Iterated Sumsets and Olson's Generalization of the Erdős-Ginzburg-Ziv Theorem

David J. Grynkiewicz [1]

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

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 $|A+B| \leq |A|+|B|$. Utilizing these results, we provide a precise structural description of all finite subsets $A \subseteq G$ with $|nA| \leq (|A|+1)n-3$ when $n \geq 3$ (also when G is infinite), in which case many of the pathological possibilities from the case $n = 2$ vanish, particularly for large $n \geq \exp(G)-1$. 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 $|S| \geq 2|G|-1$ 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 $H \leq G$. We show that the much weaker hypothesis $|S| \geq |G|+\exp(G)$ 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 $|S|$.

Keywords: zero-sum, sumset, subsequence sum, subsum, Partition Theorem, Kneser's Theorem, Kemperman Structure Theorem, n-fold sumset, iterated sumset, Olson, complete sequence, Erdős-Ginzburg-Ziv Theorem

1 Extended 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 $m_1 \mid \ldots \mid m_r = \exp(G)$. Given subsets A, $B \subseteq G$, we define their sumset

$$A + B = \{a + b : \ a \in A, b \in B\}.$$

Let S be a sequence of terms from G, let $n \geq 0$ be an integer, and let $X \subseteq G$ be a subset. Then

- $|S|$ denotes the length of S,
- $\mathsf{h}(S)$ denotes the maximum multiplicity of a term in S, and
- $\Sigma_n(S)$ denotes all elements $g \in G$ which can be expressed as the sum of an n-term subsequence of S.

A classical result in Combinatorial Number Theory, helping spawn the study of zero-sum sequences, is the Erdős-Ginzburg-Ziv Theorem [1] [3] [8].

Theorem 1.1 (Erdős-Ginzburg-Ziv Theorem) *Let G be a finite abelian group and let S be a sequence of terms from G of length $|S| \geq 2|G| - 1$. Then $0 \in \Sigma_{|G|}(S)$.*

When $G = \mathbb{Z}/n\mathbb{Z}$ is cyclic, a sequence consisting of entirely of 0's and 1's has a $|G|$-term zero-sum if and only if there is a $|G|$-term subsequence which is monochromatic (consisting entirely of 0's or entirely of 1's). In this way, the Erdős-Ginzburg-Ziv Theorem can be viewed as an algebraic generalization of the Pigeonhole Principle. Naturally, a sequence S having only one distinct term can be arbitrarily long and yet $\Sigma_{|G|}(S) = \{0\}$, so it is not possible to replace 0 with an arbitrary group element $g \in G$. More generally, if all terms from S come from a coset $\alpha + H$ of a proper subgroup $H \leq G$, then $\Sigma_{|G|}(S) = H$, and so only elements from H can be represented as subsequence sums. Nonetheless, an old result of Olson [9], generalizing the case for cyclic groups of prime order completed by Mann [7], shows this to be the only restriction to extending the Erdős-Ginzburg-Ziv Theorem from sequences with sum 0 to those with arbitrary sum $g \in G$.

Theorem 1.2 *[9] Let G be a finite abelian group and let S 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 $\Sigma_{|G|}(S) = G$.*

[1] Email: `diambri@hotmail.com`

The bound $2|G|-1$ was later improved to $|G|+\mathsf{D}(G)-1$ by Gao [2], where $\mathsf{D}(G) \leq |G|$ is the Davenport constant, which is the minimal integer ℓ such that any sequence of terms from G with length ℓ must contain a nontrivial zero-sum subsequence. This was further improved to $|G| + \mathsf{d}^*(G)$ [5], where $\mathsf{d}^*(G) \leq \mathsf{D}(G) - 1$ is the basic lower bound for the Davenport constant: $\mathsf{d}^*(G) = \sum_{i=1}^{r}(m_i - 1)$. Neither of these bounds is tight in general, only being tight for a limited class of particular groups G.

We observe that the hypothesis that S have at least $|G/H|-1$ terms lying outside any coset $\alpha + H$ reduces, in the case H is trivial, to the statement that the maximum multiplicity of S is at most $\mathsf{h}(S) \leq |S| - |G| + 1$. By strengthening this hypothesis by one, so instead assuming $\mathsf{h}(S) \leq |S| - |G|$, we are able to obtain optimal values for how long $|S|$ must be to represent all elements of G.

Theorem 1.3 *Let G be a finite abelian group, let $n \geq 1$, and let S be a sequence of terms from G with $|S| = |G| + n$ and $\mathsf{h}(S) \leq |S| - |G|$. 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. *$n \geq \exp(G)$, or*
2. *$n \geq \exp(G) - 1$ and $G \cong H \oplus C_{\exp(G)}$ with $|H|$ or $\exp(G)$ prime, or*
3. *$n \geq \frac{|G|}{p} - 1$ and G is cyclic, where p is the smallest prime divisor of $|G|$, or*
4. *$n \geq 1$ and either $\exp(G) \leq 3$, or $|G| < 12$, or $\exp(G) = 4$ with $|G| = 16$.*

The Kemperman Structure Theorem characterizes all subsets $A, B \subseteq G$ satisfying $|A+B| < |A| + |B|$ [6] [3] and has been extended to cover the case when $|A+B| \leq |A|+|B|$ [4]. It is one of the few results giving a precise inverse result for sumsets in an *arbitrary* abelian group. As a main step for proving Theorem 1.3, we provide a precise structural description of all finite subsets $A \subseteq G$ with $|nA| \leq (|A|+1)n - 3$ when $n \geq 3$ (also when G is infinite), where

$$nA = \underbrace{A + \ldots + A}_{n}$$

denotes the n-fold iterated sumset.

For the descriptions below, we say X is *H-periodic* if $H + X = X$, where $H \leq G$. This means X is a union of H-cosets. A set X is *aperiodic* if it is not H-periodic for any nontrivial subgroup $H \leq G$. Equivalently, the stabilizer group

$$\mathsf{H}(X) = \{g \in G : \; g + X = X\} \leq G$$

is trivial. We say that $X = X_1 \cup X_0$ is an *H-coset decomposition* if X_1 and X_0 are each subsets of distinct H-cosets. We say $X = X_0 \cup \ldots \cup X_r$ is an *H-coset progression decomposition* if each A_i is contained in an H-coset with the sequence of H-cosets $A_0, A_1, \ldots, A_r$ forming an arithmetic progression modulo H. We say that $X = X_1 \cup X_0$ is an *H-quasi-periodic decomposition* if X_1 is H-periodic and X_0 is a non-empty subset of an H-coset.

In the case $|A| = 3$, there are numerous additional possibilities, with the structure given according to the following result.

Theorem 1.4 *Let G be an abelian group, let $A \subseteq G$ be a subset with $\langle A - A\rangle = G$ and $|A| = 3$, and let $n \geq 3$ be an integer. Suppose*

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

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 $\langle A_1 - A_1\rangle = H \leq G$ 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 $\langle A_0 - A_0\rangle = H \leq G$ 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.

The general description is then the following.

Theorem 1.5 *Let G be a nontrivial abelian group, let $A \subseteq G$ be a finite subset with $\langle A - A\rangle = G$, and let $n \geq 3$ 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 Theorem 1.4. Otherwise, one of the following must hold.

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

(ii) *There exist subgroups* $K_1, K_2, K \leq G$, *with* $K_1 \cong K_2 \cong \mathbb{Z}/2\mathbb{Z}$ *and* $K = K_1 \oplus K_2$, *and* K*-coset progression decomposition* $A = A_1 \cup \ldots \cup A_r$ *such that* A_1 *is a* K_1*-coset,* A_r *is a* K_2*-coset, and all other* A_i *are* K*-cosets, 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* $K = \langle A_0 - A_0\rangle \leq H$, *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* $|nA| = |A|n-1 = |G|-1$.

While the above structural description is quite involved, it simplifies greatly by imposing some mild restrictions. For instance, when $|A| > |G|/n$, we obtain the following as a corollary.

Corollary 1.6 *Let* G *be a finite abelian group, let* $A \subseteq G$ *be a nonempty subset with* $\langle A - A\rangle = G$, *let* $n \geq 1$ *be an integer, let* $K = \mathsf{H}(nA)$ *and suppose* $n|A| > |G|$.

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

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

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

References

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

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

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

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

[5] 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.

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

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

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

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