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

October 17, 2008

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 terms of $\mathbf{A}$, and set $H = \mathrm{stab}(\Sigma^\ell(\mathbf{A})) = \{g \in G : g + \Sigma^\ell(\mathbf{A}) = \Sigma^\ell(\mathbf{A})\}$. Our main theorem is the following lower bound:

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

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, Grynkiewicz, and Gao, and resolves two recent conjectures of Gao, Thangadurai, and Zhuang.

*Supported by a Canada NSERC Discovery Grant.

†Supported in part by Slovenian Research Grant P1–0297 and by Canadian NSERC Discovery Grant 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* $A + B = \{a + b : a \in A, b \in B\}$ 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 $\mathrm{stab}(A) = \{g \in G \mid g + A = A\}$. Note that $\mathrm{stab}(A) \leq G$. The starting point for our subject is the following classical result of Cauchy [5] and Davenport [6] (see also [17]), 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 [16] to all abelian groups as follows.

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

Our principal subject matter is sequences of sets. If $\mathbf{A} = (A_1, A_2, \ldots, A_m)$ is a sequence of finite subsets of G, and $\ell \leq m$, we define

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

So $\Sigma^\ell(\mathbf{A})$ is the set of all elements which can be represented as a sum of ℓ terms from distinct members of $\mathbf{A}$. The following is our main result.

Theorem 1.3 *Let $\mathbf{A} = (A_1, \ldots, A_m)$ be a sequence of finite subsets of G, let $\ell \leq m$, and let $H = \mathrm{stab}(\Sigma^\ell(\mathbf{A}))$. If $\Sigma^\ell(\mathbf{A})$ is nonempty, then*

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

In the special case when $m = \ell = 2$, 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.

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

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

So $\Sigma^\ell(\mathbf{a})$ is the set of all group elements representable as a sum of an ℓ-term subsequence of $\mathbf{a}$. The study of subsequence sums features a wide expanse of interconnected results. In the remainder of the introduction, we shall take a tour of some of these theorems, and then move on to some related results on graphs and matroids. Our tour begins with the following classic theorem of Erdős, Ginzburg, and Ziv [7].

Theorem 1.4 (Erdős, Ginzburg, Ziv) *If $|G| = \ell$ and $\mathbf{a} = (a_1, a_2, \ldots, a_{2\ell-1})$ is a sequence of elements from G, then $0 \in \Sigma^\ell(\mathbf{a})$.*

This theorem has recently been generalized in a number of different directions, some of which we will discuss shortly. However, first let us point out that the special case of our theorem when each A_i has size one gives a natural lower bound for subsequence sums. This is stated below as Corollary 1.5. This corollary may be used to derive Theorem 1.4, so we may view this as another generalization of Erdős-Ginzburg-Ziv. However, as we shall show, this corollary is strong enough to imply several other generalizations of it. See Figure 1.

Corollary 1.5 *If $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ is a sequence of elements of G, $\ell \le m$, and $H = \mathrm{stab}(\Sigma^\ell(\mathbf{a}))$, then*

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

Note that if $\mathbf{a} = (a_1, \ldots, a_m)$ and $\ell \le m$, 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 to a given sequence $\mathbf{a}$, and generally these two bounds will be different.

Let us remark that Corollary 1.5 is a slight strengthening of a result in [12] which follows from Grynkiewicz's "partition analogue of the Cauchy-Davenport Theorem" (hereafter called *Grynkiewicz's partition 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 of elements from G, then there exists a subset $C \subseteq \Sigma^\ell(\mathbf{a})$ and a subgroup $H \leq \mathrm{stab}(C)$ for which inequality (1) holds with the left hand side replaced by $|C|$.

Now let us commence with our tour with some generalizations of the Erdős-Ginzburg-Ziv Theorem. In this theorem, the authors study only sequences of length $2|G| - 1$ and subsequences of length $|G|$. Perhaps the most obvious attempt at generalization would be to consider what happens when we consider different length sequences and subsequences (although it is not obvious how the conclusion should be modified). Indeed, Bollobás and Leader [3] found a nice generalization of Theorem 1.4 by considering subsequences of length $|G|$ from an arbitrary sequence. Hamidoune [14] further generalized this with the following theorem, where subsequences of arbitrary length are considered. Here $\mathbb{N}$ denotes the set of nonnegative integers.

Theorem 1.6 (Hamidoune) *Let* $\mathbf{a} = (a_1, \ldots, a_m)$ *be a sequence of elements from* G*, let* $\ell \in \mathbb{N}$*, and assume* $1 \leq \ell \leq m \leq 2\ell - 1$*. Then one of the following holds:*

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

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

Both Grynkiewicz's partition theorem and our Corollary 1.5 imply Theorem 1.6. To derive Theorem 1.6 from Corollary 1.5, note that if there is an H-coset $Q \in G/H$ so that $|\{1 \leq i \leq m : a_i \in Q\}| \geq \ell$, then $\Sigma^\ell(\mathbf{a})$ contains the H-coset ℓQ, so $\ell a_i \in \Sigma^\ell(\mathbf{a})$ for every $1 \leq i \leq m$ with $a_i \in Q$. Otherwise, our bound immediately implies $|\Sigma^\ell(\mathbf{a})| \geq m - \ell + 1$.

Perhaps the most obvious way to limit the size of $\Sigma^\ell(\mathbf{a})$ is to choose $\mathbf{a}$ so that all or almost all of its entries are the same. Accordingly, a number of authors have studied the effect of limiting the maximum multiplicity

$$\rho(\mathbf{a}) = \max_{g \in G} |\{i \in \{1, \ldots, m\} : a_i = g\}|$$

among elements in $\mathbf{a}$. Next we state a two-part conjecture due to Gao, Thangadurai, and Zhuang (Conjectures 1 and 2 in [11]) on this theme. We use the notation $\Sigma(\mathbf{a}) = \cup_{i=0}^m \Sigma^i(\mathbf{a})$.

Conjecture 1.7 (Gao, Thangadurai, Zhuang) *Let $\ell > 1$ be an integer, let p be the smallest prime divisor of ℓ, and let $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ be a sequence of elements from $\mathbb{Z}_\ell$. If $m \geq \ell + \frac{\ell}{p} - 1$ and $\rho(\mathbf{a}) \leq m - \ell$, then both of the following hold.*

(1) $0 \in \Sigma^\ell(\mathbf{a})$.

(2) *If 0 appears exactly $m - \ell$ times in $\mathbf{a}$, then $\Sigma^{m-\ell}(\mathbf{a}) = \Sigma(\mathbf{a})$.*

The proposers prove this conjecture in the case where ℓ is a prime power. More recently, Cao [4] verified part (1) when ℓ is the product of two prime powers, and Gao [10] proved a slightly weaker form of part (1) for general ℓ. Conjecture 1.7 follows from our next corollary (proved in Section 3).

Corollary 1.8 *Let G be a nontrivial finite abelian group and let p be the smallest prime divisor of $|G|$. Let $\mathbf{a} = (a_1, \ldots, a_m)$ be a sequence of elements from G, let $\ell \leq m$ and set $H = \mathrm{stab}(\Sigma^\ell(\mathbf{a}))$. If $m \geq \ell + \frac{\ell}{p} - 1$ and $\rho(\mathbf{a}) \leq m - \ell$, then one of the following holds.*

(i) $|\Sigma^\ell(\mathbf{a})| \geq \ell$.

(ii) *$H \neq \{0\}$ and there exists $Q \in G/H$ so that $|\{i \in \{1, \ldots, m\} : a_i \in Q\}| > \ell$.*

Let us pause to show that the above corollary implies Conjecture 1.7. With the assumptions of Conjecture 1.7, both parts (1) and (2) follow from Corollary 1.8 if conclusion (i) holds (as then $\Sigma^\ell(\mathbf{a}) = \Sigma^{m-\ell}(\mathbf{a}) = \mathbb{Z}_\ell$), so we may assume that (ii) holds. Then $H = \ell Q \subseteq \Sigma^\ell(\mathbf{a})$ and part (1) follows. For part (2), note that since 0 appears $m - \ell$ times, Q must equal H, so the image of $\mathbf{a}$ under the canonical quotient mapping from $\mathbb{Z}_\ell$ to $\mathbb{Z}_\ell/H$, call it $\mathbf{b}$, is a sequence with fewer than $m - \ell$ nonzero terms. Thus $\Sigma^{m-\ell}(\mathbf{b}) = \Sigma(\mathbf{b})$. It follows from this that $\Sigma^{m-\ell}(\mathbf{a}) = \Sigma(\mathbf{a})$.

Bialostocki and Dierker [2] generalized the Erdős-Ginzburg-Ziv theorem by studying sequences of length $2|G| - 2$ and characterizing those without zero-sum subsequences of length $|G|$. They prove that (for nontrivial groups), such sequences can only occur when G is cyclic, and the sequence contains exactly two group elements, each occurring exactly $|G| - 1$ times. Stated another way, every sequence of length $2|G| - 2$ with at least three distinct terms must have a zero-sum subsequence of length $|G|$. Indeed, the assumption that a sequence has many distinct terms also tends to increase the number of distinct subsequence sums, and a number of authors have studied this phenomenon. Next we state a theorem of Grynkiewicz [13] which exploits a distinctness assumption. This theorem resolved a conjecture of Hamidoune [14], and extended some earlier results of Hamidoune [14], and Hamidoune, Ordaz, and Ortuño [15], in addition to the Bialostocki-Dierker theorem mentioned above.

Theorem 1.9 (Grynkiewicz) *Let G be an abelian group of order ℓ and let $\mathbf{a} = (a_1, \ldots, a_m)$ be a sequence of elements from G with $m > \ell$. If $\mathbf{a}$ contains at least k distinct terms and $\rho(\mathbf{a}) \leq \ell - k + 2$, then one of the following holds.*

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

(ii) *There is a nontrivial subgroup $H \leq \mathrm{stab}(\Sigma^\ell(\mathbf{a}))$ with $H \subseteq \Sigma^\ell(\mathbf{a})$, there is an H-coset Q which contains all but at most t terms of $\mathbf{a}$ where $t \leq \min\{\lfloor \frac{m-\ell+k-2}{|H|} \rfloor - 1, [G : H] - 2\}$ and $|\Sigma^\ell(\mathbf{a})| \geq (t + 1)|H|$.*

By setting $k = 3$ and $m = 2\ell - 2$ and applying the above theorem, we deduce that $0 \in \Sigma^\ell(\mathbf{a})$. This is the heart of the aforementioned result of Bialostocki-Dierker. Theorem 1.9 appears to be close to the truth for small values of k, but we do not know in general when these lower bounds are tight. Our Corollary 1.5 can also be used to derive Theorem 1.9. Indeed, it implies the following stronger result where the dependence on the order of the group has been removed.

Corollary 1.10 *Let $m, k, \ell \in \mathbb{N}$ with $\ell < m$, let $\mathbf{a} = (a_1, \ldots, a_m)$ be a sequence of elements from G with $H = \mathrm{stab}(\Sigma^\ell(\mathbf{a}))$. If $\mathbf{a}$ contains at least k distinct terms, and $\rho(\mathbf{a}) \leq \ell - k + 2$, then one of the following holds.*

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

(ii) *$H \neq \{0\}$, there exists $Q \in G/H$ so that $|\{i \in \{1, \ldots, m\} : a_i \in Q\}| > \ell$.*

Next, let us indicate how the above corollary implies Theorem 1.9. Given the assumptions of Theorem 1.9 and applying Corollary 1.10, we are done immediately if conclusion (i) holds, so we may assume that conclusion (ii) holds. Assuming further that $|\Sigma^\ell(\mathbf{a})| < \ell$ (otherwise we are done) the bound from Corollary 1.5 shows that Q is the only H-coset containing $\geq \ell$ terms of $\mathbf{a}$, and further, setting $t = |\{1 \leq i \leq m : a_i \notin Q\}|$ we have $|\Sigma^\ell(\mathbf{a})| \geq |H|(t + 1)$.

Assuming $|\Sigma^\ell(\mathbf{a})| < \min\{\ell, m - \ell + k - 1\}$ (otherwise we are done), this yields the upper bound on t given in Theorem 1.9.

Finally, we introduce a fundamental result of Gao [9]. For every finite abelian group G, the *Davenport constant* of G, denoted $s(G)$, is the smallest positive integer k 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 smallest positive integer k so that every sequence of elements of G with length $\geq k$ has a subsequence of length $|G|$ which sums to 0. So the Erdős-Ginzburg-Ziv theorem asserts that $s'(G) \leq 2|G| - 1$ for every finite abelian group G. It is an easy exercise to show that $s(G) \leq |G|$ for every G. In light of this, the following theorem of Gao [9] may also be viewed as a generalization of Theorem 1.4.

Theorem 1.11 (Gao) *$s'(G) = s(G) + |G| - 1$ for every finite abelian group G.*

In the third section of our paper we will use Corollary 1.5 to obtain a new proof of Gao's Theorem. Although our proof of Gao's Theorem is no shorter than existing proofs, we have included it since it follows naturally from our result in a manner similar to that of the other generalizations of Erdős-Ginzburg-Ziv.

Instead of considering all possible ℓ-element subsequences of a given sequence $\mathbf{a}$, one might introduce some additional structure on $\mathbf{a}$ and consider only certain special types of subsequences. Bialostocki and Dierker [1] did this by introducing an underlying geometry in the form of a graph. Let X be a graph and let $w : E(X) \to G$ be a map. We define $w(X) = \{\sum_{e \in E(T)} w(e) : T \text{ is a spanning tree of } X\}$.

Theorem 1.12 (Bialostocki-Dierker) *Let p be prime, let X be a complete graph on $p+1$ vertices, and let $w : E(X) \to \mathbb{Z}_p$ be a map. Then $0 \in w(X)$.*

This theorem suggested a rather different type of zero-sum problem, and was soon extended in a number of different directions. Füredi and Kleitman [8] proved that a similar result holds for arbitrary (even nonabelian) groups. More precisely, they prove that for every multiplicative group G of order n, and every edge-labeling of the complete graph on $n+1$ vertices with elements of G, there exists a spanning tree whose edges may be ordered so that the product of the labels (in this order) is the identity. Schrijver and Seymour [19] generalized the Bialostocki-Dierker theorem to hypergraphs, thus obtaining a new proof of the Füredi-Kleitman theorem for abelian groups.

Perhaps even more excitingly, Schrijver and Seymour [18] generalized the underlying geometry further to matroids. If M is a matroid on E, and $w : E \to G$ is a map, we define $w(M) = \{\sum_{b \in B} w(b) : B \text{ is a base of } M\}$.

Conjecture 1.13 (Schrijver-Seymour) *Let M be a matroid on E with rank function* rk*. Let $w : E \to G$ where G is an abelian group. If $H = \mathrm{stab}(w(M))$, then*

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

We consider this conjecture to be very important. Indeed, our main theorem is a very special case of it. Corollary 1.5 is equivalent to the above conjecture for uniform matroids. Our main theorem is equivalent to the above conjecture for matroids obtained from uniform matroids by adding parallel elements.

Schrijver and Seymour [18] proved their conjecture in the special case when $|G|$ is prime. In their 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 prove their conjecture for two special types of groups.

Theorem 1.14 *Conjecture 1.13 holds whenever $|G| = pq$ for primes p, q or $G \cong \mathbb{Z}_{p^n}$ for a prime p and a positive integer n.*

There is a unifying framework for some above-mentioned results. If a matroid M of rank n has two disjoint cocircuits and $w\colon E(M) \to \{0,1\} \subseteq \mathbb{Z}_n$ is a weighting whose support is one of these cocircuits, then $0 \notin w(M)$. Schrijver and Seymour [18] (essentially) observe that Conjecture 1.13 implies a converse to this statement.

Proposition 1.15 (Schrijver-Seymour) *Let G be an abelian group. Let M be a matroid of rank $|G|$ in which every two cocircuits meet. If Conjecture 1.13 holds for G and the dual matroid M^*, then for any map $w : E(M) \to G$ we have $0 \in w(M)$.*

We have already seen two matroids to which this proposition applies. When M is the uniform matroid with rank $|G|$ on $2|G|-1$ points, we obtain the Erdős-Ginzburg-Ziv theorem, since M^* is uniform and satisfies Conjecture 1.13 by Corollary 1.5. When M is a complete graph on $|G|+1$ vertices and $|G|$ is prime, we obtain the Bialostocki-Dierker theorem, as was observed in [18]. Both of these matroids are minimal in the sense that deleting any element results in a matroid with two disjoint cocircuits. It appears hopeless to characterize such minimal matroids. For example, M is a *dual-paving matroid* if all its cocircuits have size at least $|M| - \mathrm{rk}(M)$. Such matroids are easily constructed by modifying a uniform matroid, and they form a very rich class (it is suspected [20] that most matroids of a given size are paving matroids). When constructing a dual-paving matroid M of size $2\,\mathrm{rk}(M)$ or $2\,\mathrm{rk}(M)+1$, it is easy to arrange that M is minimal with respect to not containing disjoint cocircuits. This shows the existence of a large class of minimal matroids M to which we can apply Theorem 1.14; if G is a cyclic group and $\mathrm{rk}(M) = |G|$ is a prime power or the product of two primes, then $0 \in w(M)$ for every $w\colon M \to G$.

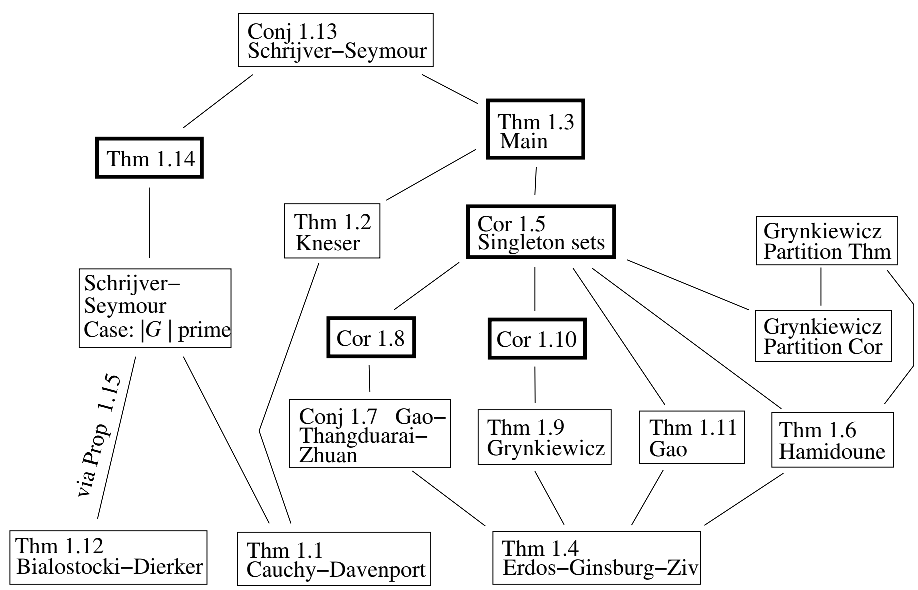

Figure 1: Implications among statements in in Section 1. New results have bold borders.

The remainder of this paper is organized as follows. We prove our main theorem in the next section. We prove three consequences of the main theorem for sequences (Corollaries 1.8, 1.10, and Theorem 1.11) in Section 3. Then, in the final section, we prove our matroidal result, Theorem 1.14.

2 Main Theorem

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

If $K \leq G$ and $\ell \in \mathbb{N}$, we call a map $\mu : G/K \to \mathbb{N}$ a *K-pattern* of *weight ℓ* if $\sum_{Q \in G/K} \mu(Q) = \ell$. If $\mathbf{A} = (A_1, A_2, \ldots, A_m)$ is a sequence of finite subsets of G and μ is a K-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 $Q \in G/K$.

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

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

We are now ready to state our main result in its most general form.

Theorem 2.1 *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 $\mathrm{stab}(\Sigma^\mu(\mathbf{A})) = J$, then*

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

Before we prove Theorem 2.1, 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 $\Theta_K^\ell(\mathbf{A}) = \ell$. Now it is obvious that the bound in Theorem 2.1 implies Theorem 1.3. In particular, Theorem 2.1 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 $1 \le i \le m$. Next we will show that our assumptions imply $J = \{0\}$. It is immediate that $\Sigma^\mu(\mathbf{A})$ is contained in the K-coset $\sum_{Q \in G/K} \mu(Q)Q$, so in particular $J \le K$. Suppose (for a contradiction) that $J \ne \{0\}$ and let $\phi : G \to G/J$ be the canonical homomorphism. Let $\mathbf{A}_\phi = (\phi(A_1), \ldots, \phi(A_m))$, 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 $\Sigma^{\mu_\phi}(\mathbf{A}_\phi) = \phi(\Sigma^\mu(\mathbf{A}))$ has trivial stabilizer, so by the minimality of our counterexample we have

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

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 $1 \le j \le m$ 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 $H = \mathrm{stab}(C)$ to be a *convergent* if it satisfies the following property

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

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 $1 \le i \le m$ let $A'_i = A_i \cap (a_i + K)$. Then set $C_0 = \sum_{i=1}^m A'_i$ and $H_0 = \mathrm{stab}(C_0)$. 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 $|C_0| \ge \sum_{i=1}^m |A'_i +$

$H_0| - (m-1)|H_0|$. Now we have

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

Thus, $|C_0| \geq \sum_{i=1}^m |A_i' + H_0| - (m-1)|H_0| \geq |H_0|(1 - m + \Theta_{H_0}^m(\mathbf{A})) - |K|(\Theta_K^m(\mathbf{A}) - m)$. It follows from this that C_0 is a convergent, and we may now choose a convergent C with $H = \mathrm{stab}(C)$ 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 $\nu(R) = |\{1 \leq i \leq m : b_i + H = R\}|$. Now set $D = \Sigma^\nu(\mathbf{A})$ and $H' = \mathrm{stab}(D)$, and note that $\mathrm{stab}(C \cup D) = H' < H$ since D is properly included in some H-coset disjoint from C. By the assumption that C is a convergent and an application of our bound to $D = \Sigma^\nu(\mathbf{A})$ we have

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

It follows that $C \cup D$ is a convergent with stabilizer $H' < H$ contradicting our choice of C. 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 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 $1 \le i \le m$ 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 $1 \le i \le m$, then $\Sigma^\mu(\mathbf{A}) = \Sigma^\mu(\mathbf{A}^1)$, $\Theta^\ell_K(\mathbf{A}) = \Theta^\ell_K(\mathbf{A}^1)$, and $\Theta^\ell_{\{0\}}(\mathbf{A}) = \Theta^\ell_{\{0\}}(\mathbf{A}^1)$ so $\mathbf{A}^1$ contradicts the choice of $\mathbf{A}$ for (ii). Thus, by rearranging (keeping A_1 fixed), we may assume that $A_1 \not\subseteq A_2$. If $A_2 \subset A_1$, then $\Sigma^\mu(\mathbf{A}^2) \supseteq \Sigma^\mu(\mathbf{A}^1) \neq \emptyset$ contradicting our choice of A_1. Hence, $A_2 \not\subseteq A_1$. Thus, we have $A_1 \setminus A_2 \neq \emptyset$, $A_2 \setminus A_1 \neq \emptyset$, 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 $1 \le i \le m$ 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 $|A_1| \le |A_2|$. If $A_1 = \{a\}$ for some $a \in G$ then the result follows by applying the theorem to the sequence $(A_2, A_3, \ldots, A_m)$. Otherwise, choose distinct $a, a' \in A_1$. Note that $\mathrm{stab}(A_2) \subseteq \mathrm{stab}(\Sigma^m(\mathbf{A})) = \{0\}$. Therefore, $a' - a \notin \mathrm{stab}(A_2)$, 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. By construction, $a \in A_1 \cap A_2$, $a' \in A_1 \setminus A_2$, and $A_2 \setminus A_1 \neq \emptyset$ (this last fact follows from the second and $|A_1| \le |A_2|$). Now setting $\mathbf{A}' = (A_1 \cap A_2, A_1 \cup A_2, A_3, \ldots, A_m)$ we have $\Sigma^\mu(\mathbf{A}') \neq \emptyset$ as desired.

Let us observe that in both cases, the new sequence $\mathbf{A}'$ satisfies $\emptyset \neq \Sigma^\mu(\mathbf{A}') \subseteq \Sigma^\mu(\mathbf{A})$. Further, since $A_1 \setminus A_2 \neq \emptyset$ and $A_2 \setminus A_1 \neq \emptyset$ our theorem applies to $\mathbf{A}'$ by minimality assumption (i) or (iii).

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 $H = \mathrm{stab}(C)$ we have

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

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

$$\begin{aligned} |C_0| &\ge |H_0|(\Theta^\ell_{H_0}(\mathbf{A}') - \ell + 1) - |K|(\Theta^\ell_K(\mathbf{A}') - \ell) \\ &\ge |H_0|(\Theta^\ell_{H_0}(\mathbf{A}') - \ell + 1) - |K|(\Theta^\ell_K(\mathbf{A}) - \ell). \end{aligned}$$

Thus, C_0 is a convergent, and we may now choose a convergent C with stabilizer H so that

H is minimal. If $H = \{0\}$, then we have

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

This contradiction implies that $H \neq \{0\}$.

Our plan is to construct three new sets C^1, C^2, and C^{12}, each of which will be a superset of C with stabilizer $\leq H$. We will then derive a contradiction under the assumption that none of them is a convergent with strictly smaller stabilizer than C.

Since $\Sigma^\mu(\mathbf{A})$ has trivial stabilizer and $\mathrm{stab}(C) = H \neq \{0\}$ we may choose a μ-feasible sequence $(b_1, b_2, \ldots, b_\ell)$ so that $R = \sum_{j=1}^\ell b_j + H \not\subseteq \Sigma^\mu(\mathbf{A})$. Note that $R \cap C = \emptyset$. Further, it follows from $\Sigma^\mu(\mathbf{A}') \subseteq C$ that $b_1 \in A_1$ and $b_2 \in A_2$. Let $\nu : G/H \to \mathbb{N}$ be the H-pattern of weight ℓ given by the rule $\nu(Q) = |\{j \in \{1, \ldots, \ell\} : b_j + H = Q\}|$ and note that $\Sigma^\nu(\mathbf{A}) \subseteq R$. Next, 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 $\nu^*(Q) = |\{j \in \{3, \ldots, \ell\} : b_j + H = Q\}|$. Then, for $\delta = 1, 2$, set $A_1^\delta = A_1 \cap (b_\delta + H)$ and set $A_2^\delta = A_2 \cap (b_{3-\delta} + H)$ (here the reader should note a deliberate "crossing" of our indices). Note further 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 $B^1 = A_1^1 + A_2^1$, set $B^2 = A_1^2 + A_2^2$ and set $B^{12} = B^1 \cup B^2$. Next we give a few definitions, culminating with C^1, C^2, and C^{12}.

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

Now for $\delta = 1, 2$ we define the set D^δ and name its stabilizer as follows.

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

Finally, for $\epsilon = 1, 2, 12$ we define the set C^ϵ as follows (for clarity, we will continue to let δ be a variable ranging over $1, 2$ and let ϵ range over $1, 2, 12$)

$$C^\epsilon = C \cup D^\epsilon.$$

Let us make a few simple observations concerning these newly defined sets. First, note that by construction, $D^1 \neq \emptyset$ and $D^{12} \neq \emptyset$. Further, $D^\epsilon \subseteq \Sigma^\nu(\mathbf{A}) \subset R$ for every $\epsilon = 1, 2, 12$ so each of these sets is disjoint from C. Since each D^ϵ is a proper subset of the H-coset R, it follows that $\mathrm{stab}(C^\epsilon) = H^\epsilon$ whenever $D^\epsilon \neq \emptyset$. Figure 2 shows the containment relationships among the sets C^ϵ and their stabilizers H^ϵ.

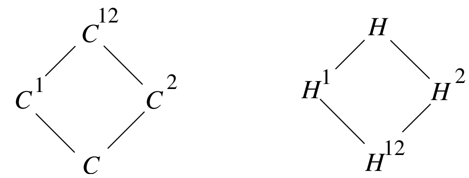

Figure 2: Containment relations among the sets C^ϵ and their stabilizers.

Let us pause to note that by (i) of our choice of $\mathbf{A}$, and the observation that $|\Sigma^\mu(\mathbf{A})| > |C| \geq |H|$, it follows that our theorem holds true (and Kneser's theorem holds) whenever the associated sumset is contained in some H-coset. This fact will be used repeatedly in the remainder of the argument.

Next we shall make two claims which hold for $\epsilon = 1, 12$ and also hold for $\epsilon = 2$ if $D^2 \neq \emptyset$. Both of these claims will help us to simplify the equations which result from inductive applications of our theorem.

Claim 1: $|\Sigma^{\nu^*}(\mathbf{A}^*) + H^\epsilon| \geq |H^\epsilon|(\Theta^{\ell-2}_{H^\epsilon}(\mathbf{A}^*) - \ell + 3) - |H|(\Theta^{\ell-2}_{H}(\mathbf{A}^*) - \ell + 2)$.

Proof of Claim: Set $\mathbf{B} = (A_3 + H^\epsilon, A_4 + H^\epsilon, \ldots, A_m + H^\epsilon)$ and note that $\Sigma^{\nu^*}(\mathbf{B}) = \Sigma^{\nu^*}(\mathbf{A}^*) + H^\epsilon$. Further, it follows from the definition of D^ϵ and H^ϵ that $\mathrm{stab}(\Sigma^{\nu^*}(\mathbf{B})) = H^\epsilon$. Thus, by applying our theorem inductively to $\Sigma^{\nu^*}(\mathbf{B})$ we have

$$\begin{aligned}
|\Sigma^{\nu^*}(\mathbf{A}^*) + H^\epsilon| &= |\Sigma^{\nu^*}(\mathbf{B})| \\
&\geq |H^\epsilon|(\Theta^{\ell-2}_{H^\epsilon}(\mathbf{B}) - \ell + 3) - |H|(\Theta^{\ell-2}_{H}(\mathbf{B}) - \ell + 2) \\
&= |H^\epsilon|(\Theta^{\ell-2}_{H^\epsilon}(\mathbf{A}^*) - \ell + 3) - |H|(\Theta^{\ell-2}_{H}(\mathbf{A}^*) - \ell + 2)
\end{aligned}$$

as desired.

For $\epsilon = 1, 2, 12$ we define X^ϵ and Y^ϵ as follows:

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

Claim 2: $|H|(\Theta^{\ell}_{H}(\mathbf{A}') - \Theta^{\ell-2}_{H}(\mathbf{A}^*)) - |H^\epsilon|(\Theta^{\ell}_{H^\epsilon}(\mathbf{A}') - \Theta^{\ell-2}_{H^\epsilon}(\mathbf{A}^*)) \geq |X^\epsilon \cup Y^\epsilon|$.

Proof of Claim: First observe that contribution of an H-coset Q to $|H|(\Theta^{\ell}_{H}(\mathbf{A}') - \Theta^{\ell-2}_{H}(\mathbf{A}^*))$ (which must be either 0, $|H|$, or $2|H|$) is always at least the contribution of the H^ϵ-cosets contained in Q to $|H^\epsilon|(\Theta^{\ell}_{H^\epsilon}(\mathbf{A}') - \Theta^{\ell-2}_{H^\epsilon}(\mathbf{A}^*))$. Next, 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 $\Sigma^\nu(\mathbf{A}) \subseteq R$ 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 $|H|(\Theta^{\ell}_{H}(\mathbf{A}') - \Theta^{\ell-2}_{H}(\mathbf{A}^*))$ is exactly $|H|$. By a similar argument, the contribution of the H^ϵ-cosets contained in $b_1 + H$ to $|H^\epsilon|(\Theta^{\ell}_{H^\epsilon}(\mathbf{A}') - \Theta^{\ell-2}_{H^\epsilon}(\mathbf{A}^*))$ is exactly $|(A_1^1 \cup A_2^2) + H^\epsilon|$. Thus, the contribution of $b_1 + H$ and its H^ϵ-cosets to the left hand side of the equation in the claim is $|X^\epsilon|$. Similarly, the coset $b_2 + H$ contributes $|Y^\epsilon|$. Whether or not $b_1 + H = b_2 + H$, our claim follows immediately.

The next equation holds for $\epsilon = 1, 12$ and for $\epsilon = 2$ if $D^2 \neq \emptyset$. It follows from the assumption that C is a convergent, but C^ϵ is not.

$$\begin{aligned} |D^\epsilon| &= |C^\epsilon| - |C| \\ &< |H^\epsilon|(\Theta^{\ell}_{H^\epsilon}(\mathbf{A}') - \ell + 1) - |H|(\Theta^{\ell}_{H}(\mathbf{A}') - \ell + 1) \end{aligned} \tag{2}$$

On the other hand, D^ϵ is defined by a sumset to which we may apply our theorem inductively. In the following equation, we have repeatedly applied our theorem inductively in the form of Kneser's theorem, and we have also applied Claim 1. This equation holds for $\epsilon = 1, 12$ and also holds for $\epsilon = 2$ if $D^2 \neq \emptyset$.

$$\begin{aligned} |D^\epsilon| &= |B^\epsilon + \Sigma^{\nu^*}(\mathbf{A}^*) + H^\epsilon| \\ &\geq |B^\epsilon + H^\epsilon| + |\Sigma^{\nu^*}(\mathbf{A}^*) + H^\epsilon| - |H^\epsilon| \\ &\geq |B^\epsilon + H^\epsilon| + |H^\epsilon|(\Theta^{\ell-2}_{H^\epsilon}(\mathbf{A}^*) - \ell + 2) - |H|(\Theta^{\ell-2}_{H}(\mathbf{A}^*) - \ell + 2) \end{aligned} \tag{3}$$

Combining equations 2 and 3 and applying Claim 2 gives us the following equation which holds for $\epsilon = 1, 12$ and also holds for $\epsilon = 2$ if $D^2 \neq \emptyset$.

$$|H| > |B^\epsilon + H^\epsilon| + |X^\epsilon \cup Y^\epsilon| + |H^\epsilon| \tag{4}$$

Using equation (4) and an inductive application of our theorem (again in the form of Kneser's theorem) gives us the following equation which holds for $\delta = 1$ and holds for $\delta = 2$ if $D^2 \neq \emptyset$.

$$|H| > |A_1^\delta + H^\delta| + |A_2^\delta + H^\delta| + |X^\delta \cup Y^\delta|.$$

Consider the above equation with $\delta = 1$. If $A_2^2 = \emptyset$, then $|X^1| = |H| - |A_1^1 + H^1|$ and we have a contradiction. 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 $D^2 \neq \emptyset$, so equations (2), (3), and (4) hold for $\epsilon = 2$, and the above equation holds for $\delta = 2$. 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 the above equation for $\delta = 1$. Thus $b_1 + H \neq b_2 + H$, and we have that X^ϵ and Y^ϵ are disjoint for $\epsilon = 1, 2, 12$.

Our next equation follows from the previous equation, and the observation that $|H|$, $|A_1^\delta + H^\delta|$, and $|A_2^\delta + H^\delta|$ are all multiples of $|H^\delta|$. It holds for $\delta = 1, 2$:

$$\begin{aligned} |H| &\geq |A_1^\delta + H^\delta| + |A_2^\delta + H^\delta| + |H^\delta| \\ &\geq |A_1^\delta + H^{12}| + |A_2^\delta + H^{12}| + |H^\delta| \end{aligned} \tag{5}$$

The next equation follows from equation (4) for $\epsilon = 12$ and another application of Kneser's theorem. Here the application of Kneser's theorem requires the observation that the stabilizer of the sumset $(A_1^\delta + H^{12}) + (A_2^\delta + H^{12}) = B^\delta + H^{12}$ is a subgroup of H^δ - a fact which follows from the definition of D^δ.

$$\begin{aligned} |H| &\geq |B^{12} + H^{12}| + |X^{12} \cup Y^{12}| \\ &\geq |B^\delta + H^{12}| + |X^{12}| + |Y^{12}| \\ &\geq |A_1^\delta + H^{12}| + |A_2^\delta + H^{12}| - |H^\delta| + |X^{12}| + |Y^{12}| \end{aligned} \tag{6}$$

Summing the four inequalities obtained by taking equations 5 and 6 for $\delta = 1, 2$ and then dividing by two yields

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

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. □

3 Corollaries

In this section use our main corollary for subsequence sums (Corollary 1.5) to derive Corollaries 1.8 and 1.10, and to give a new proof of Gao's Theorem (1.11). We use the following notation. If $\mathbf{a} = (a_1, \ldots, a_m)$ is a sequence of elements from 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 $\rho_g(\mathbf{a}) = \rho_{\{g\}}(\mathbf{a})$. The function ρ defined in the introduction (the maximum multiplicity of an element) is then $\rho(\mathbf{a}) = \max_{g \in G} \rho_g(\mathbf{a})$. For convenience we have restated Corollary 1.5 below with this new notation.

Corollary 1.5 *If $\mathbf{a} = (a_1, \ldots, a_m)$ is a sequence of elements of G and $H = \mathrm{stab}(\Sigma^\ell(\mathbf{a}))$, then*

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

Proof of Corollary 1.8: Recall that 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 (additive) inverse of the other), so we may apply Corollary 1.5 both for $\Sigma^\ell(\mathbf{a})$ and $\Sigma^{m-\ell}(\mathbf{a})$. Let $H = \mathrm{stab}(\Sigma^\ell(\mathbf{a})) = \mathrm{stab}(\Sigma^{m-\ell}(\mathbf{a}))$. If $H = \{0\}$, then applying Corollary 1.5 to $\Sigma^{m-\ell}(\mathbf{a})$ shows that $|\Sigma^\ell(\mathbf{a})| = |\Sigma^{m-\ell}(\mathbf{a})| \geq \ell + 1$ (since $\rho(\mathbf{a}) \leq m - \ell$), so (i) holds. Otherwise, applying this bound to $\Sigma^\ell(\mathbf{a})$ shows that either (ii) holds, or $|\Sigma^\ell(\mathbf{a})| \geq |H|(1 + m - \ell) \geq |H| \cdot \ell/p \geq \ell$ which implies (i). $\square$

Proof of Corollary 1.10: We shall assume that neither (i) nor (ii) holds and derive a contradiction. Set $h = |H|$ and set $t = |\{Q \in G/H : \rho_Q(\mathbf{a}) \geq m - \ell\}|$. If $t = 0$, then Corollary 1.5 (applied with $m - \ell$ in place of ℓ) 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 let $g_0 \in G$ be the unique element with $\rho_{g_0}(\mathbf{a}) \geq m - \ell$, and note that since $\rho_{g_0}(\mathbf{a}) \leq \ell - k + 2$, we must have $\sum_{g \in G} \min\{m - \ell, \rho_g(\mathbf{a})\} = m - (\rho_{g_0}(\mathbf{a}) - (m - \ell)) \geq 2m - 2\ell + k - 2$. 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 1.5 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 1.5 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

$$k - h > (h-1)(m-\ell). \tag{7}$$

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

$$\begin{aligned} |\Sigma^{m-\ell}(\mathbf{a})| &\geq h\Big(1 - m + \ell + \sum_{Q \in G/H} \min\{m-\ell, \rho_Q(\mathbf{a})\}\Big) \\ &= h\Big(1 + \sum_{Q \in (G/H)\setminus\{R\}} \min\{m-\ell, \rho_Q(\mathbf{a})\}\Big). \end{aligned} \tag{8}$$

First suppose that $m - \ell \geq h$. Then the Σ-term in the right hand side of equation (8) 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 $|\Sigma^{m-\ell}(\mathbf{a})| \geq h(1 + k - |R|) = h(1+k-h)$. Combining this with Equation (7) 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 Σ-term in the right hand side of equation (8). 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 Σ-term in the right hand side of (8) 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 1.11: 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 of elements from G. We need to show that $0 \in \Sigma^{|G|}(\mathbf{a})$. Set $H = \mathrm{stab}(\Sigma^{|G|}(\mathbf{a}))$. If $H \neq \{0\}$, then let $\phi : G \to G/H$ be the canonical homomorphism and consider the sequence $\mathbf{a}_\phi = (\phi(a_1), \phi(a_2), \ldots, \phi(a_m))$. 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 from $\mathbf{a}_\phi$, we apply the theorem again to get another such sequence. After $|H|$ repetitions, we have $|H|$ disjoint subsequences of $\mathbf{a}_\phi$ 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 is in H. Since $H = \mathrm{stab}(\Sigma^{|G|}(\mathbf{a}))$, it follows that $0 \in \Sigma^{|G|}(\mathbf{a})$. Thus, we may assume that $H = \{0\}$.

If $\rho(\mathbf{a}) < s(G)$, then by Corollary 1.5 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 $s(G)$, 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. $\square$

4 Matroids

The goal of this section is to prove Theorem 1.14. 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 to 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 abbreviate $E_g = E_{\{g\}}$. We define

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

With this notation we restate Theorem 1.14.

Theorem 4.1 *Let p, q be primes and assume that $G \cong \mathbb{Z}_{p^n}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$. If $H =$ $\mathrm{stab}(W(M))$, then*

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

Proof: We proceed by induction on $|E|$. We may assume that M has no loops or parallel elements (if $e, f \in E$ are parallel, then replace $W(e)$ by $W(e) \cup W(f)$, delete f and apply induction). If $\mathrm{rk}(M) = 1$, then the result is trivial, so we may further assume that $\mathrm{rk}(M) \geq 2$. For every $e \in E$, we define the subgroup

$$H_e = \mathrm{stab}(W(e)).$$

By possibly replacing $W(e)$ with a superset, we may assume that for every $e \in E$ and every $g \in G \backslash W(e)$, the weight function W' obtained from W by the adjustment $W'(e) = W(e) \cup \{g\}$ satisfies $W'(M) \neq W(M)$. The inequality below follows from this maximality assumption.

$$H \leq H_e \text{ for every } e \in E. \tag{9}$$

If $g \in G$ and E_g spans e, then replacing $W(e)$ by $W(e) \cup \{g\}$ does not change the set $W(M)$. To see this let $h \in g + \sum_{b \in B - e} W(b)$ where B is a basis containing e. Then $B - e + f$ is a basis for some $f \in E_g \backslash B$, whence $h \in \sum_{b \in B - e + f} W(b)$. By repeating this process, we may assume that $W(e) = \{g \in G : E_g \text{ spans } e\}$ for every $e \in E$. Equivalently (in light of equation (9)), we have

$$W(e) = \cup \{Q \in G/H : E_Q \text{ spans } e\} \tag{10}$$

Let M/e denote the matroid obtained from M by contracting e and consider the set $W(e) + W(M/e)$. By construction, this is a subset of $W(M)$ and has stabilizer $\geq H_e = \mathrm{stab}(W(e))$. However, the maximality of $W(e)$ further implies that

$$H_e = \mathrm{stab}(W(e) + W(M/e)). \tag{11}$$

Suppose now that $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$. If there exist $e, f \in E$ with H_e and H_f being distinct nontrivial subgroups, then we may choose a base B containing e and f, and we find that $\text{stab}\left(\sum_{b \in B} W(b)\right) \geq H_e + H_f = G$ so $W(M) = G$, and we have $H = G$ which contradicts either $H \leq H_e$ or $H \leq H_f$. It follows from this argument that the subgroups $\{H_e : e \in E\}$ are nested when $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Since any two subgroups of $\mathbb{Z})_{p^n}$ are nested, the same conclusion also holds for this case. Thus, we may choose $f \in E$ so that $H_f \leq H_e$ for every $e \in E$. It follows immediately from this that $H_f \leq \text{stab}(W(M)) = H$, and $H_f \leq \text{stab}(W(M/f))$. The first of these inequalities and (9) imply that $H_f = H$. It follows from the second and equation (11) that $\text{stab}(W(M/f)) = H_f = H$. So, all three sets $W(M)$, $W(M/f)$, and $W(f) + W(M/f)$ have stabilizer H. Now, applying Kneser's Theorem (Theorem 1.2), equation (10), and the induction hypothesis, we have:

$$\begin{aligned} |W(M)| &\geq |W(f) + W(M/f)| \\ &\geq |W(f)| + |W(M/f)| - |H| \\ &\geq |H|\Big(|\{Q \in G/H :\ E_Q \text{ spans } f\ \}| + 1 - \text{rk}(M/f) + \sum_{Q \in G/H} \text{rk}_{M/f}(E_Q)\Big) - |H| \\ &= |H|\Big(1 - \text{rk}(M) + \sum_{Q \in G/H} \text{rk}_M(E_Q)\Big) \end{aligned}$$

which completes the proof. $\square$

References

[1] A. Bialostocki, P. Dierker, Zero sum Ramsey theorems, Congr. Numer. 70 (1990), 119–130.

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

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

[4] H. Q. Cao, An addition theorem on the cyclic group $\mathbb{Z}_{p^\alpha q^\beta}$, The Electronic J. of Combinatorics 13 (2006), N9.

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

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

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

[8] Z. Füredi, D. J. Kleitman, On zero-trees. J. Graph Theory 16 (1992), 107–120.

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

[10] W. D. Gao, Three addition Theorems on $\mathbb{Z}_n$, preprint.

[11] W. D. Gao, R. Thangadurai, J. Zhuang, Addition Theorems on the cyclic groups $\mathbb{Z}_{p^n}$, preprint.

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

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

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

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

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

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

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

[19] A. Schrijver, P. D. Seymour, A simpler proof and a generalization of the zero-trees theorem, J. Combin. Theory Ser. A 58 (1991), 301–305.

[20] D. J. A. Welsh, Matroid theory, Academic Press [Harcourt Brace Jovanovich Publishers], London, 1976. L. M. S. Monographs, No. 8.