A generalization of Kneser's Addition Theorem

Matt DeVos, Luis Goddyn[*] and Bojan Mohar[†‡]
Department of Mathematics
Simon Fraser University
Burnaby, B.C. V5A 1S6
email: [mdevos,goddyn,mohar]@sfu.ca

September 8, 2006

Abstract

Let $\mathbf{A} = (A_1, \ldots, A_m)$ be a sequence of finite subsets from an additive abelian group G. Let $\Sigma^\ell(\mathbf{A})$ denote the set of all group elements representable as a sum of ℓ elements from distinct members of $\mathbf{A}$, and set $H = stab(\Sigma^\ell(\mathbf{A})) = \{g \in G : g + \Sigma^\ell(\mathbf{A}) = \Sigma^\ell(\mathbf{A})\}$. Our main theorem is the following lower bound:

$$|\Sigma^\ell(\mathbf{A})| \geq |H| \Big(1 - \ell + \sum_{Q \in G/H} \min\big\{\ell, \#\{1 \leq i \leq m : A_i \cap Q \neq \emptyset\}\big\} \Big).$$

In the special case when $m = \ell = 2$, this is equivalent to Kneser's addition theorem, and indeed we obtain a new proof of this result. The special case when every A_i has size one is a new result concerning subsequence sums which extends some recent work of Bollobás-Leader, Hamidoune, Hamidoune-Ordaz-Ortuño, and Grynkiewicz, and resolves a recent conjecture of Gao.

[*]Supported by a Canada NSERC Discovery Grant
[†]Supported in part by the Research Grant P1–0297 and by the CRC program.
[‡]On leave from: IMFM & FMF, Department of Mathematics, University of Ljubljana, Ljubljana, Slovenia.

1 Introduction

Throughout we shall assume that G is a (possibly infinite) additive abelian group. Let $A, B \subseteq G$ and $g \in G$. We define the *sumset* $A + B = \{a + b : a \in A \text{ and } b \in B\}$ and we define $g + A = A + g = \{g\} + A$. Any set of the form $g + A$ is called a *shift* of A. We define the *stabilizer* of A to be $stab(A) = \{g \in G \mid g + A = A\}$. Note that $stab(A) \leq G$. The starting point for our present subject is the following classical result of Cauchy [3] and Davenport [4] (see also [14]), which gives a lower bound on $|A+B|$ for groups of prime order. Here we let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Theorem 1.1 (Cauchy-Davenport) *If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then $|A + B| \geq \min\{p, |A| + |B| - 1\}$.*

This theorem was generalized by Kneser [13] to all abelian groups as follows.

Theorem 1.2 (Kneser) *If $A, B \subseteq G$ are finite and nonempty and $H = stab(A + B)$, then $|A + B| \geq |A + H| + |B + H| - |H|$.*

A rich subject closely related to sumsets is the study of subsequence sums. Given a sequence $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ of elements of G, we define

$$\Sigma^\ell(\mathbf{a}) = \{a_{i_1} + a_{i_2} + \cdots + a_{i_\ell} : 1 \leq i_1 < i_2 < \cdots < i_\ell \leq m\}.$$

So $\Sigma^\ell(\mathbf{a})$ is the set of all group elements representable as a sum of length ℓ of a subsequence of $\mathbf{a}$. The following pretty theorem of Erdős, Ginzburg, and Ziv [5] brought great interest to this topic.

Theorem 1.3 (Erdős, Ginzburg, Ziv) *If $|G| = \ell$ and $\mathbf{a} = (a_1, a_2, \ldots, a_{2\ell-1})$ is a sequence in G, then $0 \in \Sigma^\ell(\mathbf{a})$.*

Recently, this theorem has been generalized in a number of different directions. Here we shall introduce a few of these generalizations which we will later show to be consequences of our main result. The first one is a theorem of Hamidoune [10] which itself generalized an earlier theorem of Bollobás and Leader [2] (as we shall discuss, this result is also implied by a theorem of Grynkiewicz [7]). The second one is a very recent conjecture of Gao [6]. The third one is a theorem of Grynkiewicz [8] which generalized earlier results of Hamidoune

[9], and Hamidoune, Ordaz, and Ortuño [11]. The fourth is an important result of Gao [6] concerning the Davenport constant. As indicated earlier, all these statements may be viewed as generalizations of Theorem 1.3.

Theorem 1.4 (Hamidoune) *Let* $\mathbf{a} = (a_1, \ldots, a_m)$ *be a sequence in* G *and assume* $\ell \leq m \leq 2\ell - 1$. *Then one of the following holds:*

(i) $|\Sigma^\ell(\mathbf{a})| \geq m - \ell + 1$.

(ii) *There exists* $1 \leq i \leq m$ *so that* $\ell a_i \in \Sigma^\ell(\mathbf{a})$.

Conjecture 1.5 (Gao) *Let* $k, \ell \in \mathbb{N}$, *let* p *be the smallest prime divisor of* ℓ, *and let* $\mathbf{a} = (a_1, a_2, \ldots, a_{\ell+k})$ *be a sequence in* $\mathbb{Z}_\ell$. *If* $k \geq \frac{\ell}{p} - 1$ *and no element appears more than* k *times in* $\mathbf{a}$, *then* $0 \in \Sigma^\ell(\mathbf{a})$.

Gao proved his conjecture when $\ell = p^n$ for a positive integer n [**?**], and it was recently proved by Cao in the special case when $\ell = p^n q^{n'}$ where p, q are prime and n, n' are positive integers [**?**].

Theorem 1.6 (Grynkiewicz) *Let* G *be an abelian group of order* ℓ *and let* $\mathbf{a} = (a_1, \ldots, a_m)$ *be a sequence in* G *with* $m > \ell$. *If* $\mathbf{a}$ *contains at least* k *distinct terms and no group element appears more than* $\ell - k + 2$ *times in* $\mathbf{a}$, *then one of the following holds*

(i) $|\Sigma^\ell(\mathbf{a})| \geq m - \ell + k - 1$.

(ii) *There exists a nontrivial subgroup* $H \leq stab(\Sigma^\ell(\mathbf{a}))$ *with* $H \subseteq \Sigma^\ell(\mathbf{a})$. *Further, there is an* H*-coset* Q *which contains all but at most* $\min\{\frac{m-\ell+k-2}{|H|}, [G : H] - 2\}$ *terms of* $\mathbf{a}$.

Before mentioning the next generalization of the Erdős, Ginzburg, Ziv theorem, we will require a little notation. For any finite abelian group G, we define the *Davenport constant* of G, denoted $s(G)$, to be the minimum $k \in \mathbb{N}$ so that every sequence of elements of G with length $\geq k$ has a nontrivial subsequence which sums to 0. Similarly, we define $s'(G)$ to be the minimum $\ell \in \mathbb{N}$ so that every sequence of elements of G with length $\geq \ell$ has a subsequence of length $|G|$ which sums to 0. It is an easy exercise to show that $s(G) \leq |G|$ for every G. In light of this, the following theorem of Gao [**?**] (previously conjectured by Caro [**?**]) may also be viewed as a generalization of Theorem 1.3.

Theorem 1.7 (Gao) $s'(G) = s(G) + |G| - 1$ *for every finite abelian group* G.

2 Our results

The principal subject matter for this paper is sequences of sets. Extending our earlier definitions, let $\mathbf{A} = (A_1, A_2, \ldots, A_m)$ be a sequence of finite subsets of G and define

$$\Sigma^\ell(\mathbf{A}) = \{a_{i_1} + \cdots + a_{i_\ell} : 1 \leq i_1 < \cdots < i_\ell \leq m \text{ and } a_{i_j} \in A_{i_j} \text{ for every } 1 \leq j \leq \ell\}$$

The following theorem is our main result.

Theorem 2.1 *Let $\mathbf{A} = (A_1, \ldots, A_m)$ be a sequence of finite subsets of G and let $H = stab(\Sigma^k(\mathbf{A}))$. If $\Sigma^k(\mathbf{A})$ is nonempty, then*

$$|\Sigma^k(\mathbf{A})| \geq |H| \Big(1 - k + \sum_{Q \in G/H} \min \big\{ k \mid \#\{1 \leq i \leq m : A_i \cap Q \neq \emptyset\} \big\} \Big).$$

In the special case when $m = k = 2$, our result is equivalent to Kneser's Theorem, and our argument gives a new proof of this theorem. In fact, this new proof was found by the first author somewhat earlier than this more general argument, and will be published elsewhere.

In the special case when every A_i has size one, our theorem specializes to the following new bound on subsequence sums.

Corollary 2.2 *If $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ is a sequence of elements of G and $H = stab(\Sigma^\ell(\mathbf{a}))$, then*

$$|\Sigma^\ell(\mathbf{a})| \geq |H| \Big(1 - \ell + \sum_{Q \in G/H} \min \big\{ \ell, \#\{1 \leq i \leq m : a_i \in Q\} \big\} \Big).$$

If $\mathbf{a} = (a_1, \ldots, a_m)$ and $\ell \leq m$, then it follows immediately that $\Sigma^{m-\ell}(\mathbf{a}) = (\sum_{i=1}^m a_i) - \Sigma^\ell(\mathbf{a})$. Thus, the sets $\Sigma^{m-\ell}(\mathbf{a})$ and $\Sigma^\ell(\mathbf{a})$ are shifts of one another, and in particular, these two sets have the same size and the same stabilizer. As such, our theorem may be applied in two different ways, and generally these two bounds will be different.

Corollary 2.2 is quite close to a result which follows from Grynkiewicz's "partition analogue of the Cauchy-Davenport Theorem." This theorem of Grynkiewicz concerns a refinement of a partition of a sequence into sets, and we shall not state it in full, but a key consequence of it is as follows. If $\mathbf{a} = (a_1, \ldots, a_m)$ is a sequence in G, then there exists a subset $C \subseteq \Sigma^\ell(\mathbf{a})$ and a subgroup $H \leq stab(C)$ for which the inequality in Corollary 2.2 holds with the left hand side replaced by $|C|$.

Both the theorem of Grynkiewicz mentioned above and our Corollary 2.2 imply Theorem 1.4. To derive it from Corollary 2.2, note that if there is an H-coset $Q \in G/H$ so that $\#\{1 \le i \le m : a_i \in Q\} \ge \ell$, then it follows that $\ell a_i \in \Sigma^\ell(\mathbf{a})$ for some $1 \le i \le m$. Otherwise, our bound immediately implies $|\Sigma^\ell(\mathbf{a})| \ge m - \ell + 1$.

The following corollary of our result resolves Gao's conjecture.

Corollary 2.3 *Let G be a finite group and let p be the smallest prime divisor of $|G|$. Let $k, \ell \in \mathbb{N}$, let $\mathbf{a} = (a_1, \ldots, a_{\ell+k})$ be a sequence in G and set $H = stab(\Sigma^\ell(\mathbf{a}))$. If $k \ge |G|/p - 1$ and no element of G appears more than k times in $\mathbf{a}$, then one of the following holds.*

(i) $|\Sigma^\ell(\mathbf{a})| \ge \ell + 1$.

(ii) $H \neq \{0\}$ *and there exists $Q \in G/H$ so that* $\#\{1 \le i \le m : a_i \notin Q\} \ge \ell$.

To see that this corollary follows from Corollary 2.2, note that if $H = \{0\}$, our bound implies $|\Sigma^\ell(\mathbf{a})| = |\Sigma^k(\mathbf{a})| \ge \ell + 1$, so (i) holds. Otherwise, our bound (applied to $\Sigma^\ell(\mathbf{a})$) shows that either (ii) holds, or $|\Sigma^\ell(\mathbf{a})| \ge |H|(1 + k) \ge |H| \cdot |G|/p \ge |G|$. In the latter case, $\Sigma^\ell(\mathbf{a}) = G$, which again implies (ii).

Corollary 2.2 can also be used to derive Theorem 1.6. Indeed, it implies the following stronger result where the dependence on the order of the group has been removed.

Corollary 2.4 *Let $m, k, \ell \in \mathbb{N}$ with $\ell < m$, let $\mathbf{a} = (a_1, \ldots, a_m)$ be a sequence in G with $H = stab(\Sigma^\ell(\mathbf{a}))$. If $\mathbf{a}$ contains at least k distinct terms and no element of G appears more than $\ell - k + 2$ times, then one of the following holds.*

(i) $|\Sigma^\ell(\mathbf{a})| \ge \min\{\ell + 1, m - \ell + k - 1\}$.

(ii) $H \neq \{0\}$ *and there exists $Q \in G/H$ so that* $\#\{1 \le i \le m : a_i \notin Q\} \ge \ell$.

The proof of this corollary requires a bit of careful counting and will be given in the third section of the paper. Finally, Corollary 2.2 can be used to obtain a new proof of Gao's Theorem (Theorem 1.7). This consequence will also be proved in the third section.

Despite what may be the apparent generality of our result, it is actually a very special (but presumably the most important) case of a fascinating conjecture of Schrijver and Seymour. These authors consider a much more general type of sumset problem, where they introduce an underlying geometry in the form of a matroid. To state it precisely, we will need a little notation. If M is a matroid on E, and $w : E \to G$ is a map, we define $w(M) = \{\sum_{b \in B} w(b) : B \text{ is a base of } M\}$. Schrijver and Seymour [17] made the following conjecture for general abelian groups.

Conjecture 2.5 (Schrijver-Seymour) *If $H = stab(w(M))$, then*

$$|w(M)| \geq |H|\Big(1 - rk(M) + \sum_{Q \in G/H} rk(w^{-1}(Q))\Big).$$

The special case of this conjecture when the underlying matroid is uniform is precisely Corollary 2.2. Our main theorem is equivalent to the Schrijver-Seymour conjecture for matroids obtained from uniform matroids by adding parallel elements.

Schrijver and Seymour [17] proved their conjecture in the special case when $|G|$ is prime. In this paper, they state "we have convinced ourselves that it is true when $|G|$ is a power of a prime, or the product of two primes. But this last, if it is correct, will appear in a later paper." Unfortunately, this later paper was never written. In the final section of our paper, we will prove this conjecture in the special case when $|G|$ is a product of two distinct primes, and when $G \cong \mathbb{Z}_{p^n}$ for a prime p. These arguments are based on the original method of Schrijver and Seymour.

3 Main Theorem

The goal of this section is to prove our main theorem. In fact, for the purpose of our inductive arguments, we will prove a slightly stronger statement. We continue with some further notation.

If $H \leq G$ and $\ell \in \mathbb{N}$, we call a map $\mu : G/H \to \mathbb{N}$ an *H-pattern* of *weight* ℓ if $\sum_{Q \in G/H} \mu(Q) = \ell$. If $\mathbf{A} = (A_1, A_2, \ldots, A_m)$ is a sequence of finite subsets of G and μ is an H-pattern of weight ℓ, we call a sequence $(b_1, b_2, \ldots, b_\ell)$ *μ-feasible* (in $\mathbf{A}$) if there exist $1 \leq i_1 < i_2 < \cdots < i_\ell \leq m$ which satisfy the following properties:

- $b_j \in A_{i_j}$ for every $1 \leq j \leq \ell$.
- $\mu(Q) = |\{j \in \{1, \ldots, \ell\} : b_j \in Q\}|$ for every $Q \in G/H$.

Expanding our earlier notation, we now make the following definition.

$$\Sigma^{\mu}(\mathbf{A}) = \{b_1 + \cdots + b_\ell : (b_1, b_2, \ldots, b_\ell) \text{ is } \mu\text{-feasible in } \mathbf{A}\}.$$

For every $\ell \in \mathbb{N}$ and $H \leq G$ we define

$$\Xi^{\ell}_{H}(\mathbf{A}) = \sum_{Q \in G/H} \min\{\ell, \#\{1 \leq i \leq m : A_i \cap Q \neq \emptyset\}\}.$$

Theorem 3.1 *Let* $\mathbf{A} = (A_1, \ldots, A_m)$ *be a sequence of finite subsets of* G*, let* $K \leq G$ *and let* $\mu : G/K \to \mathbb{N}$ *be a* K*-pattern of weight* ℓ*. If* $\Sigma^{\mu}(\mathbf{A}) \neq \emptyset$ *and* $stab(\Sigma^{\mu}(\mathbf{A})) = J$*, then*

$$|\Sigma^{\mu}(\mathbf{A})| \geq |J|(\Xi^{\ell}_{J}(\mathbf{A}) - \ell + 1) - |K|(\Xi^{\ell}_{K}(\mathbf{A}) - \ell).$$

Before we prove Theorem 3.1, let us show that it implies our main theorem. To see this, let $\mathbf{A} = (A_1, \ldots, A_m)$ be a sequence of subsets of G and let ℓ be a positive integer. Now set $K = G$ and define $\mu : G/K \to \mathbb{N}$ by the rule $\mu(G) = \ell$. Then $\Sigma^{\ell}(\mathbf{A}) = \Sigma^{\mu}(\mathbf{A})$ and $\Xi^{\ell}_{K}(\mathbf{A}) = \ell$. Now it is obvious that the bound in Theorem 3.1 implies Theorem 2.1. In particular, Theorem 3.1 implies Kneser's Theorem. In our proof, we will argue by considering a counterexample which is in some sense minimal, and we will use the fact that our main theorem (and hence Kneser's Theorem) hold for all smaller examples.

Proof: We shall assume (for a contradiction) that the theorem is false and choose a counterexample $\mathbf{A} = (A_1, \ldots, A_m)$ so that

(i) $|\Sigma^{\mu}(\mathbf{A})|$ is minimum.

(ii) $\sum_{i=1}^{m} |A_i|$ is minimum (subject to (i)).

(iii) $\sum_{i=1}^{m} |A_i|^2$ is maximum (subject to (i),(ii)).

(iv) m is minimum (subject to (i), (ii), (iii)).

It follows from (iv) that A_i is nonempty for every $1 \leq i \leq m$. Next we will show that our assumptions imply $J = \{0\}$. For each coset $Q \in G/K$, choose $q(Q) \in G$ such that $Q = K + q(Q)$. Then

$$\Sigma^{\mu}(\mathbf{A}) \subseteq K + \Big(\sum_{Q \in G/K} \mu(Q)q(Q) \Big).$$

This shows that $\Sigma^{\mu}(\mathbf{A})$ is included in some K-coset, and hence $J \leq K$. Suppose (for a contradiction) that $J \neq \{0\}$ and let $\phi : G \to G/J$ be the canonical homomorphism. Let $A_\phi = (\phi(A_1), \ldots, \phi(A_m))$, let $K_\phi = \phi(K)$ and let $\mu_\phi : (G/J)/K_\phi \to \mathbb{N}$ be given by the rule

$\mu_\phi(Q) = \mu(\cup Q)$ for every $Q \in (G/J)/K_\phi$. Then $\Sigma^{\mu_\phi}(A_\phi) = \phi(\Sigma^\mu(\mathbf{A}))$ has trivial stabilizer, so by the minimality of our counterexample we have

$$\begin{aligned}
|\Sigma^\mu(\mathbf{A})| &= |J| \cdot |\Sigma^{\mu_\phi}(A_\phi)| \\
&\geq |J| \left(\Xi^\ell_{\{0\}}(A_\phi) - \ell + 1 - |K_\phi|(\Xi^\ell_{K_\phi}(A_\phi) - \ell) \right) \\
&= |J|(\Xi^\ell_J(\mathbf{A}) - \ell + 1) - |K|(\Xi^\ell_K(\mathbf{A}) - \ell).
\end{aligned}$$

This contradiction implies that $J = \{0\}$ as desired.

The next step in our proof is to handle one rather special case, when $\ell = m$, and there exists $1 \leq j \leq m$ so that $|A_j + K| > |K|$. Although the induction we will apply here is different than that used in the general case, the remainder of the argument is similar (but much easier in this special case). The idea is to iteratively build nested subsets of $\Sigma^\mu(\mathbf{A})$ with increasing size and decreasing stabilizers. We will call the subsets produced in this process "convergents" – a term borrowed from approximations to continued fractions. Define a set $C \subseteq \Sigma^\mu(\mathbf{A})$ with $H = \mathit{stab}(C)$ to be a *convergent* if it satisfies the following property

$$|C| \geq |H|(\Xi^\ell_H(\mathbf{A}) - \ell + 1) - |K|(\Xi^\ell_K(\mathbf{A}) - \ell).$$

As in the general argument, we will first show (using an inductive application of our theorem) that a convergent exists. Choose a μ-feasible sequence $(a_1, \ldots, a_m)$ and for every $1 \leq i \leq m$ let $A'_i = A_i \cap (a_i + K)$. Then set $C_0 = \sum_{i=1}^m A'_i$ and $H_0 = \mathit{stab}(C_0)$. Note that $|A'_j| < |A_j|$, so we can apply our theorem to the sequence $A'_1, A'_2, \ldots, A'_m$ to find that $|C_0| \geq \sum_{i=1}^m |A'_i + H_0| - (m-1)|H_0|$. Now we have

$$\begin{aligned}
|K|(\Xi^m_K(\mathbf{A}) - m) &= \sum_{i=1}^m |(A_i \setminus A'_i) + K| \\
&\geq \sum_{i=1}^m |(A_i \setminus A'_i) + H_0| \\
&= \sum_{i=1}^m |H_0|(\Xi^m_{H_0}(\mathbf{A})) - \sum_{i=1}^m |A'_i + H_0|.
\end{aligned}$$

Thus, $|C_0| \geq \sum_{i=1}^m |A'_i + H_0| - (m-1)|H_0| \geq |H_0|(1 - m + \Xi^m_{H_0}(\mathbf{A})) - |K|(\Xi^m_K(\mathbf{A}) - m)$. It follows from this that C_0 is a convergent, and we may now choose a convergent C with $H = \mathit{stab}(C)$ minimal. If $H = \{0\}$, then since $\Sigma^\mu(\mathbf{A}) \supseteq C$ our proof is complete. Thus, we may assume that H is nontrivial.

Since $J = \{0\}$, we may choose a μ-feasible sequence $(b_1, b_2, \ldots, b_m)$ for which $\sum_{i=1}^{m} b_i + H \not\subseteq \Sigma^{\mu}(\mathbf{A})$. Let $\nu : G/H \to \mathbb{N}$ be the H-pattern of weight $\ell = m$ given by the rule $\nu(R) = \#\{1 \leq i \leq m : b_i + H = R\}$. Note that $\Sigma^{\nu}(\mathbf{A})$ is included in an H-coset and is disjoint from C. Now set $D = \Sigma^{\nu}(\mathbf{A})$ and $H' = stab(D)$, and note that $stab(C \cup D) = H'$ since D is included in some H-coset. By the assumption that C is a convergent and an application of our bound to $D = \Sigma^{\nu}(\mathbf{A})$ we have

$$\begin{aligned} |C \cup D| &= |C| + |D| \\ &\geq |H|(\Xi^{\ell}_{H}(\mathbf{A}) - \ell + 1) - |K|(\Xi^{\ell}_{K}(\mathbf{A}) - \ell) \\ &\quad + |H'|(\Xi^{\ell}_{H'}(\mathbf{A}) - \ell + 1) - |H|(\Xi^{\ell}_{H}(\mathbf{A}) - \ell) \\ &\geq |H'|(\Xi^{\ell}_{H}(\mathbf{A}) - \ell + 1) - |K|(\Xi^{\ell}_{K}(\mathbf{A}) - \ell). \end{aligned}$$

It follows that $C \cup D$ is a convergent with stabilizer $H' < H$ contradicting our assumption. This completes the proof of this special case.

For the general argument, we shall arrange (after some adjusting) that our first two sets A_1 and A_2 satisfy $A_1 \setminus A_2 \neq \emptyset$ and $A_2 \setminus A_1 \neq \emptyset$. Further, we will arrange that the sequence $\mathbf{A}' = (A_1 \cap A_2, A_1 \cup A_2, A_3, \ldots, A_m)$ satisfies $\Sigma^{\mu}(\mathbf{A}') \neq \emptyset$. It will then follow from (iii) of our choice of $\mathbf{A}$ that the theorem applies (nontrivially) to $\mathbf{A}'$. This application will be our initial building block (giving us the existence of a convergent). The preparation for this intersection-union operation is slightly different depending on whether $\ell = m$ or $\ell < m$ so we shall consider these two cases separately.

First suppose that $\ell < m$. For every $1 \leq i \leq m$ let $\mathbf{A}^i = (A_1, \ldots, A_{i-1}, A_{i+1}, \ldots, A_m)$. By possibly rearranging our sequence, we may assume that A_1 has minimum size over all sets A_i for which $\Sigma^{\mu}(\mathbf{A}^i) \neq \emptyset$. If $A_1 \subseteq A_i$ for every $1 \leq i \leq m$, then $\Sigma^{\mu}(\mathbf{A}) = \Sigma^{\mu}(\mathbf{A}^i)$, $\Xi^{\ell}_{K}(\mathbf{A}) = \Xi^{\ell}_{K}(\mathbf{A}^i)$, and $\Xi^{\ell}_{\{0\}}(\mathbf{A}) = \Xi^{\ell}_{\{0\}}(\mathbf{A}^i)$ so $\mathbf{A}^i$ contradicts the choice of $\mathbf{A}$ for (ii). Thus, by rearranging, we may assume that $A_1 \not\subseteq A_2$. If $A_2 \subset A_1$, then $\Sigma^{\mu}(\mathbf{A}^2) \supseteq \Sigma^{\mu}(\mathbf{A}^1) \neq \emptyset$. Hence, the minimality of A_1 implies that $A_2 \not\subseteq A_1$. Thus, we have arranged that $A_1 \setminus A_2 \neq \emptyset$, $A_2 \setminus A_1 \neq \emptyset$, and defining $\mathbf{A}' = (A_1 \cap A_2, A_1 \cup A_2, A_3, \ldots, A_m)$, we have $\Sigma^{\mu}(\mathbf{A}') \supseteq \Sigma^{\mu}(\mathbf{A}^1) \neq \emptyset$ as desired.

Next suppose that $\ell = m$. Since we have already handled the case when $|A_i + K| > |K|$ for some $1 \leq i \leq m$ we may further assume that every A_i is included in a K-coset. Thus $\Sigma^{\mu}(\mathbf{A}) = \Sigma^{m}(\mathbf{A}) = \sum_{i=1}^{m} A_i$ and we may assume that $K = G$ since this has no effect on the bound. By possibly rearranging our sets, we may assume that $|A_1| \leq |A_2|$. If $A_1 = \{a\}$ for some $a \in G$ then the result follows by applying the theorem to the sequence $(A_2, A_3, \dots, A_m)$. Otherwise, choose distinct $a, a' \in A_1$. Note that $stab(A_2) \subseteq stab(\Sigma^m(\mathbf{A})) = \{0\}$. Therefore, $a' - a \notin stab(A_2)$, so there exists $b \in A_2$ so that $b + a' - a \notin A_2$. Now replace A_2 by $A_2 - b + a$ (and use the notation A_2 for this shifted set henceforth). This has the effect of shifting $\Sigma^m(\mathbf{A})$, but does not affect the size of this set or its stabilizer. Clearly, $a' \in A_1 \setminus A_2$ and since $|A_1| \leq |A_2|$, also $A_2 \setminus A_1 \neq \emptyset$. We have now arranged that both $A_1 \setminus A_2$ and $A_2 \setminus A_1$ are nonempty, so setting $\mathbf{A}' = (A_1 \cap A_2, A_1 \cup A_2, A_3, \dots, A_m)$ we have $\Sigma^\mu(\mathbf{A}') \neq \emptyset$.

Let us observe that in all cases the new sequence $\mathbf{A}'$ satisfies $\Sigma^\mu(\mathbf{A}') \subseteq \Sigma^\mu(\mathbf{A})$, where the latter subset sum is considered with the possible adjustment of A_2 in the step above.

Now we will *redefine* our notion of convergent. We define a set C to be a *convergent* if $\Sigma^\mu(\mathbf{A}') \subseteq C \subseteq \Sigma^\mu(\mathbf{A})$ and if setting $H = stab(C)$ we have

$$|C| \geq |H|(\Xi^\ell_H(\mathbf{A}') - \ell + 1) - |K|(\Xi^\ell_K(\mathbf{A}) - \ell).$$

Next we will show that $C_0 = \Sigma^\mu(\mathbf{A}') \neq \emptyset$ is a convergent. To see this, let $H_0 = stab(C_0)$. Because of the minimality assumption (i) or (iii), we can apply the theorem to $\mathbf{A}'$ and get the following:

$$\begin{aligned} |C_0| &= |\Sigma^\mu(\mathbf{A}')| \\ &\geq |H_0|(\Xi^\ell_{H_0}(\mathbf{A}') - \ell + 1) - |K|(\Xi^\ell_K(\mathbf{A}') - \ell) \\ &\geq |H_0|(\Xi^\ell_{H_0}(\mathbf{A}') - \ell + 1) - |K|(\Xi^\ell_K(\mathbf{A}) - \ell). \end{aligned}$$

Thus, C_0 is a convergent, and we may now choose a convergent C with stabilizer H so that H is minimal. If $H = \emptyset$, then we have

$$\begin{aligned} |\Sigma^\mu(\mathbf{A})| &\geq |C| \\ &\geq \Xi^\ell_{\{0\}}(\mathbf{A}') - \ell + 1 - |K|(\Xi_K(\mathbf{A}) - \ell) \\ &= \Xi^\ell_{\{0\}}(\mathbf{A}) - \ell + 1 - |K|(\Xi_K(\mathbf{A}) - \ell). \end{aligned}$$

This contradiction implies that $H \neq \emptyset$.

Our plan is to construct three new sets D^1, D^2, and D^{12} all of which are disjoint from C and properly included in a particular H-coset. We will then derive a contradiction under the assumption that none of $C \cup D^1$, $C \cup D^2$, $C \cup D^{12}$ is a convergent (with stabilizer strictly smaller than H). We now set about defining our three sets.

Since $\Sigma^\mu(\mathbf{A})$ has trivial stabilizer and $stab(C) = H \neq \emptyset$ we may choose a μ-feasible sequence $(b_1, b_2, \ldots, b_\ell)$ so that $\sum_{j=1}^{\ell} b_j + H \not\subseteq \Sigma^\mu(\mathbf{A})$. Note that $b_1 \in A_1$ and $b_2 \in A_2$ because $\Sigma^\mu(\mathbf{A}') \subseteq C$ and $stab(C) = H$. Also, the H-coset $\sum_{j=1}^{\ell} b_j + H$ is disjoint from C. Let $\nu : G/H \to \mathbb{N}$ be the H-pattern of weight ℓ given by the rule $\nu(R) = \#\{j \in \{1, \ldots, \ell\} : b_j + H = R\}$. Note that $\Sigma^\nu(\mathbf{A})$ is included in an H-coset which is disjoint from C. In fact, all three of our sets D_1, D_2, D_{12} will be included in $\Sigma^\nu(\mathbf{A})$ and will henceforth be all disjoint from C.

Let $\mathbf{A}'' = (A_3, A_4, \ldots, A_m)$ and let ν'' be the H-pattern of weight $\ell - 2$ given by the rule $\nu''(R) = \#\{j \in \{3, \ldots, \ell\} : b_j + H = R\}$. Next, for $i = 1, 2$ set $A_1^i = A_1 \cap (b_i + H)$ and set $A_2^i = A_2 \cap (b_{3-i} + H)$ (here the reader should note a deliberate "crossing" of our indices). Note that $b_1 \in A_1^1$ and $b_2 \in A_2^1$ so $A_1^1 \neq \emptyset \neq A_2^1$. Then set $B = (A_1^1 + A_2^1) \cup (A_1^2 + A_2^2)$. Next we define the first of our three sets and name its stabilizer as follows

$$D^{12} = B + \Sigma^{\nu''}(\mathbf{A}''), \qquad H^{12} = stab(D^{12}).$$

It is immediate from our construction that $D^{12} \subseteq \Sigma^\nu(\mathbf{A})$ so it is disjoint from C. Now for $i = 1, 2$ we define the set D^i and name its stabilizer as follows

$$D^i = A_1^i + A_2^i + \Sigma^{\nu''}(\mathbf{A}'') + H^{12}, \qquad H^i = stab(D^i).$$

For $i = 1, 2$ we have that $D^i \subseteq D^{12} \subseteq \Sigma^\nu(\mathbf{A})$ is disjoint from C. Note that $D^1 \neq \emptyset$, and that $H^{12} \leq H^1 < H$. If $D^2 \neq \emptyset$, then we also have $H^{12} \leq H^2 < H$. The next equation holds for $i = 1$ and also holds for $i = 2$ if $D^2 \neq \emptyset$. It follows from the assumption that C is a convergent, but $C \cup D^i$ (which has stabilizer $H^i < H$, since D^i is a proper subset of some H-coset) is not.

$$\begin{aligned} |D^i| &= |C \cup D^i| - |C| \\ &< |H^i|(\Xi_{H^i}^{\ell}(\mathbf{A}') - \ell + 1) - |H|(\Xi_H^{\ell}(\mathbf{A}') - \ell + 1) \end{aligned} \tag{1}$$

On the other hand, D^i is defined by a sumset to which we may apply our theorem by part (i) of the choice of our counterexample. In the inequality below, we will apply our result in the form of Kneser's theorem to deduce line 3 from line 2, and we apply it again to deduce line 4 from line 3. In line 3, we have the sequence $\mathbf{A}''' = (A_3 + H^i, A_4 + H^i, \ldots, A_m + H^i)$ of length $\ell - 2$. Let us observe that $stab(\Sigma^{\nu''}(\mathbf{A}''')) = H^i$ and $\Xi_{H^i}^{\ell-2}(\mathbf{A}''') \geq \Xi_{H^i}^{\ell-2}(\mathbf{A}'')$. For the equality in line 1, observe that $H^{12} \leq H^i = stab(D^i)$. The following inequality holds for $i = 1$ and for $i = 2$ if $D^2 \neq \emptyset$.

$$\begin{aligned} |D^i| &= |A_1^i + A_2^i + \Sigma^{\nu''}(\mathbf{A}'') + H^{12}| = |A_1^i + A_2^i + \Sigma^{\nu''}(\mathbf{A}'') + H^i| \\ &= |(A_1^i + H^i) + (A_2^i + H^i) + (\Sigma^{\nu''}(\mathbf{A}'') + H^i)| \\ &\geq |A_1^i + H^i| + |A_2^i + H^i| + |\Sigma^{\nu''}(\mathbf{A}''')| - 2|H^i| \\ &\geq |A_1^i + H^i| + |A_2^i + H^i| + |H^i|(\Xi_{H^i}^{\ell-2}(\mathbf{A}'') - \ell + 1) - |H|(\Xi_H^{\ell-2}(\mathbf{A}'') - \ell + 2) \quad (2) \end{aligned}$$

To help manage our Ξ-terms, we next make a claim which we will use repeatedly.

Claim: Let $H' \leq H$ and define X' and Y' as follows

$$\begin{aligned} X' &= (b_1 + H) \setminus ((A_1^1 \cup A_2^2) + H'), \\ Y' &= (b_2 + H) \setminus ((A_1^2 \cup A_2^1) + H'). \end{aligned}$$

Then

$$|H|(\Xi_H^{\ell}(\mathbf{A}') - \Xi_H^{\ell-2}(\mathbf{A}'')) - |H'|(\Xi_{H'}^{\ell}(\mathbf{A}') - \Xi_{H'}^{\ell-2}(\mathbf{A}'')) \geq |X' \cup Y'|.$$

Proof of Claim: The contribution of an H-coset R to $|H|(\Xi_H^{\ell}(\mathbf{A}') - \Xi_H^{\ell-2}(\mathbf{A}''))$ (which must be either 0, $|H|$, or $2|H|$) is always at least the contribution of the H'-cosets contained in R to $|H'|(\Xi_{H'}^{\ell}(\mathbf{A}') - \Xi_{H'}^{\ell-2}(\mathbf{A}''))$. Next we consider the coset $b_1 + H$. If this coset has nontrivial intersection with $A_1 \cap A_2$ or has nontrivial intersection with $> \ell - 2$ members of $\mathbf{A}''$, then $\Sigma^{\nu}(\mathbf{A}') \neq \emptyset$. However, this contradicts the assumption that $\Sigma^{\nu}(\mathbf{A})$ is disjoint from C since $\Sigma^{\nu}(\mathbf{A}) \supseteq \Sigma^{\nu}(\mathbf{A}') \subseteq \Sigma^{\mu}(\mathbf{A}') \subseteq C$. It follows that the contribution of $b_1 + H$ to $|H|(\Xi_H^{\ell}(\mathbf{A}') - \Xi_H^{\ell-2}(\mathbf{A}''))$ is exactly $|H|$. By the same argument, the contribution of the H'-cosets contained in $b_1 + H$ to $|H'|(\Xi_{H'}^{\ell}(\mathbf{A}') - \Xi_{H'}^{\ell-2}(\mathbf{A}''))$ is exactly $|(A_1^1 \cup A_2^2) + H'|$. Since $(A_1^1 \cup A_2^2) + H' = (A_1^1 \cup A_2^2) + H = (A_1 \cup A_2) + (b_1 + H)$, the difference between these two quantities is at least $|X'|$. By a similar argument, the contribution of the coset $b_2 + H$ to $|H|(\Xi_H^{\ell}(\mathbf{A}') - \Xi_H^{\ell-2}(\mathbf{A}''))$ is exactly $|H|$, and the contribution of the H'-cosets contained in $b_2 + H$ to $|H'|(\Xi_{H'}^{\ell}(\mathbf{A}') - \Xi_{H'}^{\ell-2}(\mathbf{A}''))$ is exactly $|(A_1^2 \cup A_2^1) + H'|$, and the difference is at least $|Y'|$. Note that it is possible that $b_1 + H = b_2 + H$. Whether this holds or not, our claim is an immediate consequence of the above conclusions.

For $i = 1, 2$ set $X^i = (b_1 + H) \setminus ((A_1^1 \cup A_2^2) + H^i)$ and $Y^i = (b_2 + H) \setminus ((A_1^2 \cup A_2^1) + H^i)$. Then combining the above claim with equations (1) and (2) gives the following equation, which holds for $i = 1$ and for $i = 2$ if $D^2 \neq \emptyset$.

$$|H| > |A_1^i + H^i| + |A_2^i + H^i| + |X^i \cup Y^i| \tag{3}$$

If $A_2^2 = \emptyset$, then $|X^1| = |H| - |A_1^1 + H^1|$ and we have a contradiction to the above equation for $i = 1$. Thus $A_2^2 \neq \emptyset$. We get a similar contradiction (by considering Y^1) under the assumption that $A_2^1 = \emptyset$. It follows that $D^2 \neq \emptyset$ and equation (3) holds for $i = 1, 2$. If $b_1 + H = b_2 + H$, then $A_2^1 = A_2^2$ so $|X^1| = |(b_1 + H) \setminus ((A_1^1 \cup A_2^1) + H^1)| \geq |H| - |A_1^1 + H^1| - |A_2^1 + H^1|$, but again this contradicts equation (3) for $i = 1$. Thus $b_1 + H \neq b_2 + H$. Our next equation follows from equation (3) and the observation that $|H|$, $|A_1^i + H^i|$, and $|A_2^i + H^i|$ are all multiples of $|H^i|$. It holds for $i = 1, 2$:

$$\begin{aligned} |H| &\geq |A_1^i + H^i| + |A_2^i + H^i| + |H^i| \\ &\geq |A_1^i + H^{12}| + |A_2^i + H^{12}| + |H^i| \end{aligned} \tag{4}$$

Let $X^{12} = (b_1+H)\setminus((A_1^1+H^{12})\cup(A_2^2+H^{12}))$, let $Y^{12} = (b_2+H)\setminus((A_1^2+H^{12})\cup(A_2^1+H^{12}))$, and note that X^{12} and Y^{12} are disjoint. Since $C \cup D^{12}$ is not a convergent, we have

$$\begin{aligned} |D^{12}| &= |C \cup D^{12}| - |C| \\ &< |H^{12}|(\Xi^{\ell}_{H^{12}}(\mathbf{A}') - \ell + 1) - |H|(\Xi^{\ell}_{H}(\mathbf{A}') - \ell + 1). \end{aligned}$$

On the other hand D^{12} is defined by a sumset to which we can apply our theorem by the minimality condition (i) of our choice of counterexample. This gives us the next equation (which holds for $i = 1, 2$). Here line 3 follows from line 2 by using Kneser's theorem. Line 4 follows from line 3 and the observation that the stabilizer of $A_1^i + (A_2^i + H^{12})$ contains H^{12} and is contained in H^i. To get the last line, we again apply Kneser's theorem (as a special case of ours) and again apply our theorem inductively for the sumset $\Sigma^{\nu''}$.

$$\begin{aligned} |D^{12}| &= |B + \Sigma^{\nu''}(\mathbf{A}'') + H^{12}| \\ &= |(B + H^{12}) + (\Sigma^{\nu''}(\mathbf{A}'') + H^{12})| \\ &\geq |B + H^{12}| + |\Sigma^{\nu''}(\mathbf{A}'') + H^{12}| - |H^{12}| \\ &\geq |(A_1^i + H^{12}) + (A_2^i + H^{12})| + |\Sigma^{\nu''}(A_3 + H^{12}, A_4 + H^{12}, \ldots, A_m + H^{12})| - |H^{12}| \\ &\geq |A_1^i + H^{12}| + |A_2^i + H^{12}| - |H^i| + |H^{12}|(\Xi^{\ell-2}_{H^{12}}(\mathbf{A}'') - \ell + 2) - |H|(\Xi^{\ell-2}_{H}(\mathbf{A}'') - \ell + 2) \end{aligned}$$

Combining these two equations and applying the claim with $H' = H^{12}$ (in which case $X' = X^{12}$ and $Y' = Y^{12}$) gives us

$$|H| \geq |A_1^i + H^{12}| + |A_2^i + H^{12}| - |H^i| + |H^{12}| + |X^{12}| + |Y^{12}| \tag{5}$$

Summing the four inequalites obtained by taking equations 4 and 5 for $i = 1, 2$ and then dividing by two yields

$$2|H| > |A_1^1 + H^{12}| + |A_1^2 + H^{12}| + |A_2^1 + H^{12}| + |A_2^2 + H^{12}| + |X^{12}| + |Y^{12}| + |H^{12}|.$$

However, $b_1 + H = X^{12} \cup (A_1^1 + H^{12}) \cup (A_2^2 + H^{12})$ and $b_2 + H = Y^{12} \cup (A_1^2 + H^{12}) \cup (A_2^1 + H^{12})$. This yields the final contradiction and completes the proof. $\square$

4 Two Applications

The goal for this section is to derive Corollary 2.4, and then Gao's theorem from Corollary 2.2. Before proceeding, we require one added bit of notation. If $\mathbf{a} = (a_1, \ldots, a_m)$ is a sequence in G and $S \subseteq G$, we let $\rho_S(\mathbf{a}) = \#\{1 \leq i \leq m : a_i \in S\}$. Similarly, if $g \in G$ we define $\rho_g(\mathbf{a}) = \rho_{\{g\}}(\mathbf{a})$. For convenience we restate both Corollary 2.2 and Corollary 2.4 below with this new notation.

Corollary 2.2 *If $\mathbf{a} = (a_1, \ldots, a_m)$ is a sequence of elements of G and $H = stab(\Sigma^k(\mathbf{a}))$, then*

$$|\Sigma^k(\mathbf{a})| \geq |H| \Big(1 - k + \sum_{Q \in G/H} \min\big\{k, \rho_Q(\mathbf{a})\big\} \Big).$$

Corollary 2.4 *Let $m, k, \ell \in \mathbb{N}$ with $\ell < m$, let $\mathbf{a} = (a_1, \ldots, a_m)$ be a sequence in G with $H = stab(\Sigma^\ell(\mathbf{a}))$. If $\mathbf{a}$ contains at least k distinct terms and $\rho_g(\mathbf{a}) \leq \ell - k + 2$ for every $g \in G$, then one of the following holds:*

(i) $|\Sigma^\ell(\mathbf{a})| \geq \min\{\ell + 1, m - \ell + k - 1\}$.

(ii) *$H \neq \{0\}$ and there exists $Q \in G/H$ so that $\rho_Q(\mathbf{a}) \geq \ell$.*

Proof: We shall assume that neither (i) nor (ii) holds and derive a contradiction. Since the sets $\Sigma^\ell(\mathbf{a})$ and $\Sigma^{m-\ell}(\mathbf{a})$ have the same size and the same stabilizer (one is just a shift of the other), we may apply Corollary 2.2 both for $\Sigma^\ell(\mathbf{a})$ and $\Sigma^{m-\ell}(\mathbf{a})$.

Set $h = |H|$ and set $t = \#\{Q \in G/H : \rho_Q(\mathbf{a}) \geq m - \ell\}$. If $t = 0$, then Corollary 2.2 (with $m - \ell$ in terms of k) shows that $|\Sigma^\ell(\mathbf{a})| = |\Sigma^{m-\ell}(\mathbf{a})| \geq h(1 - (m - \ell) + m) = h(1 + \ell)$, so (i) holds. Thus $t \geq 1$.

Suppose that $H = \{0\}$. If $t = 1$, then since $\rho_g(\mathbf{a}) \leq \ell - k + 2$ for every $g \in G$, we must have $\sum_{g\in G} \min\{m-\ell, \rho_g(\mathbf{a})\} \geq m - ((\ell - k + 2) - (m - \ell)) = 2m - 2\ell + k - 2$. If $t \geq 2$, then since $\mathbf{a}$ contains at least k distinct terms, we have $\sum_{g\in G} \min\{m-\ell, \rho_g(\mathbf{a})\} \geq t(m-\ell)+k-t = t(m-\ell-1)+k \geq 2m-2\ell+k-2$. Since this inequality holds for all possible values of t, Corollary 2.2 shows that $|\Sigma^{m-\ell}(\mathbf{a})| \geq 1-(m-\ell)+(2m-2\ell+k-2) = m-\ell+k-1$ and conclusion (i) holds.

Thus $H \neq \{0\}$, i.e., $h > 1$. Assuming that (i) and (ii) do not hold, Corollary 2.2 gives

$$\begin{aligned} m - \ell + k &> |\Sigma^{\ell}(\mathbf{a})| \\ &\geq |H|\Big(1 - \ell + \sum_{Q\in G/H} \rho_Q(\mathbf{a})\Big) \\ &= h(m - \ell + 1) \end{aligned}$$

so we have

$$k - h > (h-1)(m-\ell). \tag{6}$$

Note that this implies in particular that $k \geq h + 2$. Since $t \geq 1$, we may choose $R \in G/H$ so that $\rho_R(\mathbf{a}) \geq m - \ell$. Then our bound gives

$$\begin{aligned} |\Sigma^{m-\ell}(\mathbf{a})| &\geq h\Big(1 - m + \ell + \sum_{Q\in G/H} \min\{m-\ell, \rho_Q(\mathbf{a})\}\Big) \\ &= h\Big(1 + \sum_{Q\in (G/H)\setminus\{R\}} \min\{m-\ell, \rho_Q(\mathbf{a})\}\Big). \end{aligned} \tag{7}$$

First suppose that $m - \ell \geq h$. Then the summation term in the right hand side of equation (7) must be at least the number of distinct elements in $G \setminus R$ which appear at least once in $\mathbf{a}$. Thus, in this case we have $|\Sigma^{m-\ell}(\mathbf{a})| \geq h(1 + k - |R|) \geq h(1 + k - h)$. Combining this with Equation (6) and the assumption that (i) does not hold we have

$$\begin{aligned} (k-h)/(h-1) &> m - \ell \\ &> |\Sigma^{\ell}(\mathbf{a})| - k = |\Sigma^{m-\ell}(\mathbf{a})| - k \\ &\geq h(1 + k - h) - k \\ &= (k-h)(h-1). \end{aligned}$$

However, this is contradictory since $k \geq h + 2$ and $h \geq 2$.

Thus we may now assume $m - \ell < h$. Again let us consider the summation term in the right hand side of equation (7). There are at least $k - |R| = k - h$ distinct elements in $G \setminus R$

which appear in $\mathbf{a}$. If $Q \in G/H \setminus \{R\}$ contains s distinct elements of G which appear in $\mathbf{a}$, then the contribution of this coset to the Σ term will be at least $\min\{s, m-\ell\} \geq \frac{m-\ell}{h}s$. Thus, the summation term in the right hand side of (7) is at least $\frac{m-\ell}{h}(k-h)$. Combining this with the assumption that (i) does not hold we have

$$\begin{aligned}(m-\ell)+(k-h) &> |\Sigma^{m-\ell}(\mathbf{a})| - h \\ &\geq (k-h)(m-\ell).\end{aligned}$$

Since we have already observed that $k \geq h+2$, the above equation implies that $m = \ell + 1$ (recall that $m > \ell$ by assumption). But then $|\Sigma^1(\mathbf{a})| \geq k$ since $\mathbf{a}$ contains k distinct terms, so we find $|\Sigma^\ell(\mathbf{a})| = |\Sigma^1(\mathbf{a})| \geq k = m - \ell + k - 1$ and conclusion (i) holds. This completes the proof. $\square$

Proof of Theorem 1.7: To see that $s'(G) \geq s(G) + |G| - 1$, choose a sequence $\mathbf{a}$ of length $s(G) - 1$ without a nontrivial subsequence which sums to 0 and append $|G| - 1$ copies of 0 to $\mathbf{a}$. This new sequence demonstrates $s'(G) \geq s(G) + |G| - 1$.

Next we shall prove $s'(G) \leq s(G) + |G| - 1$ by induction on $|G|$. Let $m = s(G) + |G| - 1$ and let $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ be a sequence in G. We need to show that $0 \in \Sigma^{|G|}(\mathbf{a})$. Set $H = stab(\Sigma^{|G|}(\mathbf{a}))$. If $H \neq \{0\}$, then let $\phi : G \to G/H$ be the canonical homomorphism and consider the sequence $a_\phi = (\phi(a_1), \phi(a_2), \ldots, \phi(a_m))$. Since $s(G/H) \leq s(G)$, we may apply our theorem inductively to get a subsequence of length $[G : H]$ and sum zero in G/H. After removing this subsequence, we apply the theorem again to get another such sequence. After $|H|$ repetitions, we have $|H|$ disjoint subsequences of a_ϕ each with length $[G : H]$ and sum equal to zero in G/H. Combining the corresponding subsequences of $\mathbf{a}$ gives a subsequence of length $|G|$ whose sum s is in H. Since $H = stab(\Sigma^{|G|}(\mathbf{a}))$, we have $\Sigma^{|G|}(\mathbf{a}) - s = \Sigma^{|G|}(\mathbf{a})$. However, $0 \in \Sigma^{|G|}(\mathbf{a}) - s$, so $0 \in \Sigma^{|G|}(\mathbf{a})$. Thus, we may assume that $H = \{0\}$.

If $\rho_g(\mathbf{a}) < s(G)$ for every $g \in G$ then by Corollary 2.2 we have $|\Sigma^{s(G)-1}(\mathbf{a})| \geq 2 - s(G) + \sum_{g\in G} \min\{s(G) - 1, \rho_g(\mathbf{a})\} \geq |G| + 1$ which is contradictory. It follows that there exists $g \in G$ so that $\rho_g(\mathbf{a}) \geq s(G)$. By replacing $\mathbf{a}$ by $(a_1 - g, a_2 - g, \ldots, a_m - g)$ we do not affect the set $\Sigma^{|G|}(\mathbf{a})$ but may now assume that $\rho_0(\mathbf{a}) \geq s(G)$. By rearranging our sequence, we may further assume that $a_{|G|+1}, a_{|G|+2}, \ldots a_{|G|+s(G)-1}$ are all 0. Now, by the definition of the Davenport constant, we may repeatedly choose disjoint subsequences of $(a_1, a_2, \ldots, a_{|G|})$ each of which has zero sum, so that the number of leftover elements is at most $s(G) - 1$.

By concatenating these sequences, and then adding an appropriate number of zero terms a_i with $i > |G|$, we obtain a subsequence of length $|G|$ with zero sum, as required. □

5 Matroids

The goal of this section is to prove two special cases of Conjecture 2.5. Fix an abelian group G, a matroid M on E with rank function rk, and let $\mathcal{B}(M)$ denote the set of bases of M. Departing from the original treatment of Schrijver and Seymour, we let W be a weight function which assigns each element $e \in E$ a nonempty set $W(e) \subseteq G$. For every $S \subseteq G$ let $E_S = \{e \in E : S \cap W(e) \neq \emptyset\}$ and if $g \in G$ let $E_g = E_{\{g\}}$. Now we set

$$W(M) = \bigcup_{B \in \mathcal{B}(M)} \sum_{b \in B} W(b).$$

Theorem 5.1 *Let p, q be distinct primes and assume that $G \cong \mathbb{Z}_{p^n}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$. If $H = stab(W(M))$, then*

$$|W(M)| \geq |H| \Big(1 - rk(M) + \sum_{Q \in G/H} rk(E_Q) \Big).$$

Proof: We proceed by induction on $rk(M) + |E|$. If $rk(M) \leq 1$, then the result is trivial, so we may assume $rk(M) \geq 2$. By deleting loops and applying induction, we may also assume that M has no loops. Similarly, if $e, f \in E$ are parallel, then the result follows by replacing $W(e)$ by $W(e) \cup W(f)$, deleting f, and then applying induction (this operation has no effect on either the set of weights or on our bounds). Thus, we may assume that M has no loops and no parallel elements.

Consider an element $e \in E$. By possibly replacing $W(e)$ with a superset, we may assume that for every $g \in G \setminus W(e)$, the weight function W' obtained from W by the adjustment $W'(e) = W(e) \cup \{g\}$ satisfies $W'(M) \neq W(M)$. If $g \in G$ and E_g spans e, then replacing $W(e)$ by $W(e) \cup \{g\}$ does not change the set $W(M)$, since any group element formed by taking weight g from $W(e)$ under a basis $B \in \mathcal{B}(M)$ can also be produced by replacing e with another element $f \notin B$ whose set $W(f)$ contained g (for the basis $B - e + f$). By repeating this process, we may assume that $W(e) = \{g \in G : E_g \text{ spans } e\}$ for every $e \in E$.

Let M/e denote the matroid obtained from M by contracting e. Now for every $e \in E$ consider the following set and its stabilizer:

$$A_e = W(e) + W(M/e), \qquad H_e = stab(A_e).$$

It is easy to see that A_e is precisely the set of weights of bases which contain e. It follows from our maximality assumption that $H_e = stab(W(e))$ and $H \leq H_e$. Suppose there exists $e \in E$ with $H_e = H$. Then since $A_e = W(e) + W(M/e)$ it follows that both $W(e)$ and $W(M/e)$ have stabilizer equal to H. So by applying induction to $W(M/e)$ and Kneser's theorem (Theorem 1.2) we have:

$$\begin{aligned}
|W(M)| &\geq |A_e| \\
&= |W(e) + W(M/e)| \\
&\geq |W(e)| + |W(M/e)| - |H| \\
&\geq |H|\Big(\#\{Q \in G/H :\ E_Q \text{ spans } e\ \} + 1 - rk(M/e) + \sum_{Q \in G/H} rk_{M/e}(E_Q)\Big) - |H| \\
&= |H|\Big(1 - rk(M) + \sum_{Q \in G/H} rk_M(E_Q)\Big).
\end{aligned}$$

This proves the theorem in the case when $H_e = H$.

Thus, we may assume that $H_e \neq H$ for every $e \in E$. If $G \cong \mathbb{Z}_{p^n}$, then the subgroups of G are nested, and thus there is a unique minimal nontrivial subgroup K of G (which has order p). Then $K \leq H_e = stab(W(e))$ for every $e \in E$ so $K \leq stab(W(M))$ which is contradictory.

If $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$, then let K_1, K_2 be the two distinct proper nontrivial subgroups of G. If $\cap_{e \in E} H_e$ is nontrivial, then we have a contradiction to $stab(W(M)) = \{0\}$ as before. Otherwise we may choose $e, f \in E$ so that $H_e = K_1$ and $H_f = K_2$. But then, since e, f are not parallel we may choose a base B with $e, f \in B$ and we find that $W(M) \supseteq \sum_{b \in B} W(b)$ contains a shift of $W(e) + W(f)$. However, the latter one is the whole group G. This final contradiction completes the proof.

***COMMENT: In the last two paragraphs we have assumed that $stab(W(M)) = \{0\}$. Why we can do that has to be added somewhere at the beginning of the proof. $\square$

References

[1] A. Bialostocki and P. Dierker, On the Erdős-Ginzburg-Ziv Theorem and the Ramsey numbers for stars and matchings, Discrete Math. 110 (1992), 1–8.

[2] B. Bollobás and I. Leader, The number of k-sums modulo k, J. Number Theory 78 (1999), 27–35.

[3] A.L. Cauchy, Recherches sur les nombres, J. École polytech. 9 (1813), 99–116.

[4] H. Davenport, On the addition of residue classes, J. London Math. Soc. 10 (1935), 30–32.

[5] P. Erdős, A. Ginzburg, and A. Ziv, Theorem in the additive number theory, Bull. Res. Coucil 10F (1961), 41–43.

[6] W. Gao, A combinatorial problem on finite abelian groups, J. Number Theory 58 (1996), 100–103.

[7] D. Grynkiewicz, On a partition analog of the Cauchy-Davenport Theorem, Acta Math. Hungar. 107 (2005), 167–181.

[8] D. Grynkiewicz, On a conjecture of Hamidoune for subsequence sums, Integers: Electr. J. Comb. Number Theory 5 (2) (2005) #A07.

[9] Y. O. Hamidoune, On weighted sums in abelian groups, Discrete Math. 162 (1996), 127–132.

[10] Y. O. Hamidoune, Subsequence sums, Combin. Probab. Comput. 12 (2003), 413–425.

[11] Y. O. Hamidoune, O. Ordaz, and A. Ortuño, On a combinatorial theorem of Erdős, Ginzburg, and Ziv, Combin. Probab. Comput. 7 (1998), 403–412.

[12] J. H. B. Kempermann, On small sumsets in an abelian group, Acta Math. 103 (1960), 63–88.

[13] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, Math. Z. 58 (1953), 459–484.

[14] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics 165, Springer-Verlag, New York, 1996.

[15] J. E. Olson, On a combinatorial problem of Erdős, Ginzburg, and Ziv, J. Number Theory 8 (1976), 52–57.

[16] J. E. Olson, An addition theorem for finite abelian groups, J. Number Theory 9 (1977), 63–70.

[17] A. Schrijver and P. D. Seymour, Spanning trees of different weights, DIMACS Series in Discrete Math. and Theoret. Comp. Sci., Vol 1 (1990), 281–288.