4 \times C_{\exp(G)}$. Thus 2(b) holds.

If $|H/K| = |G/H| = 5$, $n = 7$ and $|nX| = 4n - 4 = |G/K| - 1 = 24$, then $5 \mid \exp(G)$. We must have $5 = |G/H| = \exp(G)$, for otherwise $\exp(G) \ge 2|G/H| = 10$, contradicting that $7 = n \ge \exp(G) - 1$. Hence $G \cong C_5^s$, $H \cong C_5^{s-1}$ and $K \cong C_5^{s-2}$, where $s \ge 2$. We now have $(|A| + 1)n - 3 > |nA| = |nX||K| = 24|K| = 3n|K| + 3|K| \ge n|A| + 3|K|$, implying $3|K| < 4$, and thus $|K| = 1$. Hence $G \cong C_5^2$, $|A| = 3$, and $|G| - 1 = |nA| = 24 = (|A| + 1)n - 4$. Thus 1 holds.

Case E. Suppose Lemma 3.1(iv) holds, in which case there is an H/K-coset decomposition $X = \{x, z\} \cup \{y\}$ with $2(y + z) = 4x$ and $\langle x - z\rangle = H/K \le G/K$ a cyclic subgroup such that $|G/H| = 2$. Moreover, $G/K \cong C_2 \times C_m$ with m even. Hence $\exp(G) \ge \exp(G/K) = \frac{1}{2}|G/K|$. We have $|nX| = 4n - 5 = |G/K| - 1$, ensuring that $3 \le n = \frac{1}{4}|G/K| + 1 = \frac{1}{2}\exp(G/K) + 1 \le \frac{1}{2}\exp(G) + 1$, which contradicts that $n \ge \exp(G) - 1$ unless $m = \exp(G/K) = \exp(G) = 4$. Thus $G/K \cong C_2 \times C_4$ and $n = \frac{1}{4}|G/K| + 1 = 3$. By lemma 3.1(iv), we also have $2(y - z) = 4(x - z) = 0$, with the latter equality in view of $\exp(G/K) = 4$. Thus $X = \{y, z\} \cup \{x\}$ is an H'/K-coset decomposition with $H'/K = \langle y - z\rangle$ a subgroup of order 2, in which case Theorem 1.1(iii)(a) holds with $\epsilon = 0$ and $|X_0| = 1$, which was handled in Case C.

Case F. Suppose Lemma 3.1(vi) holds, in which case G/K is cyclic and $4n - 5 = |nX| = |G/K| - 1$. Thus $3 \le n = \frac{1}{4}|G/K| + 1 \le \frac{1}{4}\exp(G) + 1 \le \exp(G) - 2$, contrary to assumption. As this exhausts the last possibility for X, the proof is now complete. □

When $|A|$ is large, the previous corollary simplifies drastically.

Corollary 3.3. *Let G be a finite abelian group, let $A \subseteq G$ be a nonempty subset with $\langle A\rangle_* = G$, let $n \ge 1$ be an integer, let $K = \mathsf{H}(nA)$ and suppose $n|A| > |G|$.*

1. *If $n \ge \exp(G)$, then $nA = G$.*
2. *If $n = \exp(G) - 1$ and $nA \ne G$, then $\exp(G)$ is composite, $G = H_0 \oplus H_1 \oplus \ldots \oplus H_r$ with $K < H_0$ proper, $r \ge 1$ and $H_i = \langle x_i\rangle \cong C_{\exp(G)}$ for all $i \in [1, r]$ (thus G is non-cyclic),*

$$z + A + K = \bigcup_{j=0}^{r} \big(K + \sum_{i=0}^{j-1} H_i + \sum_{i=j+1}^{r} x_i\big) \quad \text{for some } z \in G,$$

$|A|n \le |G| - |H_0| + (\exp(G) - 1)|K| \le \frac{p\exp(G)^r + \exp(G) - p - 1}{p\exp(G)^r}|G|$, where p is the smallest prime divisor of $\exp(H_0)$, and $|nA| = |G| - |H_0| + |K|$.

Proof. Since $n|A| > |G|$, we must have $n \geq 2$. If $n = 2$, then Theorem F and $2|A| = n|A| > |G|$ implies $nA = G$, either as desired or contrary to hypothesis. Therefore we can assume $n \geq 3$. We may assume $nA \neq G$, as there is nothing to prove otherwise, in which case $|nA| < |G| < n|A| \leq n|A| + n - 3$, allowing us to apply Corollary 3.2. We observe that $|nA| \geq |A|n \geq |G|$ for all possibilities with $n \geq \exp(G) + 1$. If $n = \exp(G)$, all possibilities from Corollary 3.2 have $|A|n \leq |G|$, contrary to hypothesis. This establishes Item 1. Next suppose that $n = \exp(G) - 1$. Then the hypothesis $|A|n > |G|$ means that Corollary 3.2.4(d) must hold with $\exp(G)$ composite, else $|A|n \leq \frac{p\exp(G)^r + \exp(G) - p - 1}{p\exp(G)^r}|G| = \frac{p\exp(G)^r - 1}{p\exp(G)^r}|G| < |G|$, and now Item 2 follows. □

4. Subsequence Sums

In this section, we provide the proofs for Theorems 1.2 and 1.3. We begin with a lemma that can be combined with the Partition Theorem to show that only one of two extremes is possible for the subgroup $\langle X\rangle_*$.

Lemma 4.1. *Let G be an abelian group, let $n \geq 1$, let $S \in \mathcal{F}(G)$ be a sequence, let $S' \mid S$ be a subsequence with $\mathsf{h}(S') \leq n \leq |S'|$, let $H = \mathsf{H}(\Sigma_n(S))$, let $X \subseteq G/H$ be the subset of all $x \in G/H$ for which x has multiplicity at least n in $\phi_H(S)$, and let $Z = \phi_H^{-1}(X)$. Suppose $|\Sigma_n(S)| < |S'| - n + 1$. Then either*

$$\langle Z\rangle_* = H \quad \text{or} \quad \langle Z\rangle_* = \langle \mathrm{Supp}(S)\rangle_*.$$

Proof. By translating the terms of S appropriately, we can w.l.o.g. assume $0 \in \mathrm{Supp}(S) \cap Z$. Let $L = \langle Z\rangle_* = \langle Z\rangle$. Since $|\Sigma_n(S)| < |S'| - n + 1$, we can apply Theorem E.2 to $\Sigma_n(S)$ and let $\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n$ be the resulting setpartition. Then $\Sigma_n(S) = \sum_{i=1}^{n} A_i$, H is nontrivial, $Z \neq \emptyset$, and

$$|S'| - n \geq |\sum_{i=1}^{n} A_i| \geq |S'| - n + 1 - (n - e - 1)(|H| - 1) + \rho, \tag{11}$$

with e and $\rho \geq 0$ as defined in Theorem E. Note (11) implies that $e \leq n-2$. Since $H = \mathsf{H}(\Sigma_n(S))$, we have $H \leq \langle \mathrm{Supp}(S)\rangle_*$, while $H \leq \langle Z\rangle_* = L$ follow by definition of Z. Thus it suffices to show $\langle \phi_H(\mathrm{Supp}(S))\rangle_* = \langle \phi_H(Z)\rangle_* = \langle X\rangle_* = L/H$. Since $\phi_H(Z) \subseteq \phi_H(\mathrm{Supp}(S))$, the inclusion $L/H \leq \langle \phi_H(\mathrm{Supp}(S))\rangle_*$ is trivial. Assuming by contradiction that the reverse inclusion is false, then there must some $x \in \mathrm{Supp}(S) \setminus L$. Re-index the A_i so that $\phi_H(A_i) = X \subseteq L/H$ for $i = 1, \ldots, k$ and $A_{k+1} \nsubseteq L$, where $k = n - e \geq 2$.

Let $N = |X|$. We may assume $L/H = \langle X\rangle_*$ is nontrivial and $N \geq 2$, else $H = L$ follows, yielding the other desired conclusion. Since $H = \mathsf{H}(\Sigma_n(S)) = \mathsf{H}(\sum_{i=1}^{n} A_i)$, it follows that $\sum_{i=1}^{n} \phi_H(A_i)$ is aperiodic. In particular, kX is aperiodic, whence Kneser's Theorem implies that $|\sum_{i=1}^{k} \phi_H(A_i)| = |kX| \geq kN - k + 1$. Since $0 \in X \subseteq \phi_H(A_{k+1}) \nsubseteq L/H$ and $\sum_{i=1}^{k} A_i \subseteq L$, we have $|\sum_{i=1}^{k+1} \phi_H(A_i)| \geq$

$2|\sum_{i=1}^{k}\phi_H(A_i)| \ge 2kN-2(k-1)$. Since $\sum_{i=1}^{n}\phi_H(A_i)$ is aperiodic, Kneser's Theorem implies

$$\begin{aligned} |\sum_{i=1}^{n}\phi_H(A_i)| &\ge |\sum_{i=1}^{k+1}\phi_H(A_i)| + \sum_{i=k+2}^{n}|\phi_H(A_i)| - (n-k)+1 \\ &\ge 2kN-2(k-1)+(n-k-1)(N+1)-n+k+1 \\ &= (n+k-1)N-2(k-1). \end{aligned}$$

Thus, since $H = \mathsf{H}(\sum_{i=1}^{n}A_i)$, it follows that $|\sum_{i=1}^{n}A_i| \ge (n+k-1)N|H|-2(k-1)|H|$. By hypothesis, $|\sum_{i=1}^{n}A_i| = |\Sigma_n(S)| \le |S'|-n \le nN|H|+e-n = nN|H|-k$. Combining this with the previous estimate, we obtain $nN|H|-k \ge (n+k-1)N|H|-2(k-1)|H|$, implying $-k \ge (k-1)N|H|-2(k-1)|H| \ge 0$, where the final inequality makes use of $N \ge 2$. But since $k = n-e \ge 2$, this is a contradiction, completing the proof. □

Proof of Theorem 1.3. Let $H = \mathsf{H}(\Sigma_n(S))$, let $X \subseteq G/H$ be the subset of all $x \in G/H$ for which x has multiplicity at least n in $\phi_H(S)$, and let $Z = \phi_H^{-1}(X) \subseteq G$. Apply Theorem E to $\Sigma_n(S)$ using $S' = S$ and let $\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n$ be the resulting setpartition. If $|\sum_{i=1}^{n}A_i| \ge \sum_{i=1}^{n}|A_i|-n+1 = |S|-n+1 \ge |G|$, then $\Sigma_n(S) = G$ follows from Theorem E. Therefore we can assume Theorem E.2 holds. Thus, letting $N = |X|$ and $e = \sum_{i=1}^{n}|A_i \setminus Z|$, it follows that

$$(|S|-n+1)-(n-e-1)(|H|-1) \le ((N-1)n+e+1)|H| \le |\Sigma_n(S)| = |\sum_{i=1}^{n}A_i| \le |G|-|H|, \tag{12}$$

else the desired conclusion $\Sigma_n(S) = G$ follows. In particular, $e \le n-2$ in view of $|S|-n+1 \ge |G|$, and $H < G$ is a nontrivial subgroup. We also must have $N \ge 1$, else $e = |S|$ follows, in which case (12) implies $|\Sigma_n(S)| \ge (|S|-n+1)|H| \ge |G|$, contrary to assumption. Thus X is nonempty. If $N = 1$, then (12) implies that $e \le |G/H|-2$, contrary to the coset condition hypothesis. Therefore we must have $N = |X| \ge 2$. By translating, we can w.l.o.g. assume $0 \in Z \cap \mathrm{Supp}(S)$. By re-indexing the A_i, we can also assume

$$\phi_H(A_i) = X \quad \text{for } i = 1, \ldots, k,$$

where $k = n-e \ge 2$.

We must have $\langle \mathrm{Supp}(S)\rangle_* = G$, for if $L = \langle \mathrm{Supp}(S)\rangle_* < G$ is a proper subgroup, then all but $0 \le |G/L|-2$ terms of S are from the subgroup L, contrary to hypothesis. Consequently, if $\langle Z\rangle_* < G = \langle \mathrm{Supp}(S)\rangle_*$ is proper, then, since $|X| = |\phi_H(Z)| \ge 2$, Lemma 4.1 implies that $|\Sigma_n(S)| \ge |S|-n+1 \ge |G|$, contrary to hypothesis. Therefore we instead conclude that

$$\langle Z\rangle_* = G \quad \text{and} \quad \langle X\rangle_* = G/H. \tag{13}$$

Assume by contradiction that $\Sigma_n(S) \neq G$. Then, in view of $H = \mathsf{H}(\sum_{i=1}^{n} A_i)$, we have

$$nX \neq G/H. \tag{14}$$

Since $e \leq n-2$, we have $|Z|n \geq |S|-e \geq (n+|G|-1)-(n-2) > |G|$. Thus, since $|X| \geq |Z|/|H|$, we conclude that

$$|X|n > |G/H|. \tag{15}$$

If $n = 1$, then $|S| \geq |G|+n-1$ and $\mathsf{h}(S) \leq n$ imply $\mathrm{Supp}(S) = G$, whence $\Sigma_n(S) = G$ follows, contrary to assumption. If $n = 2$, then $|S| \geq |G| + n - 1 \geq |G| + 1$ and $\mathsf{h}(S) \leq 2$. Applying Theorem F to $A_1 + A_2$ yields $|\Sigma_n(S)| = |\sum_{i=1}^{n} A_i| = |A_1 + A_2| = |G|$, contrary to assumption. Therefore we must have $n \geq 3$.

If $n \geq \exp(G) \geq \exp(G/H)$, we can apply Corollary 3.3.1 to nX (in view of (13) and (15)) to obtain $nX = G/H$, contradicting (14). Thus Item 1 is complete.

If $n \geq \exp(G)-1 \geq \exp(G/H)-1$, we can apply Corollary 3.3 to nX to conclude $\exp(G/H) = \exp(G)$ is composite and G/H is non-cyclic. This completes Item 2 when $\exp(G)$ is prime. Moreover, if $G \cong H' \oplus C_{\exp(G)}$ with $|H'|$ prime, then $\exp(G/H) = \exp(G)$ is only possible if $G \cong H \oplus C_{\exp(G)}$ with $G/H \cong C_{\exp(G)}$ cyclic, contrary to assumption. Thus Item 2 is complete in all cases.

If G is cyclic and $n \geq \frac{1}{p}|G| - 1$, where p is the smallest prime divisor of $|G|$, then $n \geq |G/H| - 1 = \exp(G/H) - 1$ follows in view of H being nontrivial. Then, since G/H is cyclic, Corollary 3.3.2 implies that $nX = G/H$, contrary to hypothesis.

If $\exp(G) \leq 3$, then $n \geq 3 \geq \exp(G)$, in which case Item 1 implies that Item 4 holds. If $|G| < 10$, then $|G/H| \leq 4$ (since H is nontrivial). Thus (12) yields the contradiction $|G| > |\sum_{i=1}^{n} A_i| \geq ((N-1)n+1)|H| \geq (n+1)|H| \geq 4|H| \geq |G|$. □

Next, we give the proof of Theorem 1.2, which follows rather quickly using Theorem 1.3.

Proof of Theorem 1.2. Let $n = |S|-|G|$. Then $\Sigma_{|G|}(S) = \sigma(S)-\Sigma_n(S)$ and $|S| = n+|G|$. Thus Theorem 1.2 follows immediately from Theorem 1.3 except when $\exp(G) = 4$ and $|G| = 16$, or when $|G| = 10$. Assume by contradiction that $\Sigma_{|G|}(S) \neq G$, and thus $\Sigma_n(S) \neq G$ as well. If $n = 1$, then $\mathsf{h}(S) \leq n$ and $|S| = |G| + n$ cannot both hold, meaning $n \geq 2$. If $n = 2$, then $\mathsf{h}(S) \leq n$ and $|S| \geq |G| + n$ imply $\Sigma_n(S) = G$ as argued in the proof of Theorem 1.3. Therefore we must have $n \geq 3$. Assume by contradiction that $|\Sigma_n(S)| < |G| < |S| - n + 1$. We proceed as in the proof of Theorem 1.3, including all notation used there, e.g., H, $X \subseteq G/H$, Z, $\mathcal{A} = A_1 \cdot \ldots \cdot A_n$, N and e. In particular, we again conclude that $H < G$ is proper and nontrivial, $nX \neq G/H$, $e \leq n-2$, $|X| = N \geq 2$, $\langle X \rangle_* = G/H$ and $|X|n > |G/H|$, allowing us to apply Corollary 3.3 to nX. By Theorem E applied to $\Sigma_n(S)$ with $S = S'$, we have

$$((N-1)n + e + 1)|H| \leq |\Sigma_n(S)| \leq |G| - |H|. \tag{16}$$

If $|G| = 10$, then G is cyclic and $\exp(G/H) = |G/H| \in \{2, 5\}$. If $\exp(G/H) = 2 < n$, then Corollary 3.3.1 implies $nX = G/H$, contrary to assumption. Therefore $|H| = 2$ and $\exp(G/H) = 5$ is prime, whence G/H is cyclic. Thus, if $n \geq 4 = \exp(G/H) - 1$, then Corollary 3.3.2 again gives the contradiction $nX = G/H$. Therefore we must have $n = 3$. If $N \geq 3$, then Theorem F implies that $2X = G/H$, contradicting that $nX = 3X \neq G/H$. Therefore $N = |X| = 2$, which combined with $e \leq n - 2 = 1$ ensures that $13 = |G| + n = |S| \leq n|H|N + e \leq 13$, forcing equality to hold in all estimates. In particular, $e = 1$. But then (16) yields the contradiction $10 = 2(e + 4) = (n + e + 1)|H| \leq 8$.

If $\exp(G) = 4$ and $|G| = 16$, then Corollary 3.3 yields the contradiction $nX = G/H$ unless $n = 3 = \exp(G/H) - 1$ with G/H non-cyclic, which is only possible if $|H| = 2$ and $G/H \cong C_2 \times C_4$. In this case, Corollary 3.3.2 instead implies $3|X| = |X|n \leq \frac{2\exp(G/H)+\exp(G/H)-2-1}{2\exp(G/H)}|G/H| = 9$. Hence $|X| \leq 3$, $e \leq n-2 = 1$ and $19 = |G|+n = |S| \leq |X||H|n+e \leq 18+1 = 19$. We therefore conclude that equality must hold in all estimates, in which case $e = 1$ and $N = |X| = 3$. But then (16) yields the contradiction $16 = 2(e + 7) = (2n + e + 1)|H| \leq 14$. □

References

[1] M. DeVos, L. Goddyn and B. Mohar, A generalization of Knesers addition theorem, *Adv. Math.* **220** (2009), no. 5, 1531-1548.

[2] P. Erdős, A. Ginzburg, A. Ziv, Theorem in Additive Number Theory, *Bull. Res. Council Israel* **10F** (1961), 41–43.

[3] W. Gao, Addition theorems for finite abelian groups, *J. Number Theory* **53** (1995), no.2, 241-246.

[4] W. Gao and A. Geroldinger, Zero-sum problems in finite abelian groups: A survey, *Expositiones Mathematicae* **24** (2006), no. 4, 337-369.

[5] A. Geroldinger and I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory*, Birkhäuser (2009), Basel.

[6] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics: A series of Monographs and Textbooks **278** (2006), Chapman & Hall, an imprint of Taylor & Francis Group, Boca Raton, FL.

[7] D. J. Grynkiewicz, On a partition analog of the Cauchy-Davenport theorem, *Acta Math. Hungar.* **107** (2005), no. 1–2, 161–174.

[8] D. J. Grynkiewicz, On a conjecture of Hamidoune for subsequence sums, *Integers* **5** (2005), no. 2, A7 (electronic).

[9] D. J. Grynkiewicz, A Step Beyond Kemperman's Structure Theorem, *Mathematika* **55** (2009), 67–114.

[10] D. J. Grynkiewicz, E. Marchan and O. Ordaz, Representation of finite abelian group elements by subsequence sums, *J. Théor. Nombres Bordeaux* **21** (2009), no. 3, 559–587.

[11] D. J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics **30**, Springer (2013), Switzerland.

[12] Y. O. Hamidoune, O. Serra, and G. Zémor, On the critical pair theory in abelian groups: beyond Chowla's theorem, *Combinatorica* 28 (2008), no. 4, 441-467.

[13] Y. O. Hamidoune, Hyper-Atoms Applied to the Critical Pair Theory, to appear in *Combinatorica*.

[14] J. H. B. Kemperman, On small sumsets in an abelian group, *Acta Math.* **103** (1960), 63-88.

[15] M. Kneser, Ein Satz uber abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, *Math. Z.* **61** (1955), 429–434.

[16] H. B. Mann, Two addition theorems, *J. Combinatorial Theory* **3** (1967), 233-235.

[17] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer (1996), Harrisonburg, VA.

[18] J. E. Olson, An addition theorem for finite abelian groups, *J. Number Theory* **9** (1977), no. 1, 63-70.

[19] O. Ordaz, A. Philipp, I. Santos, and W. A. Schmid, On the Olson and the strong Davenport constants, *J. Théor. Nombres Bordeaux* 23 (2011), no. 3, 715-750.

[20] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge University Press (2006), Cambridge.

E-mail address: diambri@hotmail.com

Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA