

JOURNAL

de Théorie des Nombres

de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

David J. GRYNKIEWICZ, Luz E. MARCHAN et Oscar ORDAZ

Representation of finite abelian group elements by subsequence sums

Tome 21, n° 3 (2009), p. 559-587.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_3_559_0>

© Université Bordeaux 1, 2009, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jtnb.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

Representation of finite abelian group elements by subsequence sums

par DAVID J. GRYNKIEWICZ, LUZ E. MARCHAN et OSCAR ORDAZ

RÉSUMÉ. Soit $G \cong C_{n_1} \oplus \dots \oplus C_{n_r}$ un groupe abélien fini non trivial avec $n_1 | n_2 | \dots | n_r$. Une conjecture d'Hamidoune dit que si $W = w_1 \dots w_n$ est une suite d'entiers, tous, sauf au plus un, premiers à $|G|$, et S une suite d'éléments de G avec $|S| \geq |W| + |G| - 1 \geq |G| + 1$, la multiplicité maximale de S au plus $|W|$, et $\sigma(W) \equiv 0 \pmod{|G|}$, alors il existe un sous-groupe non trivial H tel que tout élément $g \in H$ peut être représenté par une somme pondérée de la forme $g = \sum_{i=1}^n w_i s_i$, avec $s_1 \dots s_n$ une sous-suite de S . Nous donnons deux exemples qui montrent que cela n'est pas vrai en général, et nous caractérisons les contre-exemples pour les grands $|W| \geq \frac{1}{2}|G|$.

Un théorème de Gao, généralisant un résultat plus ancien d'Olson, dit que si G est un groupe abélien fini, et S une suite d'éléments de G avec $|S| \geq |G| + D(G) - 1$, alors, soit tout élément de G peut être représenté par une sous-somme de S à $|G|$ termes, soit il existe une classe $g + H$ telle que tous sauf au plus $|G/H| - 2$ termes de S sont dans $g + H$. Nous établissons quelques cas très spéciaux d'un analogue pondéré de ce théorème, conjecturé par Ordaz et Quiroz, et quelques conclusions partielles dans les autres cas, qui impliquent un résultat récent d'Ordaz et Quiroz. Cela est fait, en partie, en étendant un théorème de Gryniewicz sur les partitions pondérées, que nous utilisons également pour améliorer le résultat de Gao cité précédemment en montrant que l'hypothèse $|S| \geq |G| + D(G) - 1$ peut être affaiblie en $|S| \geq |G| + d^*(G)$, où $d^*(G) = \sum_{i=1}^r (n_i - 1)$. Nous utilisons aussi cette méthode pour déduire une variante de la conjecture d'Hamidoune valide si au moins $d^*(G)$ des w_i sont premiers à $|G|$.

Manuscrit reçu le 3 juin 2008.

This project was begun while the first author was supported by NSF grant DMS-0502193, and completed while he was supported by FWF project number M1014-N13.

Mots clefs. zero-sum problem, Davenport constant, weighted subsequence sums, setpartition, $d^*(G)$.

Classification math. 11B75, 20K01.

ABSTRACT. Let $G \cong C_{n_1} \oplus \dots \oplus C_{n_r}$ be a finite and nontrivial abelian group with $n_1|n_2|\dots|n_r$. A conjecture of Hamidoune says that if $W = w_1 \cdot \dots \cdot w_n$ is a sequence of integers, all but at most one relatively prime to $|G|$, and S is a sequence over G with $|S| \geq |W| + |G| - 1 \geq |G| + 1$, the maximum multiplicity of S at most $|W|$, and $\sigma(W) \equiv 0 \pmod{|G|}$, then there exists a nontrivial subgroup H such that every element $g \in H$ can be represented as a weighted subsequence sum of the form $g = \sum_{i=1}^n w_i s_i$, with $s_1 \cdot \dots \cdot s_n$ a subsequence of S . We give two examples showing this does not hold in general, and characterize the counterexamples for large $|W| \geq \frac{1}{2}|G|$.

A theorem of Gao, generalizing an older result of Olson, says that if G is a finite abelian group, and S is a sequence over G with $|S| \geq |G| + D(G) - 1$, then either every element of G can be represented as a $|G|$ -term subsequence sum from S , or there exists a coset $g + H$ such that all but at most $|G/H| - 2$ terms of S are from $g + H$. We establish some very special cases in a weighted analog of this theorem conjectured by Ordaz and Quiroz, and some partial conclusions in the remaining cases, which imply a recent result of Ordaz and Quiroz. This is done, in part, by extending a weighted setpartition theorem of Grynkiewicz, which we then use to also improve the previously mentioned result of Gao by showing that the hypothesis $|S| \geq |G| + D(G) - 1$ can be relaxed to $|S| \geq |G| + d^*(G)$, where $d^*(G) = \sum_{i=1}^r (n_i - 1)$. We also use this method to derive a variation on Hamidoune’s conjecture valid when at least $d^*(G)$ of the w_i are relatively prime to $|G|$.

1. Notation

We follow the conventions of [9] and [11] for notation concerning sequences over an abelian group. For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$. Throughout, all abelian groups will be written additively. Let G be an abelian group, and let $A, B \subseteq G$ be nonempty subsets. Then

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

denotes their *sumset*. The *stabilizer* of A is defined as $H(A) = \{g \in G \mid g + A = A\}$, and A is called *periodic* if $H(A) \neq \{0\}$, and *aperiodic* otherwise. If A is a union of H -cosets (i.e., $H \leq H(A)$), then we say A is *H-periodic*. The order of an element $g \in G$ is denoted $\text{ord}(g)$, and we use $\phi_H : G \rightarrow G/H$ to denote the natural homomorphism. We use $\text{gcd}(a, b)$ to denote the greatest common divisor of $a, b \in \mathbb{Z}$.

For a set P (often with $P = G$ an abelian group), let $\mathcal{F}(P)$ be the free abelian monoid with basis P . The elements of $\mathcal{F}(P)$ are called *sequences*

over P . We write sequences $S \in \mathcal{F}(P)$ in the form

$$S = s_1 \cdot \dots \cdot s_r = \prod_{g \in G} g^{v_g(S)}, \quad \text{where } v_g(S) \geq 0 \text{ and } s_i \in G.$$

We call $|S| := r = \sum_{g \in P} v_g(S)$ the *length* of S , and $v_g(S)$ the *multiplicity* of g in S . The *support* of S is

$$\text{supp}(S) := \{g \in P \mid v_g(S) > 0\}.$$

A sequence S_1 is called a *subsequence* of S if $S_1|S$ in $\mathcal{F}(P)$ (equivalently, $v_g(S_1) \leq v_g(S)$ for all $g \in P$), and in such case, SS_1^{-1} denotes the subsequence of S obtained by removing all terms from S_1 . The *sum* of S is

$$\sigma(S) := \sum_{i=1}^r s_i = \sum_{g \in G} v_g(S)g,$$

and we use

$$h(S) := \max\{v_g(S) \mid g \in P\}$$

to denote the maximum multiplicity of a term of S . A sequence S is *zero-sum* if $\sigma(S) = 0$. Given any map $\varphi : G \rightarrow G'$, we extend φ to a map of sequences, $\varphi : \mathcal{F}(G) \rightarrow \mathcal{F}(G')$, by letting $\varphi(S) := \varphi(s_1) \cdot \dots \cdot \varphi(s_r)$. We say that two sequences $S_1, S_2 \in \mathcal{F}(\mathbb{Z})$ are *congruent modulo n* , and we write $S_1 \equiv S_2 \pmod n$, if $\varphi(S_1) = \varphi(S_2)$ for the canonical homomorphism $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$. We say that at most n terms of the sequence $S = g_1 \cdot \dots \cdot g_l$ are from a given subset $A \subseteq G$ if

$$|\{i \in [1, l] \mid g_i \in A\}| \leq n.$$

Next we introduce notation for weighted subsequence sums, which we will do in the more general context of R -modules (though the focus of this paper is $R = \mathbb{Z}$). Let R be a ring and G a (left) R -module (thus G is also an abelian group with the two notions coinciding when $R = \mathbb{Z}$). If $w \in R$ and $A \subseteq G$, then $w \cdot A = \{wa \mid a \in A\}$ denotes the dilation of A . Let $S \in \mathcal{F}(G)$, $W \in \mathcal{F}(R)$ and $s = \min\{|S|, |W|\}$. Define

$$W \cdot S = \left\{ \sum_{i=1}^s w_i g_i \mid \begin{array}{l} w_1 \cdot \dots \cdot w_s \text{ is a subsequence of } W \text{ and} \\ g_1 \cdot \dots \cdot g_s \text{ is a subsequence of } S \end{array} \right\},$$

and for $1 \leq n \leq s$, let

$$\begin{aligned} \Sigma_n(W, S) &= \{W' \cdot S' : S'|S, W'|W \text{ and } |W'| = |S'| = n\} \\ \Sigma_{\leq n}(W, S) &= \bigcup_{i=1}^n \Sigma_i(W, S) \quad \text{and} \quad \Sigma_{\geq n}(W, S) = \bigcup_{i=n}^s \Sigma_i(W, S), \\ \Sigma(W, S) &= \Sigma_{\leq s}(W, S). \end{aligned}$$

If $W = 1^{|S|}$ (with 1 the identity in R), then $\Sigma(W, S)$ (and other such notation) is abbreviated by $\Sigma(S)$, which is the usual notation for the set of *subsequence sums*. Note that $\Sigma_{|W|}(W, S) = W \cdot S$ when $|W| \leq |S|$.

Let P denote the set of nonempty subsets of G . The elements of $\mathcal{F}(P)$ will be called *setpartitions* (over G), and an *n-setpartition* B (over G) is an element in $\mathcal{F}(P)$ of length n (in other words, B is a formal product of n nonempty subsets of G). If $B = B_1 \cdot \dots \cdot B_n \in \mathcal{F}(P)$, with $\emptyset \neq B_i \subseteq G$ for all $i \in [1, n]$, then we say that B is an *n-setpartition* of the sequence

$$T := \prod_{i=1}^n \prod_{b \in B_i} b \in \mathcal{F}(G),$$

and we call T the sequence associated to B . Note T is finite if and only if each B_i is finite. Conversely, we say that S has an *n-setpartition* if S is the associated sequence of some *n-setpartition*. It is easily shown (see [4] [18] [19]) that S has an *n-setpartition* if and only if $h(S) \leq n \leq |S|$, and if such is the case, then S has an *n-setpartition* with sets of as near equal a size as possible (i.e., $||B_i| - |B_j|| \leq 1$ for all $i, j \in [1, n]$).

2. Introduction

Let

$$G \cong C_{n_1} \oplus \dots \oplus C_{n_r}$$

be a finite abelian group with $n_1|n_2| \dots |n_r$, where C_{n_j} denotes a cyclic group of order $n_j \geq 2$. Thus r is the rank $r(G)$, $n_1 \cdots n_r$ is the order $|G|$, and n_r is the exponent $\text{exp}(G)$. In 1961, Erdős, Ginzburg and Ziv proved that every sequence $S \in \mathcal{F}(G)$ with $|S| \geq 2|G| - 1$ has $0 \in \Sigma_{|G|}(S)$ [6] [30]. This sparked the field of zero-sum combinatorics, which has now seen much development and become an essential component in Factorization Theory (see [9] [11] for a recent survey and text on the subject).

One of the oldest and most important invariants in this area is the *Davenport constant* of G , denoted $D(G)$, which is the least integer so that $S \in \mathcal{F}(G)$ with $|S| \geq D(G)$ implies $0 \in \Sigma(S)$. A very basic argument shows

$$(1) \quad d^*(G) + 1 \leq D(G) \leq |G|$$

(see [11]), where

$$d^*(G) := \sum_{i=1}^r (n_i - 1).$$

Originally, the lower bound was favored as the likely truth, but later examples with $D(G) > d^*(G) + 1$ were found (see [8] [12]), and it is not now well understood when $d^*(G) + 1 = D(G)$ fails, though it is still thought that equality should hold for many instances (and known to be the case for a few) [11].

Gao later linked the study of zero-sums with the study of $|G|$ -term zero-sums (and hence results like the Erdős-Ginzburg-Ziv Theorem), by showing that $\ell(G) = |G| + D(G) - 1$, where $\ell(G)$ is the least integer so that $S \in \mathcal{F}(G)$ with $|S| \geq \ell(G)$ implies $0 \in \Sigma_{|G|}(S)$ [7]. In the same paper, he also proved the following generalization of an older result of Olson [31].

Theorem A. *Let G be a finite abelian group, and let $S \in \mathcal{F}(G)$ with $|S| \geq |G| + D(G) - 1$. Then either $\Sigma_{|G|}(S) = G$ or there exist a proper subgroup $H < G$ and some $g \in G$ such that all but at most $|G/H| - 2$ terms of S are from the coset $g + H$.*

Thus the number $\ell(G) = |G| + D(G) - 1$ also guarantees that every element (not just zero) can be represented as an $|G|$ -term subsequence sum, provided no coset contains too many of the terms of S .

In this paper, we concern ourselves with weighted zero-sum problems related to the above results, though some of our results are new in the non-weighted case as well. Such variations were initiated by Caro in [5] where he conjectured the following weighted version of the Erdős-Ginzburg-Ziv Theorem, which, after much partial work [3] [10] [22] [23], was recently proven in [14]. (Note the condition $\sigma(W) \equiv 0 \pmod{\exp(G)}$ is necessary, else S with $\text{supp}(S) = \{1\}$ would give a counterexample.)

Theorem B. *Let G be a finite abelian group, and let $S \in \mathcal{F}(G)$ and $W \in \mathcal{F}(\mathbb{Z})$ with $\sigma(W) \equiv 0 \pmod{\exp(G)}$. If $|S| \geq |W| + |G| - 1$, then $0 \in \Sigma_{|W|}(W, S)$.*

Since then, there have been several other results along these lines (see [1] [2] [13] [32] for some examples). However, the following conjecture of Hamidoune remained open [22].

Conjecture 2.1. *Let G be a nontrivial, finite abelian group, and let $S \in \mathcal{F}(G)$ and $W \in \mathcal{F}(\mathbb{Z})$ with $|S| \geq |W| + |G| - 1 \geq |G| + 1$ and $\sigma(W) \equiv 0 \pmod{|G|}$. If $h(S) \leq |W|$ and there is some $w \in \text{supp}(W)$ such that $\gcd(w', \exp(G)) = 1$ for all $w' \in \text{supp}(w^{-1}W)$, then $\Sigma_{|W|}(W, S)$ contains a nontrivial subgroup.*

Hamidoune verified his conjecture in the case $|W| = |G|$ [22], and under the additional hypothesis of either $h(S) < |W|$ or $|W| \geq |G|$ or $\gcd(w_i, \exp(G)) = 1$ for all $w_i \in W$, Conjecture 2.1 follows from the result in [14]. In Section 3, we give two examples which show that Conjecture 2.1 is false in general, and prove the following theorem, which characterizes the (rather limited) counter-examples for large $|W| \geq \frac{1}{2}|G|$.

Theorem 2.2. *Let G be a finite, nontrivial abelian group, and let $S \in \mathcal{F}(G)$ and $W \in \mathcal{F}(\mathbb{Z})$ with $|S| \geq |W| + |G| - 1 \geq |G| + 1$ and $\sigma(W) \equiv 0 \pmod{|G|}$. Suppose $h(S) \leq |W|$ and that there is some $w \in \text{supp}(W)$ such that $\gcd(w', \exp(G)) = 1$ for all $w' \in \text{supp}(w^{-1}W)$. If also $|W| \geq \frac{1}{2}|G|$, then either:*

- (i) $\Sigma_{|W|}(W, S)$ contains a nontrivial subgroup, or
- (ii) $|\text{supp}(S)| = 2$, $|W| = |G| - 1$, $G \cong \mathbb{Z}/2^r\mathbb{Z}$ and

$$W \equiv x^{(n-1)/2}(-x)^{(n-1)/2}0 \pmod{|G|},$$

for some $r, n, x \in \mathbb{Z}^+$.

Another open conjecture is the following weighted generalization of Theorem A [32]. We remark that, in the same paper, they showed Conjecture 2.3 to be true when $|S| = 2|G| - 1$, and thus for cyclic groups.

Conjecture 2.3. *Let G be a finite abelian group, and let $W \in \mathcal{F}(\mathbb{Z})$ with $|W| = |G|$, $\sigma(W) \equiv 0 \pmod{\exp(G)}$ and $\gcd(w, \exp(G)) = 1$ for all $w \in \text{supp}(W)$. If $S \in \mathcal{F}(G)$ with $|S| = |G| + D(G) - 1$, then either:*

- (i) $\Sigma_{|G|}(W, S) = G$, or
- (ii) *there exist a proper subgroup $H < G$ and some $g \in G$ that all but at most $|G/H| - 2$ terms of S are from the coset $g + H$.*

In section 5, we prove some limited results related to Conjecture 2.3. In particular, we verify it in the extremal case $h(S) \geq D(G) - 1$ (allowing also $|S| \geq |G| + D(G) - 1$ provided $h(S) \leq |G|$), and give a corollary that extends the result of [32] and shows, when $h(S) \leq D(G) - 1$, that the hypotheses of Conjecture 2.3 (assuming (ii) fails) instead imply $\Sigma_{|S|-|G|}(W, S) = G$. This latter result will follow from the following pair of theorems, which improve (for non-cyclic groups) a corollary from the end of [14] (see also [16] for the non-weighted version, of which this is also an improvement).

Theorem 2.4. *Let G be a finite abelian group, let $S, S' \in \mathcal{F}(G)$ with $S' | S$ and let $W = w_1 \cdot \dots \cdot w_n \in \mathcal{F}(\mathbb{Z})$ be a sequence of integers relatively prime to $\exp(G)$ such that $h(S') \leq |W| = n \leq |S'|$ and $d^*(G) \leq |W|$. Then S has a subsequence S'' with $|S''| = |S'|$ such that either:*

- (i) *there exists an n -setpartition $A = A_1 \cdot \dots \cdot A_n$ of S'' such that*

$$\left| \sum_{i=1}^n w_i \cdot A_i \right| \geq \min\{|G|, |S'| - n + 1\},$$

or

- (ii) *there exist an n -setpartition $A = A_1 \cdot \dots \cdot A_n$ of S'' , a proper, nontrivial subgroup $H < G$ and some element $g \in G$, such that the following properties are satisfied:*

- (a) $(g + H) \cap A_i \neq \emptyset$ for all $i \in [1, n]$, and $\text{supp}(SS''^{-1}) \subseteq g + H$,
- (b) $A_i \subseteq g + H$ for all $i \leq d^*(H)$ and all $i > d^*(H) + d^*(G/H)$,
- (c) $|\sum_{i=1}^n w_i \cdot A_i| \geq (e + 1)|H|$ and all but $e \leq |G/H| - 2$ terms of S are from $g + H$, and
- (d)

$$\sum_{i=1}^{d^*(H)} w_i \cdot A_i = \left(\sum_{i=1}^{d^*(H)} w_i \right) g + H.$$

Theorem 2.5. *Let G be a finite abelian group, let $S, S' \in \mathcal{F}(G)$ with $S' | S$ and let $W = w_1 \dots w_n \in \mathcal{F}(\mathbb{Z})$ be a sequence of integers relatively prime to $\text{exp}(G)$ such that $h(S') \leq |W| = n \leq |S'|$ and $d^*(G) \leq |W|$. Suppose there exists a nontrivial subgroup $K \leq G$ with the following properties:*

there exist $g' \in G, T \in \mathcal{F}(g' + K)$ with $T | S$, and a $d^(K)$ -setpartition $B_1 \dots B_{d^*(K)}$ of T , such that*

$$\sum_{i=1}^{d^*(K)} w_i \cdot B_i = \left(\sum_{i=1}^{d^*(K)} w_i \right) g' + K$$

and $T^{-1}S$ contains at least $n - d^(K) + |S| - |S'|$ terms from $g' + K$.*

Let $K^ \leq G$ be the maximal subgroup having the above properties. Then the following hold.*

- (i) *If $K^* = G$, then there is an n -setpartition $A = A_1 \dots A_n$ of a subsequence S'' of S such that $|S'| = |S''|$ and*

$$\sum_{i=1}^n w_i \cdot A_i = G.$$

- (ii) *If $K^* \neq G$, then the conclusion of Theorem 2.4(ii) holds with $H = K^*$.*

Notice that in both Theorems 2.4 and 2.5 one is allowed to chose the ordering on the sequence $W = w_1 \dots w_n$ (given by the choice of indices) in any way, which will affect the implication given by Theorem 2.4(ii)(d). Theorem 2.4 allows the result to applied when $n \geq d^*(G)$, rather than $n \geq \frac{|G|}{p} - 1$ (as in the original corollary), where p is the smallest prime divisor of $|G|$ (note, for non-cyclic groups, the number $d^*(G)$ is generally much smaller than $\frac{|G|}{p} - 1$), and contains similar improvements of bounds present in (ii)(b). However, the bound present in (ii)(c) remains unaltered, and improvements here would likely be more difficult. Theorem 2.5 will be used to prove Theorem 2.4, and also gives a way to force Theorem 2.4(ii) to hold.

As a second consequence of Theorems 2.4 and 2.5, we prove the following variation on Theorem 2.2, which extends Hamidoune’s result from [23] by showing that it is only necessary to have at least $d^*(G)$ of the weights relatively prime to $\exp(G)$.

Corollary 2.6. *Let G be a nontrivial, finite abelian group, and let $S \in \mathcal{F}(G)$ and $W \in \mathcal{F}(\mathbb{Z})$ with $|S| \geq |W| + |G| - 1$, $h(S) \leq |W|$ and $\sigma(W) \equiv 0 \pmod{\exp(G)}$. If W has a subsequence W' such that $|W'| + d^*(G) \leq |W|$ and $\gcd(w, \exp(G)) = 1$ for all $w \in \text{supp}(W'^{-1}W)$, then $\Sigma_{|W|}(W, S)$ contains a nontrivial subgroup.*

As a third consequence, we improve Theorem A by relaxing the required hypothesis from $|S| \geq |G| + D(G) - 1$ to $|S| \geq |G| + d^*(G)$ (recall from (1) that $D(G) - 1 \geq d^*(G)$). This should be put in contrast to the fact that $\ell(G) = |G| + D(G) - 1 > |G| + d^*(G)$ is in general possible (since $D(G) - 1 > d^*(G)$ is possible). The methods of employing Theorems 2.4 and 2.5 from these three applications should also be applicable for other zero-sum problems.

3. On Conjecture 2.1

We begin by giving the two counter examples to Conjecture 2.1.

Example 1. Let $p \equiv -1 \pmod{4}$ be a prime, let $G = C_p$ be cyclic of prime order, let $n = \frac{p-1}{2}$, let $W = 1^{(n-1)/2}(-1)^{(n-1)/2}0 \in \mathcal{F}(\mathbb{Z})$, and let $S = 0^n g^n (2g)^n$, where $g \in G \setminus \{0\}$. Note that $h(S) = n = |W|$, that $|S| = 3n = |W| + |G| - 1$, that $\sigma(W) = 0$, and that

$$\Sigma_{|W|}(W, S) = \sum_{i=1}^{(n-1)/2} \{0, g, 2g\} - \sum_{i=1}^{(n-1)/2} \{0, g, 2g\} = G \setminus \left\{ \frac{p+1}{2}g, \frac{p-1}{2}g \right\}.$$

Thus $G \not\subseteq \Sigma_{|W|}(W, S)$, which, since $|G|$ is prime, implies $\Sigma_{|W|}(W, S)$ does not contain a nontrivial subgroup.

Example 2. Let $m = 2^r$, let $G = C_m$, let $n = m - 1$, let $W = 1^{(n-1)/2}(-1)^{(n-1)/2}0$, and let $S = 0^n g^n$, where $g \in G$ with $\text{ord}(g) = m$. Note that $h(S) = n = |W|$, that $|S| = 2n = |W| + |G| - 1$, that $\sigma(W) = 0$, and that

$$\Sigma_{|W|}(W, S) = \sum_{i=1}^{(n-1)/2} \{0, g\} - \sum_{i=1}^{(n-1)/2} \{0, g\} = G \setminus \left\{ \frac{m}{2}g \right\}.$$

Hence, since every nontrivial subgroup of $G \cong \mathbb{Z}/2^r\mathbb{Z}$ contains the unique element of order 2, namely $\frac{m}{2}g$, it follows that $\Sigma_{|W|}(W, S)$ does not contain a nontrivial subgroup.

For the proof of Theorem 2.2, we will need to make use of the Kemperman critical pair theory (though an isoperimetric approach would also be viable, see e.g. [21]). We begin by stating Kneser’s Theorem [26] [27] [30] [33].

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

$$\left| \sum_{i=1}^n \phi_H(A_i) \right| \geq \sum_{i=1}^n |\phi_H(A_i)| - n + 1,$$

where $H = H(\sum_{i=1}^n A_i)$.

Note that $|H| \cdot \phi_H(A_i) = |A_i + H|$. Also, if $H = H(A + B)$ and $\rho = |A + H| - |A| + |B + H| - |B|$ is the number of holes in A in B (by a hole in A , with respect to H , we mean an element from $(A + H) \setminus A$), then Kneser’s Theorem implies $|A + B| \geq |A| + |B| - |H| + \rho$. Consequently, if either A or B contains a unique element from some H -coset, then $|A + B| \geq |A| + |B| - 1$.

More generally, if $\rho = \sum_{i=1}^n (|A_i + H| - |A_i|)$ is the total number holes in the A_i , then $|\sum_{i=1}^n A_i| \geq \sum_{i=1}^n |A_i| - (n - 1)|H| + \rho$.

Next we continue with the following two simple cases of Kemperman’s Structure Theorem [25, Theorem 5.1]. The reader is directed to [15] [19] [20] [29] for more detailed exposition regarding Kemperman’s critical pair theory, including the (somewhat lengthy and involved) statement of the Kemperman Structure Theorem. In what follows, a set $A \subseteq G$ is *quasi-periodic* if there is a nontrivial subgroup H (the *quasi-period*) such that $A = A_0 \cup A_1$ with A_0 nonempty and H -periodic and A_1 a subset of an H -coset.

Lemma 3.1. *Let A_1, \dots, A_n , be a collection of $n \geq 3$ finite subsets in an abelian group G of order m with $0 \in A_i$ and $|A_i| \geq 2$ for all i . Moreover, suppose each A_i is not quasi-periodic and $\langle A_i \rangle = G$. If $\sum_{i=1}^n A_i$ is aperiodic and*

$$(2) \quad \left| \sum_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - n + 1,$$

then the A_i are arithmetic progressions with common difference.

Proof. We provide a short proof using the formulation (including relevant notation and definitions) of Kemperman’s Structure Theorem as given in [25, Theorem 5.1].

Since $\sum_{i=1}^n A_i$ is aperiodic, it follows that $A_j + A_k$ is aperiodic for any $j \neq k$. Thus Kneser’s Theorem implies $|A_j + A_k| \geq |A_j| + |A_k| - 1$, and we must have

$$|A_j + A_k| = |A_j| + |A_k| - 1,$$

else Kneser’s Theorem would imply

$$\left| \sum_{i=1}^n A_i \right| \geq \sum_{\substack{i=1 \\ i \neq j, k}}^n |A_i| + |A_j + A_k| - (n - 1) + 1 \geq \sum_{i=1}^n |A_i| - n + 2,$$

contradicting (2). Thus we can apply Kemperman’s Structure Theorem to an arbitrary pair A_j and A_k with $j \neq k$.

Since A_i is not quasi-periodic, for $i = j, k$, we conclude from the Kemperman Structure Theorem that (A_j, A_k) is an elementary pair of type (I), (II), (III) or (IV). Since $|A_j|, |A_k| \geq 2$ and $A_j + A_k$ is aperiodic, we cannot have type (I) or (III). Since $n \geq 3$, since $|A_i| \geq 2$ for all i , and since $\sum_{i=1}^n A_i$ is aperiodic (and in particular, $|\sum_{i=1}^n A_i| < |G|$), it follows in view of Kneser’s Theorem that $|A_j + A_k| < |\sum_{i=1}^n A_i| < |G|$. Thus, in view of $0 \in A_j$ and $\langle A_j \rangle = G$, it follows that we cannot have type (IV) and that $|A_j|, |A_k| \leq |G| - 2$. Hence (A_j, A_k) is an elementary pair of type (II), i.e., A_j and A_k are arithmetic progressions of common difference (say) $d \in G$. Note $\text{ord}(d) = |G|$, since $\langle A_j \rangle = G$. Since the difference d of an arithmetic progression A is unique up to sign when $2 \leq |A| \leq \text{ord}(d) - 2$, since $2 \leq |A_j|, |A_k| \leq |G| - 2$, and since A_j and A_k with $j \neq k$ were arbitrary, it now follows that all the A_i are arithmetic progressions of common difference d , as desired. \square

Lemma 3.2. *Let G be an abelian group and let $A, B \subseteq G$ be finite with $|A| \geq 2$ and $|B| = 2$. If neither A nor B is quasi-periodic and $|A + B| = |A| + |B| - 1$, then A and B are arithmetic progressions of common difference.*

Proof. This follows immediately from the Kemperman Structure Theorem or may be taken as an easily verified observation. \square

The following result from [14] will also be used.

Theorem D. *Let G be a nontrivial, finite abelian group, $S \in \mathcal{F}(G)$ and $W = w_1 \cdot \dots \cdot w_n \in \mathcal{F}(\mathbb{Z})$ such that $\sigma(W) \equiv 0 \pmod{\exp(G)}$ and $|S| \geq |W| + |G| - 1$. If S has an n -setpartition $A = A_1 \cdot \dots \cdot A_n$ such that*

$|w_i \cdot A_i| = |A_i|$ for all $i \in [1, n]$, then there exists a nontrivial subgroup H of G and an n -setpartition $A' = A'_1 \cdot \dots \cdot A'_n$ of S such that

$$H \subseteq \sum_{i=1}^n w_i \cdot A'_i \subseteq \Sigma_{|W|}(W, S) \quad \text{and} \quad |w_i \cdot A'_i| = |A'_i| \quad \text{for all } i \in [1, n].$$

We now proceed with the proof of Theorem 2.2.

Proof. Let $m = \exp(G)$ and $n = |W|$. By considering G as a $\mathbb{Z}/m\mathbb{Z}$ -module (for notational convenience), we may w.l.o.g. consider W as a sequence from $\mathbb{Z}/m\mathbb{Z}$, say w.l.o.g. $W = w_1 \cdot \dots \cdot w_n$, where $\text{ord}(w_i) = m$ for $i \leq n - 1$ (in view of the hypothesis $\gcd(w_i, \exp(G)) = 1$ for $i \leq n - 1$). Observe that we may assume $|S| = n + |G| - 1$ (since $n \geq 2$, so that, if $|\text{supp}(S)| \geq 3$, then we can remove terms from S until there are only $n + |G| - 1 \geq 3$ left while preserving that $|\text{supp}(S)| \geq 3$), and that there are distinct $x, y \in G$ with $x^n y^n |S$ such that $w_n(x - y) = 0$, else Theorem D implies the theorem (as if such is not the case, then there would exist, in view of $h(S) \leq |W| = n$, an n -setpartition of S satisfying the hypothesis of Theorem D). Since $\sigma(W) = 0$, we may w.l.o.g. by translation assume $x = 0$. If $\text{ord}(y) < |G|$, then, since $w_i y \in \langle y \rangle$ and

$$n - 1 \geq \frac{|G|}{2} - 1 \geq \text{ord}(y) - 1 = \text{ord}(w_i y) - 1,$$

for $i \leq n - 1$ (in view of $\text{ord}(w_i) = m$ for $i \leq n - 1$), it would follow in view of Kneser's Theorem that

$$\langle y \rangle = \sum_{i=1}^{n-1} \{0, w_i y\} = \sum_{i=1}^{n-1} w_i \cdot \{0, y\} + w_n \cdot 0 \subseteq \Sigma_{|W|}(W, S),$$

as desired. Therefore we may assume $\text{ord}(y) = |G|$, whence w.l.o.g. G is cyclic, $m = |G|$ and $y = 1$. Consequently, since $\sigma(W) = 0$, $w_n(x - y) = 0$ and $x = 0$, it follows that $w_n = 0$ and $\sigma(W') = 0$, where $W' := W w_n^{-1}$.

Since $n \geq \frac{m}{2}$, $0^n 1^n |S$ and $|S| = n + m - 1$, it follows that

$$(3) \quad 2n \leq |S| \leq 3n - 1.$$

Hence let $A = A_1 \cdot \dots \cdot A_{n-1}$ be an arbitrary $(n - 1)$ -setpartition of $S' := S(01)^{-1}$. Note $\{0, 1\} \subseteq A_i$ for all i , so that

$$(4) \quad 0 \in \sum_{i=1}^{n-1} w_i \cdot A_i + w_n \cdot 0 \subseteq \Sigma_{|W|}(W, S).$$

Thus we may assume $\sum_{i=1}^{n-1} w_i \cdot A_i$ is aperiodic, else the proof is complete. Consequently, Kneser's Theorem and $\text{ord}(w_i) = m$ for $i \leq n - 1$ imply

$\left| \sum_{i=1}^{n-1} w_i \cdot A_i \right| \geq \sum_{i=1}^{n-1} |A_i| - (n-1) + 1 = m-1$, whence

$$(5) \quad \left| \sum_{i=1}^{n-1} w_i \cdot A_i \right| = \sum_{i=1}^{n-1} |A_i| - (n-1) + 1 = m-1,$$

else $G \subseteq \sum_{i=1}^{n-1} w_i \cdot A_i + w_n \cdot 0 \subseteq \Sigma_{|W|}(W, S)$, as desired.

Suppose m is not a prime power. Then we can choose $H, K \leq G$ with $|H|$ and $|K|$ distinct primes, so that $H \cap K = \{0\}$. In view of (5), it follows that $\Sigma_{|W|}(W, S)$ is missing exactly one element, which in view of (4) cannot be zero. Consequently, either $H \subseteq \Sigma_{|W|}(W, S)$ or $K \subseteq \Sigma_{|W|}(W, S)$, as desired. So we may assume $m = p^r$ for some prime p and $r \geq 1$.

Claim A: If $x(-x)|W'$, for some $x \in \mathbb{Z}/m\mathbb{Z}$, then $|S| = 2n$ or $|S| = 3n-1$, else the proof is complete.

Proof. Suppose the claim is false. Thus (3) implies $2n+1 \leq |S| \leq 3n-2$, so that $n \geq 3$, and it follows by the pigeonhole principle that $|A_i| \leq 2$ for some i , say $i = n-1$, and that $|A_j| \geq 3$ for some j , say $j = n-2$, whence we may w.l.o.g. assume $x = w_{n-2}$ and $-x = w_{n-1}$. Let $g \in A_{n-2} \setminus \{0, 1\}$ (in view of $|A_{n-2}| = |A_j| \geq 3$). Observe that

$$(6) \quad \sum_{i=1}^{n-2} w_i \cdot A_i + w_{n-1} \cdot (A_{n-1} \cup \{g\}) = \left(\sum_{i=1}^{n-1} w_i \cdot A_i \right) \cup \left(\sum_{i=1}^{n-3} w_i \cdot A_i + w_{n-2} \cdot (A_{n-2} \setminus \{g\}) + w_{n-1} \cdot (A_{n-1} \cup \{g\}) \right) \cup \left(\sum_{i=1}^{n-3} w_i \cdot A_i + w_{n-2}g + w_{n-1}g \right).$$

Note that the first two terms of the right hand side of (6) are contained in $\Sigma_{|W|}(W, S)$. Moreover,

$$w_{n-2}g + w_{n-1}g = xg + (-x)g = 0 = w_{n-2} \cdot 0 + w_{n-1} \cdot 0 \in w_{n-2} \cdot A_{n-2} + w_{n-1} \cdot A_{n-1},$$

so that the third term of the right hand side of (6) is contained in $\sum_{i=1}^{n-1} w_i \cdot A_i + w_n \cdot 0 \subseteq \Sigma_{|W|}(W, S)$ as well. Consequently, it follows from (6) that

$$(7) \quad \sum_{i=1}^{n-2} w_i \cdot A_i + w_{n-1} \cdot (A_{n-1} \cup \{g\}) \subseteq \Sigma_{|W|}(W, S).$$

However, since $\sum_{i=1}^{n-1} w_i \cdot A_i$ is aperiodic and $w_{n-1}g \notin w_{n-1} \cdot A_{n-1}$ (in view of $\text{ord}(w_{n-1}) = m$, $|A_{n-1}| = |A_i| = 2$, and $\{0, 1\} \subseteq A_i$), it follows from Kneser's theorem that

$$\left| \sum_{i=1}^{n-2} w_i \cdot A_i + w_{n-1} \cdot (A_{n-1} \cup \{g\}) \right| > \sum_{i=1}^{n-1} |A_i| - (n-1) + 1 = m - 1.$$

Thus (7) implies that $G \subseteq \Sigma_{|W|}(W, S)$, as desired, completing the proof of Claim A. □

If $n = 2$, then $\sigma(W') = 0$ implies $w_1 = 0$, contradicting $\text{ord}(w_i) = m$ for $i \leq n - 1$. Therefore we may assume $n \geq 3$.

Suppose $|S| = 2n$ (so that $S = 0^n 1^n$). Since $|S| = n + m - 1 = 2n$ and $n \geq 3$, it follows that $m = n + 1 \geq 4$. In view of (5) and Lemmas 3.1 and 3.2, it follows that each $w_i \cdot A_i = w_i \cdot \{0, 1\} = \{0, w_i\}$ is an arithmetic progression with common difference. Consequently, it follows that $w_i = \pm w_j$ for all $i, j \leq n - 1$. Since $n - 1 < m$, since $\sigma(W') = 0$, and since $\text{ord}(w_i) = m$ for all $i \leq n - 1$, it follows that the w_i cannot all be equal. As a result, $w_i = \pm w_j$ for all $i, j \leq n - 1$ implies that $w_i = \pm x$ for all $i \leq n - 1$, with $(x)(-x)|W'$ (for some $x \in \mathbb{Z}/m\mathbb{Z}$), whence $\sigma(W') = 0$ further implies that $W' = x^{(n-1)/2}(-x)^{(n-1)/2}$ with $n - 1$ even. Hence, since $m = n + 1$ is a prime power, it follows that $m = 2^r$, and we see that (ii) holds. So we may assume $|S| > 2n$.

Suppose $n = 3$. Then $\sigma(W') = 0$ implies that $w_1 = -w_2$. Thus, since $2n < |S|$ and $x(-x)|W'$, where $x = w_1$, it follows in view of Claim A that $|S| = 3n - 1 = 8$. Since $|S| = n + m - 1 = m + 2$, this implies that $m = 6$, contradicting that m is a prime power. So we may assume $n \geq 4$.

In view of (3), choose A such that $|A_i| \in \{2, 3\}$ for all i (possible by the remarks from Section 1). If, for some j , there is $g \in A_j \setminus \{0, 1\}$ such that $\{x, g\}$ is a coset of a cardinality two subgroup H , where $x \in \{0, 1\}$, then

$$\sum_{\substack{i=1 \\ i \neq j}}^{n-1} w_i x + w_j \cdot \{x, g\} + w_n \cdot 0$$

is an H -periodic subset of $\Sigma_{|W|}(W, S)$ that contains $\sum_{i=1}^{n-1} w_i x = \sigma(W') \cdot x = 0$; thus $H \subseteq \Sigma_{|W|}(W, S)$, as desired. Therefore we may assume otherwise, and consequently that no A_j is quasi-periodic (in view of $|A_j| \leq 3$ and $\sum_{i=1}^{n-1} A_i$ aperiodic).

As a result, it follows, in view of $n \geq 4$, (5) and Lemma 3.1, that the $w_i \cdot A_i$ are all arithmetic progressions of common difference. Thus each A_i is an arithmetic progression of length two or three that contains $\{0, 1\}$. Hence, since $n \geq 4$ and $n + m - 1 = |S| > 2n$, so that

$$m \geq 5,$$

it follows that each A_i is an arithmetic progression with difference 1 or $\frac{m+1}{2}$ (which both are of order m), and thus each $w_i \cdot A_i$ is an arithmetic progression with difference w_i or $w_i \cdot \frac{m+1}{2}$.

Thus, since $n - 1 \geq 3$, it follows by the pigeonhole principle that there is a pair A_j and A_k , with $j \neq k$, that are arithmetic progressions with common difference d , where $\text{ord}(d) = m$. Thus $w_j \cdot A_k$ and $w_k \cdot A_k$ are arithmetic progression with common difference $w_j d = \pm w_k d$, implying $w_j = \pm w_k$ (since $\text{ord}(d) = m$). Since the indexing for the w_i was arbitrary, then, by applying this argument to all possible permutations of the indices of the w_i (leaving w_n fixed), we conclude that $w_i = \pm w_j$ for all $i, j \leq n - 1$. As in the case $|S| = 2n$, we cannot have all the w_i , with $i \leq n - 1$, equal to each other (in view of $\sigma(W') = 0$ and $n - 1 < m = \text{ord}(w_i)$), whence $W = x^{(n-1)/2}(-x)^{(n-1)/2}0$ and n is odd, for some $x \in \mathbb{Z}/m\mathbb{Z}$.

Thus, from claim A and $|S| > 2n$, we infer that $n + m - 1 = |S| = 3n - 1$, implying $2n = m$. Hence m is even. Thus, since m is a prime power, it follows that $m = 2^r$, whence $2n = m = 2^r \geq 5$ implies that n is even, a contradiction, completing the proof. \square

4. On $d^*(G)$

The main goal of this section is to prove the following pair of seemingly innocuous lemmas, which will be needed for the proof of Theorem 2.4. Lemma 4.1 should be compared with the similar [11, Proposition 5.1.11], whose proof is much easier.

Lemma 4.1. *If G is a finite abelian group and $H \leq G$, then*

$$d^*(H) + d^*(G/H) \leq d^*(G).$$

Lemma 4.2. *Let G be a finite abelian group, let $A \subseteq G$ with $|A| \geq 2$, let $H = \langle -a_0 + A \rangle$, where $a_0 \in A$, and let $W = w_1 \cdot \dots \cdot w_{d^*(H)}$ be a sequence of integers relatively prime to $\exp(H)$. Then*

$$\sum_{i=1}^{d^*(H)} w_i \cdot A = \left(\sum_{i=1}^{d^*(H)} w_i \right) a_0 + H.$$

We first gather some basic results from algebra. Proposition 4.3 is easily proved from the machinery of dual groups, and Proposition 4.4 from the notion and basic properties of independent elements.

Proposition 4.3. *Let G be a finite abelian group and $H \leq G$. Then there exists $K \leq G$ such that $K \cong G/H$ and $G/K \cong H$.*

Proof. Since finite abelian groups are self-dual [28, Theorem I.9.1], this follows from [28, Corollary I.9.3]. □

Proposition 4.4. *Let G be a finite abelian group, say $G \cong \bigoplus_{i=1}^r C_{m_i} \cong \bigoplus_{i=1}^l \left(\bigoplus_{j=1}^r C_{p_i^{k_{i,j}}} \right)$, with $1 < m_1 | \dots | m_r$, each p_i a distinct prime, and $1 \leq k_{i,1} \leq \dots \leq k_{i,r}$. If $H \leq G$, then*

$$H \cong \bigoplus_{i=1}^r C_{m'_i} \cong \bigoplus_{i=1}^l \left(\bigoplus_{j=1}^r C_{p_i^{k'_{i,j}}} \right),$$

with $1 \leq m'_1 | \dots | m'_r$ and $m'_i | m_i$ and $0 \leq k'_{i,1} \leq \dots \leq k'_{i,r}$ and $k'_{i,j} \leq k_{i,j}$, for all i and j . Moreover, if $m'_s = m_s$ for some s , then $k'_{i,s} = k_{i,s}$ for all i .

Proof. Since $m_j = p_1^{k_{1,j}} p_2^{k_{2,j}} \dots p_l^{k_{l,j}}$ (see [24, Section II.2]), it suffices to show $k'_{i,j} \leq k_{i,j}$ for all i and j . For this, it suffices to consider p -groups (the case $l = 1$). We may assume $k'_{1,1} \leq \dots \leq k'_{1,r}$, and now, if the proposition is false, then $k'_{1,j} > k_{1,j}$ for some j , whence H , and hence also G , contains $r - j + 1$ independent elements of order at least $p_1^{k_{1,j}+1}$, say e_1, \dots, e_{r-j+1} . But now $p_1^{k_{1,j}} e_1, \dots, p_1^{k_{1,j}} e_{r-j+1}$ are $r - j + 1$ independent elements in $p_1^{k_{1,j}} \cdot G$ (the image of G under the multiplication by $p_1^{k_{1,j}}$ map), which has total rank $r^*(p_1^{k_{1,j}} \cdot G)$ at most $r - j$ (in view of $k_{i,1} \leq \dots \leq k_{i,r}$), contradicting that the total rank of a group is the maximal number of independent elements (see [11, Appendix A]). □

The next lemma will provide the key inductive mechanism for the proof of Lemma 4.1.

Lemma 4.5. *Let G be a finite abelian group, say $G \cong \bigoplus_{i=1}^r C_{m_i}$, with $1 < m_1 | \dots | m_r$, and let $H \leq G$, say $H \cong \bigoplus_{i=1}^r C_{m'_i}$, with $1 \leq m'_1 | \dots | m'_r$. If $m'_t = m_t$ for some t , then there exists a subgroup $K \leq H$ such that $K \cong C_{m_t}$ and K is a direct summand in both H and G .*

Proof. Let $G \cong \bigoplus_{i=1}^l \left(\bigoplus_{j=1}^r C_{p_i^{k_{i,j}}} \right)$ and $H \cong \bigoplus_{i=1}^l \left(\bigoplus_{j=1}^r C_{p_i^{k'_{i,j}}} \right)$, with each p_i a distinct prime, $1 \leq k_{i,1} \leq \dots \leq k_{i,r}$ and $0 \leq k'_{i,1} \leq \dots \leq k'_{i,r}$ for all i . In view of Proposition 4.4 and our hypotheses, we have $m'_i | m_i$ and $k'_{i,j} \leq k_{i,j}$, for all i and j , and $k'_{i,t} = k_{i,t}$ for all i . Thus it suffices to prove the lemma for p -groups, and so we assume $m_i = p^{s_i}$ and $m'_i = p^{s'_i}$ for some prime p .

By hypothesis, H contains $r - t + 1$ independent elements f_1, \dots, f_{r-t+1} of order at least $m_t = p^{st}$ (by an appropriate subselection of elements from a basis of H). Let e_1, \dots, e_r be a basis for G with $\text{ord}(e_i) = p^{si}$, and let $f_j = \sum_{i=1}^r \alpha_{j,i} e_i$, where $\alpha_{j,i} \in \mathbb{Z}$. If

$$\text{ord}(f_j) = \text{ord}(\alpha_{j,i} e_i) = \text{ord}(e_i) = p^{st},$$

for some i and j , then $e_1, \dots, e_{i-1}, f_j, e_{i+1}, \dots, e_r$ is also a basis for G , and the result follows with $K = \langle f_j \rangle$. So we may assume otherwise.

Now $f'_1 := p^{st-1} f_1, f'_2 := p^{st-1} f_2, \dots, f'_{r-t+1} := p^{st-1} f_{r-t+1}$ are $r - t + 1$ independent elements in $p^{st-1} \cdot G$. However, in view of the conclusion of the previous paragraph, each $p^{st-1} f_j$ with $\text{ord}(f_j) = p^{st}$ must lie in the span of $p^{st-1} e_{t+1}, \dots, p^{st-1} e_r$ (as $\text{ord}(e_i) \leq p^{st}$ for $i \leq t$).

Let $\phi_L : p^{st-1} \cdot G \rightarrow (p^{st-1} \cdot G)/L$, where $L = \langle p^{st-1} e_1, \dots, p^{st-1} e_t \rangle$, be the natural homomorphism. Then $\phi_L(f'_1), \dots, \phi_L(f'_{r-t+1})$ are $r - t + 1$ independent elements in $\phi_L(p^{st-1} \cdot G)$, as the following argument shows. Take any relation

$$0 = \sum_{i=1}^{r-t+1} \alpha_i \phi_L(f'_i) = \sum_{i \in I} \alpha_i \phi_L(f'_i) + \sum_{i \notin I} \alpha_i \phi_L(f'_i),$$

where $i \in I$ are those indices such that $\text{ord}(f'_i) > p$ (and thus $\text{ord}(f_i) > p^{st}$) and $\alpha_i \in \mathbb{Z}$. Then, in view of the conclusion of the previous paragraph, we see that

$$0 = \sum_{i=1}^{r-t+1} p^{s'} \alpha_i f'_i$$

is a relation in $p^{st-1} \cdot G$, where $s' := \max\{0, 1 - \min\{v_p(\alpha_i) \mid i \in I\}\}$ (here $v_p(\alpha_i)$ is the p -valuation of $\alpha_i \in \mathbb{Z}$). If $s' = 0$, then the independence of the f'_i implies that $\alpha_i f'_i = 0$, and thus $\phi_L(\alpha_i f'_i) = \alpha_i \phi_L(f'_i) = 0$, for all i . If $s' = 1$, then the definition of s' implies that $v_p(\alpha_j) = 0$ for some $j \in I$, whence $\text{ord}(\alpha_j f'_j) > p$ follows from the definition of I . As a result, $p \alpha_j f'_j \neq 0$, contradicting that the f'_i are independent. Thus $\phi_L(f'_1), \dots, \phi_L(f'_{r-t+1})$ are $r - t + 1$ independent elements in $\phi_L(p^{st-1} \cdot G)$, which is a group of total rank at most $r - t$, contradicting that the total rank is the maximal number of independent elements (see [11, Appendix A]). This completes the proof. \square

We can now prove Lemma 4.1.

Proof. If G is cyclic, then $d^*(G) = |G| - 1$, $d^*(H) = |H| - 1$ and $d^*(G/H) = \frac{|G|}{|H|} - 1$. Hence $d^*(G) \geq d^*(H) + d^*(G/H)$ follows from the general inequality $xy \geq x + y - 1$ for $x, y \in \mathbb{Z}_{\geq 1}$. Therefore we may assume $r(G) \geq 2$ and proceed by induction on the rank $r(G) = r$.

Let $G \cong \bigoplus_{i=1}^r C_{m_i}$, $H \cong \bigoplus_{i=1}^r C_{m'_i}$ and $G/H \cong \bigoplus_{i=1}^r C_{m''_i}$, with $1 < m_1 | \dots | m_r$ and $1 \leq m'_1 | \dots | m'_r$ and $1 \leq m''_1 | \dots | m''_r$. In view of Propositions 4.4 and 4.3, we see that $m'_i | m_i$ and $m''_i | m_i$ for all i . Hence, if $m'_i < m_i$ and $m''_i < m_i$ for all i , then $m'_i \leq \frac{1}{2}m_i$ and $m''_i \leq \frac{1}{2}m_i$, whence $m'_i - 1 + m''_i - 1 < m_i - 1$; consequently, summing over all i yields the desired bound $d^*(G) \geq d^*(H) + d^*(G/H)$. Therefore we may assume $m'_s = m_s$ or $m''_s = m_s$ for some s , and in view of Proposition 4.3, we may w.l.o.g. assume $m'_s = m_s$.

Now applying Lemma 4.5, we conclude that there are subgroups $K, H_0 \leq H$ and $G_0 \leq G$ such that $H = K \oplus H_0$ and $G = K \oplus G_0$ with $K \cong C_{m_s}$. Moreover, we can choose the complimentary summand H_0 such that $H_0 \leq G_0$. Note $d^*(H) = d^*(K) + d^*(H_0)$ and $d^*(G) = d^*(K) + d^*(G_0)$, while $G/H = (K \oplus G_0)/(K \oplus H_0) \cong G_0/H_0$, so that $d^*(G_0/H_0) = d^*(G/H)$. Thus $d^*(G) \geq d^*(H) + d^*(G/H)$ follows by applying the induction hypothesis to G_0 with subgroup H_0 . □

Having established Lemma 4.1, we conclude the section with the proof of Lemma 4.2.

Proof. By translation, we may w.l.o.g. assume $a_0 = 0 \in A$ and $H = G$. Since $|A| \geq 2$, we have $\langle A \rangle = H = G$ nontrivial. Let $K \leq H = G$ be the maximal subgroup such that there exists a subset $B \subseteq A$ with $0 \in B$, $K = \langle B \rangle$ and

$$(8) \quad d^*(K) \quad \left| \sum_{i=1}^{d^*(K)} w_i \cdot B \right| = |K|,$$

if such K exists, and otherwise let $K = B = \{0\}$. We may assume $K < H = G$, else the proof is complete.

Since $\langle B \rangle = K \neq G$ and $\langle A \rangle = G$, choose $g \in A \setminus B$ such that $\langle B' \rangle := K' > K$, where $B' = B \cup \{g\}$. Let $L = \langle g \rangle$. Note $K'/K = (K + L)/K \cong L/(K \cap L)$ is cyclic. Hence, in view of Lemma 4.1, we have

$$|K'/K| - 1 = d^*(K'/K) \leq d^*(K') - d^*(K) \leq d^*(G) - d^*(K).$$

Thus Kneser's Theorem implies, in view of $w_i g \in L$ and $\gcd(w_i, \exp(H)) = 1$ (so that $\text{ord}(w_i g) = \text{ord}(g)$) and $\langle g \rangle = L$ (so that $\langle \phi_K(g) \rangle = K'/K = (K + L)/K$), that

$$\left| \sum_{i=d^*(K)+1}^{d^*(K')} \phi_K(w_i \cdot B') \right| = \left| \sum_{i=d^*(K)+1}^{d^*(K')} \phi_K(w_i \cdot \{0, g\}) \right| = |K'/K|,$$

and thus from (8) it follows that

$$\left| \sum_{i=1}^{d^*(K')} w_i \cdot B' \right| = |K'|,$$

contradicting the maximality of K , and completing the proof. □

5. Theorems 2.4 and 2.5

Theorems 2.4 and 2.5 will be derived by an inductive argument from the following result. (Theorem E is easily derived from the proof of [16] using the both the modifications mentioned in [14] and those in [17]; see [19] for a unified presentation of the arguments, though the condition $\gcd(w, \text{ord}(g)) = 1$, for all $w \in \text{supp}(W)$ and all torsion elements $g \in \text{supp}(S)$, is misstated in the statement of Theorem 3.1 in [19], and is corrected below.)

Theorem E. *Let G be an abelian group, let $S, S' \in \mathcal{F}(G)$ with $S'|S$, and let $W = w_1 \cdot \dots \cdot w_n \in \mathcal{F}(\mathbb{Z})$ be a sequence of integers such that $h(S') \leq n \leq |S'|$ and $\gcd(w, \text{ord}(g)) = 1$ for all $w \in \text{supp}(W)$ and all torsion elements $g \in \text{supp}(S)$. Then there exists $H \leq G$ and an n -setpartition $A = A_1 \cdot \dots \cdot A_n$ of a subsequence S'' of S such that $\sum_{i=1}^n w_i \cdot A_i$ is H -periodic, $|S'| = |S''|$, and*

$$(9) \quad \left| \sum_{i=1}^n w_i \cdot A_i \right| \geq ((N - 1)n + e + 1)|H|,$$

where

$$N = \frac{1}{|H|} \left| \bigcap_{i=1}^n (A_i + H) \right| \quad \text{and} \quad e = \sum_{j=1}^n (|A_j| - |A_j \cap \bigcap_{i=1}^n (A_i + H)|).$$

Furthermore, if H is nontrivial, then $N \geq 1$ and $\text{supp}(S''^{-1}S) \subseteq \bigcap_{i=1}^n (A_i + H)$.

The following basic result, which is a simple consequence of the pigeon-hole principle, will be used in the proof [11, Lemma 5.2.9].

Proposition F. *Let G be a finite abelian group and let $A, B \subseteq G$ be nonempty subsets. If $|A| + |B| \geq |G| + 1$, then $A + B = G$.*

We proceed with the proof of Theorems 2.4 and 2.5 simultaneously.

Proof. Observe that the hypotheses of Theorem 2.4 allow us to apply Theorem E with $G, S'|S, W = w_1 \cdot \dots \cdot w_n$ and n the same in both theorems. Let $H, S'', A = A_1 \cdot \dots \cdot A_n, N$ and e be as given by Theorem E. If H is trivial, then (9) implies $|\sum_{i=1}^n w_i \cdot A_i| \geq |S'| - n + 1$, and if $H = G$, then $\sum_{i=1}^n w_i \cdot A_i$ being H -periodic implies $|\sum_{i=1}^n w_i \cdot A_i| = |G|$; in either case, (i) follows. Therefore we may assume H is a proper, nontrivial subgroup. This completes the case when $|G|$ is prime in Theorem 2.4.

Concerning Theorem 2.5(i), in view of $h(S') \leq n$ and $|T^{-1}S| \geq n - d^*(G) + |S| - |S'|$, it is easily seen that the setpartition $B_1 \cdot \dots \cdot B_{d^*(G)}$ of T can be extended to a setpartition $A_1 \cdot \dots \cdot A_n$ of a sequence $S'''|S$, with $B_i \subseteq A_i$ for $i \leq d^*(G)$, $T|S'''$ and $|S'''| = |S'|$, by the following argument. Begin with $A_i = B_i$ for $i \leq d^*(G)$ and $A_i = \emptyset$ for $d^*(G) < i \leq n$. If $W|S$ are all terms with multiplicity at least n and $W' = \prod_{g \in \text{supp}(W)} g^n$, then augment the sets A_i so that $\text{supp}(W) \subseteq A_i$ for all i (that is, simply include each $g \in \text{supp}(W)$ in each set A_i if it was not already there). We must have $|W'^{-1}W| \leq |S| - |S'|$, else it would have been impossible that a subsequence of S with length $|S'|$ had an n -setpartition, which we know is the case since $h(S') \leq n \leq |S'|$. All remaining terms in $T^{-1}W^{-1}S$ have multiplicity at most $n - 1$, and so we can distribute all but $|S| - |S'| - |W'^{-1}W|$ of them among the A_i so that no A_i contains two equal terms, always choosing to place an element in an empty set if available. Since $|T^{-1}S| \geq n - d^*(G) + |S| - |S'|$, we are either assured that there are enough terms to fill all empty sets in this manner, or that we can move some of the terms from W' (but not from T) placed in the A_i with $i \leq d^*(G)$ so that this is the case, and then the resulting A_i give the n -setpartition with the desired properties.

Consequently, (i) in Theorem 2.5 is trivial, and since the only nontrivial subgroup of G , when $|G|$ is prime, is G , we see that the case $|G|$ prime is complete for Theorem 2.5 as well.

We now proceed by induction on the number of prime factors of $|G|$. We first show that (i) failing in Theorem 2.4 implies the hypotheses of Theorem 2.5 hold (this is Claim B below), from which we infer that Theorem 2.5 implies Theorem 2.4. The remainder of the proof will then be devoted to proving Theorem 2.5 assuming by induction hypothesis that Theorem 2.4 holds in any abelian group G' with $|G'|$ having a smaller number of prime factors than $|G|$.

To this end, we assume (i) fails. Since (i) holds trivially when $n = 1$ (in view of $n \geq h(S')$), we may assume $n \geq 2$. Let $x := |S| - |S'| \geq 0$. Since (i) fails, it follows from (9) that

$$(10) \quad ((N - 1)n + e + 1)|H| \leq |S'| - n.$$

Much of the proof is contained in the following claim.

Claim B: There exists a nontrivial subgroup K , $g' \in G$, and an $d^*(K)$ -setpartition $B = B_1 \cdot \dots \cdot B_{d^*(K)}$ of a subsequence $T|S$ with $T \in \mathcal{F}(g' + K)$, such that

$$(11) \quad \sum_{i=1}^{d^*(K)} w_i \cdot B_i = \left(\sum_{i=1}^{d^*(K)} w_i \right) g' + K$$

and $T^{-1}S$ contains at least $n - d^*(K) + x$ terms from $g' + K$.

Proof. There are two cases.

Case 1: $N \geq 2$. If there does not exist $g' \in \bigcap_{i=1}^n (A_i + H)$ and A_j and A_k such that $j \neq k$ and

$$(12) \quad |A_k \cap (g' + H)| + |A_j \cap (g' + H)| \geq |H| + 1,$$

then it would follow from the pigeonhole principle (since $n \geq 2$) that

$$|S'| = |S''| \leq \frac{1}{2}|H|Nn + e,$$

which combined with (10) implies $((N - 1)n + e)|H| \leq \frac{1}{2}|H|Nn + e - n$, whence

$$|H|nN \leq 2(|H| - 1)(n - e) \leq 2n(|H| - 1),$$

implying $N < 2$, a contradiction. Therefore we may assume such g' and A_j and A_k exist, and w.l.o.g. $j = 1$ and $k = 2$ (by re-indexing the A_i but *not* the w_i ; note we lose the sumset bound given by (9) in doing so, but we will only need the information it implied about the structure of S and not use the bound itself in the remainder of Case 1). By translation we may also assume $g' = 0$.

From Proposition F, (12) and $\gcd(w_i, \exp(G)) = 1$, it follows that

$$(13) \quad |w_1 \cdot (A_1 \cap H) + w_2 \cdot (A_2 \cap H)| = |H|.$$

Let $B_j = A_j \cap \bigcap_{i=1}^n (A_i + H)$ for $j = 1, \dots, n$, and note that $\phi_H(B_i) = \phi_H(B_j)$ for all i and j . Let $K = H + \langle B_i \rangle$ and $T = \prod_{i=1}^{d^*(K)} B_i \in \mathcal{F}(K)$. From the conclusion of Theorem E, we know $T^{-1}S$ contains at least $n - d^*(K) + x$ terms from K (since each A_i intersects $\bigcap_{i=1}^n (A_i + H)$ in at least $N \geq 1$ points and $\text{supp}(S''^{-1}S) \subseteq \bigcap_{i=1}^n (A_i + H)$, both of which were preserved when re-indexing the A_i).

If $d^*(H) \geq 2$, then from (13) and $g' = 0$ we find that

$$(14) \quad H \subseteq \sum_{i=1}^{d^*(H)} w_i \cdot B_i.$$

On the otherhand, if $d^*(H) = 1$, then $|H| = 2$, whence (12) and the pigeonhole principle imply that w.l.o.g. $|A_1 \cap H| = |H|$, and thus (14) holds in this case as well. Since $n \geq d^*(G) \geq d^*(K)$, it follows by Lemma 4.1 that

$$n - d^*(H) \geq d^*(K) - d^*(H) \geq d^*(K/H).$$

Thus, applying Lemma 4.2, taking $\phi_H(B_i)$ for A and G/H for G (recall that $g' = 0$ and $|\phi_H(B_i)| = N \geq 2$), it follows that

$$\sum_{i=d^*(H)+1}^{d^*(K)} \phi_H(w_i \cdot B_i) = K/H,$$

which in view of (14) implies that (11) holds. In view of the conclusion of the previous paragraph, this completes the claim.

Case 2: $N = 1$. Let T be the subsequence of S consisting of all terms from $g + H$, let $T'|T$ be the subsequence consisting of all terms with multiplicity at least $d^*(H)$, and let $B = \text{supp}(T')$. From (10) and Theorem E, it follows that

$$(15) \quad |T| \geq x + |S'| - e \geq (e + 1)|H| + n + x - e \geq n + |H| + x.$$

By translation, we may w.l.o.g. assume $0 \in \text{supp}(T)$, and that $0 \in \text{supp}(T')$ if $\text{supp}(T') \neq \emptyset$. We handle two subcases.

Subcase 2.1: Suppose there exists a subsequence $T_0|T$ with $h(T_0) \leq d^*(H)$ and $|T_0| = d^*(H) + |H| - 1$. Then we can apply the induction hypothesis to $T_0|T$ with G taken to be H and n taken to be $d^*(H)$. Let $B = B_1 \cdot \dots \cdot B_{d^*(H)}$ be the resulting setpartition and T'_0 the resulting subsequence of T . From (15), we see that

$$(16) \quad |T_0'^{-1}T| = |T| - |T'_0| = |T| - |T_0| = |T| - d^*(H) - |H| + 1 \geq n + x - d^*(H).$$

If (i) holds, then $|T_0| = d^*(H) + |H| - 1$ implies that

$$\left| \sum_{i=1}^{d^*(H)} w_i \cdot B_i \right| = |H|,$$

and the claim is complete (in view of (16)) using T'_0 for T and H for K . On the otherhand, if (ii) holds with (say) subgroup $K \leq H$, $g' \in H$ and setpartition $B_1 \cdot \dots \cdot B_{d^*(H)}$, then (11) follows from (ii)(d) (taking T to be the associated sequence to $B_1 \cdot \dots \cdot B_{d^*(K)}$), while (ii)(a) and (15) imply $T_0''^{-1}T$ contains at least

$$d^*(H) - d^*(K) + |T| - |T_0| = -d^*(K) + |T| - |H| + 1 \geq n - d^*(K) + x$$

terms from $g' + K$, whence the claim follows.

Subcase 2.2: There does not exist a subsequence $T_0|T$ with $h(T_0) \leq d^*(H)$ and $|T_0| = d^*(H) + |H| - 1$. Consequently,

$$|\text{supp}(T')|d^*(H) + |T'^{-1}T| \leq d^*(H) + |H| - 2,$$

which, in view of (15), yields

$$(17) \quad |T'| \geq n + x + 2 + (|\text{supp}(T')| - 1)d^*(H).$$

Since $v_g(T') \leq v_g(T) \leq n + x$ for all $g \in G$ (in view of $h(S') \leq n$), it follows that $|T'| \leq (n + x)|\text{supp}(T')|$. Thus, in view of $n \geq d^*(G) \geq d^*(H)$ and $x \geq 0$, we conclude from (17) that $|\text{supp}(T')| \geq 2$.

Let $K = \langle \text{supp}(T') \rangle \leq H$ and let $T_0 := \prod_{g \in \text{supp}(T')} g^{d^*(K)}$ be the subsequence of T' (recall the definition of T') obtained by taking each term

with multiplicity exactly $d^*(K) \leq d^*(H)$. Observe, in view of (17) and $d^*(K) \leq d^*(H)$, that

$$\begin{aligned}
 (18) \quad |T_0^{-1}T'| &= |T'| - |T_0| = |T'| - |\text{supp}(T')|d^*(K) \\
 &\geq n + x + 2 + (|\text{supp}(T')| - 1)(d^*(H) - d^*(K)) - d^*(K) \\
 &\geq n + x - d^*(K).
 \end{aligned}$$

Applying Lemma 4.2 with A taken to be $\text{supp}(T')$, we conclude (recall $0 \in \text{supp}(T')$) that

$$\sum_{i=1}^{d^*(K)} w_i \cdot B_i = K,$$

where $B_i = \text{supp}(T')$ for $i = 1, \dots, d^*(K)$. Hence, in view of (18), we see that the claim follows (taking T to be T_0). \square

Having now established Claim B, we see that it suffices to prove Theorem 2.5 to complete the inductive proofs of Theorems 2.4 and 2.5. Let K be a maximal subgroup satisfying Claim B, and let g', T and $B_1 \cdot \dots \cdot B_{d^*(K)}$ be as given by Claim B. By translation we may w.l.o.g. assume $g' = 0$. Let $S_0|S$ be the subsequence consisting of all terms x with $\phi_K(x) \neq 0$, and let $e := |S_0|$. As remarked earlier, if $K = G$, then Theorem 2.5(i) follows trivially. Therefore assume $K < G$. Observe that Claim B implies

$$(19) \quad |T^{-1}S_0^{-1}S| \geq n - d^*(K) + x.$$

Suppose $h(\phi_K(S_0)) \geq d^*(G/K)$. Then let $g \in \text{supp}(S_0)$ with $v_{\phi_K(g)}(\phi_K(S_0)) \geq d^*(G/K)$ and let $L = K + \langle g \rangle$. By Lemma 4.1, we have

$$(20) \quad d^*(L) \geq d^*(K) + d^*(L/K).$$

In view of (19), $h(\phi_K(S_0)) \geq d^*(G/K) \geq d^*(L/K)$ and $n \geq d^*(G) \geq d^*(L)$, we can find a subsequence $T'|T^{-1}S$ such that $\phi_K(T') = \phi_K(g)^{d^*(L/K)}0^{d^*(L)-d^*(K)}$, and thus such that $(TT')^{-1}S$ contains at least

$$(21) \quad n - d^*(K) + x - (d^*(L) - d^*(K)) = n - d^*(L) + x$$

terms from L . In view of (20), let $B_{d^*(K)+1} \cdot \dots \cdot B_{d^*(L)}$ be a setpartition of T' such that $|B_i| = 2$ and $\phi_K(B_i) = \{0, \phi_K(g)\}$, for $i = d^*(K) + 1, \dots, d^*(K) + d^*(L/K)$, and $|B_i| = 1$ and $\phi_K(B_i) = \{0\}$, for $i = d^*(K) + d^*(L/K) + 1, \dots, d^*(L)$.

Applying Lemma 4.2 to $\{0, \phi_K(g)\}$, we conclude that

$$\left| \sum_{i=d^*(K)+1}^{d^*(K)+d^*(L/K)} \phi_K(w_i \cdot B_i) \right| = |L/K|,$$

and consequently (in view of (11) and (20)) that

$$\left| \sum_{i=1}^{d^*(L)} w_i \cdot B_i \right| = |L|.$$

But now, in view also of (21), we see that the maximality of K is contradicted by L . So we may instead assume $h(\phi_K(S_0)) < d^*(G/K)$.

Let R be a subsequence of $T^{-1}S$ such that $S_0|R$ and $|R| = |S_0| + d^*(G/K)$ (possible in view of (19), $x \geq 0$, $n \geq d^*(G)$ and Lemma 4.1). Moreover, from (19),

$$(22) \quad |(TR)^{-1}S| \geq n + x - d^*(K) - d^*(G/K),$$

with all term of $(TR)^{-1}S$ contained in K (since $S_0|R$).

Since $h(\phi_K(S_0)) < d^*(G/K)$, since $\phi_K(y) = 0$ for $y|S_0^{-1}S$, and since $\phi_K(y) \neq 0$ for $y|S_0$, it follows that $h(\phi_K(R)) \leq d^*(G/K)$. Thus we can apply the induction hypothesis to the subsequence $\phi_K(R)|\phi_K(R)0^{|G/K|-1}$ with $n = d^*(G/K)$ and G taken to be G/K . Let $\phi_K(B_{d^*(K)+1}) \cdot \dots \cdot \phi_K(B_{d^*(K)+d^*(G/K)})$ be the resulting setpartition and $\phi_K(R')$ the resulting sequence, where $R'|R0^{|G/K|-1}$ and $B_{d^*(K)+1} \cdot \dots \cdot B_{d^*(K)+d^*(G/K)}$ is a setpartition of R' . Observe, since $v_0(\phi_K(R)) = d^*(G/K)$, that $\text{supp}(\phi_K(R')^{-1}\phi_K(R)0^{|G/K|-1}) = \{0\}$, and thus that we can w.l.o.g. assume $R' = R$ and likewise that $B_{d^*(K)+1} \cdot \dots \cdot B_{d^*(K)+d^*(G/K)}$ is a setpartition of R .

Suppose (ii) holds and let L/K be the corresponding subgroup. Since $v_0(\phi_K(R)0^{|G/K|-1}) \geq |G/K| - 1$, it follows in view of (ii)(c) that w.l.o.g. $g = 0$ (where g is as given by (ii)). But then (ii)(d) implies

$$\sum_{i=d^*(K)+1}^{d^*(K)+d^*(L/K)} w_i \cdot \phi_K(B_i) = L/K,$$

whence (11) implies

$$\sum_{i=1}^{d^*(K)+d^*(L/K)} w_i \cdot B_i = L.$$

In view of (ii)(a) and (22), it follows that there are still at least

$$(23) \quad n + x - d^*(K) - d^*(G/K) + (d^*(G/K) - d^*(L/K)) = n + x - d^*(K) - d^*(L/K)$$

terms remaining in $(\prod_{i=1}^{d^*(K)+d^*(L/K)} B_i)^{-1}S$ that are contained in L . Thus (in view of Lemma 4.1) by appending on an additional $d^*(L) - d^*(L/K) - d^*(K) \geq 0$ terms B_i , for $i = d^*(K) + d^*(L/K) + 1, \dots, d^*(L)$, with each such new B_i consisting of a single element from L contained in

$(\prod_{i=1}^{d^*(K)+d^*(L/K)} B_i)^{-1} S$ (that is, $\text{supp}(\prod_{i=d^*(K)+d^*(L/K)+1}^{d^*(L)} B_i) \subseteq L$ where we have $\prod_{i=d^*(K)+d^*(L/K)+1}^{d^*(L)} B_i | (\prod_{i=1}^{d^*(K)+d^*(L/K)} B_i)^{-1} S$), we see that

$$\sum_{i=1}^{d^*(L)} w_i \cdot B_i = L$$

and with $(\prod_{i=1}^{d^*(L)} B_i)^{-1} S$ containing at least (in view of (23))

$$n + x - d^*(K) - d^*(L/K) - (d^*(L) - d^*(L/K) - d^*(K)) = n + x - d^*(L)$$

terms from L . Hence L contradicts the maximality of K . So we may assume instead that (i) holds.

As above, let B_i , for $i = d^*(K) + d^*(G/K) + 1, \dots, n$ (in view of (22)), be defined by partitioning, as singleton terms (i.e., $|B_i| = 1$), $n - d^*(K) - d^*(G/K)$ of the terms of the sequence $(\prod_{i=1}^{d^*(K)+d^*(G/K)} B_i)^{-1} S = (TR)^{-1} S$ (which are all from K in view of the comment after (22)).

If

$$(24) \quad \sum_{i=d^*(K)+1}^{d^*(K)+d^*(G/K)} w_i \cdot \phi_K(B_i) = G/K,$$

then (11), $n \geq d^*(G)$ and Lemma 4.1 imply that

$$\sum_{i=1}^{d^*(G)} w_i \cdot B_i = G.$$

Thus, in view of (22), we see that Claim B holds with $K = G$, contrary to assumption. Therefore we can assume (24) fails, which, in view of $|R| = |S_0| + d^*(G/K)$ and (i) holding for $\phi_K(R)$ with $n = d^*(G/K)$, implies that $e := |S_0| \leq |G/K| - 2$ and, in view of (11), that

$$|\sum_{i=1}^n w_i \cdot B_i| \geq (e + 1)|K|.$$

The remaining conclusions for (ii) now follow easily from Claim B holding with K (by the same arguments used for establishing Theorem 2.5(i)), so that (ii) holds for S' with subgroup K , as desired. This completes the proof. □

With the proof of Theorems 2.4 and 2.5 complete, the improvement to Theorem A follows as a simple corollary.

Corollary 5.1. *Let G be a finite abelian group, and let $S \in \mathcal{F}(G)$ with $|S| \geq |G| + d^*(G)$. Then either*

- (i) $\Sigma_{|G|}(S) = G$, or

- (ii) *there exist a proper subgroup $H < G$ and some $g \in G$ such that all but at most $|G/H| - 2$ terms of S are from the coset $g + H$.*

Proof. Let $|S| = |G| + d^*(G) + x$, so $x \geq 0$. We assume (ii) fails for every H and prove (i) holds. Note (ii) failing with H trivial implies $h(S) \leq d^*(G) + x + 1$.

Suppose $h(S) \leq d^*(G) + x$. Then we can apply Theorem 2.4 with $n = d^*(G) + x$, $S = S'$ and $w_i = 1$ for all i . If Theorem 2.4(ii) holds, then Theorem 2.4(ii)(c) implies Corollary 5.1(ii), contrary to assumption. If instead Theorem 2.4(i) holds, then from $|S| = |G| + d^*(G) + x$ we conclude that $\Sigma_{d^*(G)+x}(S) = G$. Since $\Sigma_n(S) = \sigma(S) - \Sigma_{|S|-n}(S)$ holds trivially for any n (there is a natural correspondence between $S_0|S$ and $S_0^{-1}S|S$), it now follows that (i) holds for S , as desired. So we may assume $h(S) = d^*(G) + x + 1$.

By translation, we may w.l.o.g. assume 0 is a term with multiplicity $h(S)$ in S . We may also assume there is a nonzero $g \in G$ with $v_g(S) = v_0(S) = h(S)$, else applying Theorem 2.4 to $0^{-1}S|S$ completes the proof as in the previous paragraph. Let $S'|S$ be a maximal length subsequence with $h(S') = d^*(G) + x$, let $A = \text{supp}(S'^{-1}S)$, and let $K = \langle A \rangle$. Notice $\{0, g\} \subseteq A$. Hence, since $h(S) = d^*(G) + x + 1$, it follows from Lemma 4.2 that the hypotheses of Theorem 2.5 hold with $n = d^*(G) + x$, $S'|S$, K , and $w_i = 1$ and $B_i = A$ for all i . If Theorem 2.5(i) holds, then $|G| = |\Sigma_{d^*(G)+x}(S)| = |\Sigma_{|G|}(S)|$ (as in the case $h(S) \leq d^*(G) + x$), yielding (i). On the otherhand, Theorem 2.5(ii) implies (ii) holds (in view of Theorem 2.4(ii)(c)). Thus the proof is complete. □

Next, the related corollary concerning Conjecture 2.3. Note the coset condition assumed below for H trivial implies $h(S) \leq |S| - |G| + 1$, so the hypothesis $h(S) \leq h \leq |S| - |G| + 1$ is not vacuous. The case $h = |G|$ and $|S| = 2|G| - 1$ in Corollary 5.2 is the result from [32].

Corollary 5.2. *Let G be a finite abelian group, let $S \in \mathcal{F}(G)$, let $h \in \mathbb{Z}$ with $\max\{h(S), d^*(G)\} \leq h \leq |S| - |G| + 1$, and let $W \in \mathcal{F}(\mathbb{Z})$ be a sequence of integers relatively prime to $\exp(G)$ with $|W| \geq h$. Suppose there does not exist a proper subgroup $H < G$ and $g \in G$ such that all but at most $|G/H| - 2$ terms of S are from the coset $g + H$. Then $\Sigma_h(W, S) = G$. In particular, $\Sigma(W, S) = G$*

Proof. The proof is identical to the case $h(S) \leq d^*(G) + x$ in Corollary 5.1 using $n = h$, the only other exception being that the identity $|\Sigma_n(W, S)| = |\Sigma_{|S|-n}(W, S)|$ is not necessarily valid for arbitrary W , S and n , thus preventing the proof of Conjecture 2.3 itself. □

Now we derive Corollary 2.6 from Theorem 2.5.

Proof. Let $m = \exp(G)$, $n = |W|$ and $t = |W'|$. By considering G as a $\mathbb{Z}/m\mathbb{Z}$ -module (for notational convenience), we may w.l.o.g. consider W as a sequence from $\mathbb{Z}/m\mathbb{Z}$, say w.l.o.g. $W = w_1 \cdot \dots \cdot w_n$, where $\text{ord}(w_i) = m$ for $i \leq n - t$ (in view of the hypothesis $\gcd(w, \exp(G)) = 1$ for all $w \in \text{supp}(W'^{-1}W)$). Observe that we may assume $|S| = n + |G| - 1$ and that there are distinct $x, y \in G$ with $x^{n-t+1}y^{n-t+1}|S$, else Theorem D implies the theorem (as if such is not the case, then in view of $h(S) \leq n = |W|$ there would exist a n -setpartition of S with t sets of cardinality one). Since $\sigma(W) = 0$, we may w.l.o.g. by translation assume $x = 0$.

Let $A \subseteq \text{supp}(S)$ be all those elements with multiplicity at least $n - t$, let $K = \langle A \rangle$, let $R|S$ be the maximal subsequence with $\text{supp}(R) = A$, let $T := \prod_{g \in A} g^{d^*(K)}$, and let $T_0 = \prod_{g \in A} g^{n-t}$. Notice $\{0, y\} \subseteq A$. Hence, since $h(S) \leq n$ and $|W| - t = n - t \geq d^*(G)$ by hypothesis, it follows from Lemma 4.2 applied to A that the hypotheses of Theorem 2.5 hold with n taken to be $n - t$, $B_i = A$ for $i = 1, \dots, d^*(K)$, and $S' = T_0(R^{-1}S)|S$.

If $|R| \leq |A|(n - t) + t$, then Theorem D once more completes the proof (as then there exists an n -setpartition of S with at least t sets of cardinality one, in view of $h(S) \leq n$). Therefore $|R| \geq |A|(n - t) + t + 1$, and so

$$(25) \quad |S| - |S''| = |S| - |S'| = |R| - |T_0| \geq t + 1,$$

where S'' is as given by Theorem 2.5. Consequently, if Theorem 2.5(i) holds, then it follows that $\Sigma_{n-t}(W'^{-1}W, S'') = G$ with $|S''^{-1}S| \geq t$, whence $\Sigma_n(W, S) = \Sigma_{|W|}(W, S) = G$ follows, as desired. On the otherhand, if Theorem 2.5(ii) holds, then Theorem 2.4(ii)(a)(d) implies

$$\left(\sum_{i=1}^{n-t} w_i \right) g + H \subseteq \sum_{i=1}^{n-t} w_i \cdot A_i \subseteq \Sigma_{n-t}(W'^{-1}W, S''),$$

where g, H and the A_i are as given by Theorem 2.4(ii), whence (25), $\text{supp}(S''^{-1}S) \subseteq g + H$ (in view of (ii)(a)), and $\sigma(W) = 0$ imply

$$H = \left(\sum_{i=1}^n w_i \right) g + H \subseteq \Sigma_n(W, S) = \Sigma_{|W|}(W, S),$$

as desired. □

Finally, we show Conjecture 2.3 holds when $h(S) \geq D(G) - 1$. For this, we need the following modification of a result from [7].

Lemma 5.3. *Let R be a ring, G an R -module, $W \in \mathcal{F}(R)$ and $S \in \mathcal{F}(G)$ with $|S| \geq |W| + D(G) - 1$. If $v_0(S) = h(S) \geq D(G) - 1$, then*

$$\Sigma(W, S) = \Sigma_{|W|}(W, S).$$

Proof. Let $S'|S$ be the subsequence consisting of all nonzero terms. Let $g \in \Sigma(W, S)$ be arbitrary. Since $\Sigma_{|W|}(W, S) \subseteq \Sigma(W, S)$, we need to show that $g \in \Sigma_{|W|}(W, S)$.

If $g = 0$ and $h(S) \geq |W|$, then $0 \in \Sigma_{|W|}(W, 0^{h(S)}) \subseteq \Sigma_{|W|}(W, S)$ (in view of $v_0(S) = h(S)$), as desired. If $g = 0$ and $h(S) \leq |W| - 1$, then $h(S) \geq D(G) - 1$ implies $|W| \geq D(G)$, while $|S'| \geq |W| + D(G) - 1 - h(S) \geq D(G)$. Thus

$$(26) \quad g \in \Sigma(W, S')$$

follows from the definition of $D(G)$ applied to the sequence $(w_1s_1)(w_2s_2) \cdots (w_{D(G)}s_{D(G)}) \in \mathcal{F}(G)$, where $w_1 \cdots w_{D(G)}|W$ and $s_1 \cdots s_{D(G)}|S'$. On the otherhand, if $g \neq 0$, then (26) holds trivially. Thus we can assume (26) regardless, and we choose $W_1|W$ and $S_1|S'$ such that $W_1 = w_1 \cdots w_t$, $S_1 = s_1 \cdots s_t$ and $g = \sum_{i=1}^t w_i s_i$, with t maximal.

Note $t \leq |W|$. If $t \geq |W| - h(S)$, then $g \in \Sigma_{|W|}(W, S_1 0^{h(S)}) \subseteq \Sigma_{|W|}(W, S)$, as desired. So we may assume

$$(27) \quad t \leq |W| - h(S) - 1.$$

Hence

$$(28) \quad |S_1^{-1}S'| \geq |W| + D(G) - 1 - h(S) - t \geq D(G).$$

Observe, in view of (27) and the hypotheses, that

$$(29) \quad |W_1^{-1}W| = |W| - t \geq h(S) + 1 \geq D(G).$$

Let $S' = s_1 \cdots s_t s_{t+1} \cdots s_{|S|-h(S)}$ and $W = w_1 \cdots w_t w_{t+1} \cdots w_n$. In view of (28) and (29), let

$$T := (w_{t+1}s_{t+1})(w_{t+2}s_{t+2}) \cdots (w_{t+D(G)}s_{t+D(G)}) \in \mathcal{F}(G).$$

Observe $|T| = D(G)$, whence the definition of $D(G)$ implies T has a zero-sum subsequence, say (by re-indexing if necessary) $(w_{t+1}s_{t+1})(w_{t+2}s_{t+2}) \cdots (w_{t+r}s_{t+r})$, where $r \geq 1$. But now the sequences $w_1 \cdots w_{t+r}$ and $s_1 \cdots s_{t+r}$ contradict the maximality of t , completing the proof. \square

Note that Corollary 5.4(ii) failing with H trivially implies $h(S) \leq |G|$ for $|S| \leq 2|G| - 1$, and that $2|G| - 1 \geq |G| + D(G) - 1$ in view of the trivial bound $D(G) \leq |G|$ (see [11]). Thus the restriction $h(S) \leq |G|$ in Corollary 5.4 can be dropped when $|S| \leq 2|G| - 1$, and thus, in particular, when $|S| = |G| + D(G) - 1$.

Corollary 5.4. *Let G be a finite abelian group, $S \in \mathcal{F}(G)$ with $|S| \geq |G| + D(G) - 1$ and $|G| \geq h(S) \geq D(G) - 1$, and let $W \in \mathcal{F}(\mathbb{Z})$ with $|W| = |G|$ and $\gcd(w, \exp(G)) = 1$ for all $w \in \text{supp}(W)$. Then either*

- (i) $\Sigma_{|G|}(W, S) = G$, or

- (ii) *there exist a proper subgroup $H < G$ and some $g \in G$ such that all but at most $|G/H| - 2$ terms of S are from the coset $g + H$.*

Proof. We may w.l.o.g. assume $v_0(S) = h(S)$. Thus our hypotheses allow us to apply Lemma 5.3, whence

$$(30) \quad \Sigma(W, S) = \Sigma_{|G|}(W, S).$$

Since we may assume (ii) fails with H trivial, it follows that $h(S) \leq |S| - |G| + 1$. Consequently, since $|W| = |G| \geq h(S)$, then the result follows from (30) and Corollary 5.2 applied with $h = h(S)$ (in view of $D(G) \geq d^*(G) + 1$). \square

Acknowledgements: We thank F. Kainrath, A. Geroldinger, and W. Schmid, for several helpful conversations regarding Section 4. We also thank the referee for their helpful suggestions.

References

- [1] SUKUMAR DAS ADHIKARI AND PURUSOTTAM RATH, *Davenport constant with weights and some related questions*. *Integers* **6** (2006), A30, 6 pp (electronic).
- [2] SUKUMAR DAS ADHIKARI AND YONG-GAO CHEN, *Davenport constant with weights and some related questions II*. *J. Combin. Theory Ser. A* **115** (2008), no. 1, 178–184.
- [3] N. ALON, A. BIALOSTOCKI AND Y. CARO, *The extremal cases in the Erdős-Ginzburg-Ziv Theorem*. Unpublished.
- [4] A. BIALOSTOCKI, P. DIERKER, D. J. GRYNKIEWICZ, AND M. LOTSPEICH, *On Some Developments of the Erdős-Ginzburg-Ziv Theorem II*. *Acta Arith.* **110** (2003), no. 2, 173–184.
- [5] Y. CARO, *Zero-sum problems—a survey*. *Discrete Math.* **152** (1996), no. 1–3, 93–113.
- [6] P. ERDŐS, A. GINZBURG AND A. ZIV, *Theorem in Additive Number Theory*. *Bull. Res. Council Israel* **10F** (1961), 41–43.
- [7] W. GAO, *Addition theorems for finite abelian groups*. *J. Number Theory* **53** (1995), 241–246.
- [8] W. GAO AND A. GEROLDINGER, *On Long Minimal Zero Sequences in Finite Abelian Groups*. *Periodica Math. Hungar.* **38** (1999), no. 3, 179–211.
- [9] W. GAO AND A. GEROLDINGER, *Zero-sum problems in finite abelian groups: A survey*. *Expositiones Mathematicae*, **24** (2006), no. 4, 337–369.
- [10] W. GAO AND W. JIN, *Weighted sums in finite cyclic groups*. *Discrete Math.* **283** (2004), no. 1–3, 243–247.
- [11] A. GEROLDINGER AND F. HALTER-KOCH, *Non-unique factorizations: Algebraic, combinatorial and analytic theory*. *Pure and Applied Mathematics (Boca Raton)* **278**. Chapman & Hall/CRC, Boca Raton, FL, 2006.
- [12] A. GEROLDINGER AND R. SCHNEIDER, *On Davenport’s Constant*. *J. Combin. Theory, Ser. A* **61** (1992), no. 1, 147–152.
- [13] S. GRIFFITHS, *The Erdős-Ginzburg-Ziv theorem with units*. To appear in *Discrete math.*
- [14] D. J. GRYNKIEWICZ, *A Weighted Erdős-Ginzburg-Ziv Theorem*. *Combinatorica* **26** (2006), no. 4, 445–453.
- [15] D. J. GRYNKIEWICZ, *Quasi-periodic Decompositions and the Kemperman Structure Theorem*, *European J. Combin.* **26** (2005), no. 5, 559–575.
- [16] D. J. GRYNKIEWICZ, *On a Partition Analog of the Cauchy-Davenport Theorem*. *Acta Math. Hungar.* **107** (2005), no. 1–2, 161–174.
- [17] D. J. GRYNKIEWICZ, *On a conjecture of Hamidoune for subsequence sum.*, *Integers* **5** (2005), no. 2, A7, 11 pp. (electronic).
- [18] D. J. GRYNKIEWICZ AND R. SABAR, *Monochromatic and zero-sum sets of nondecreasing modified diameter*. *Electron. J. Combin.* **13** (2006), no. 1, Research Paper 28, 19 pp. (electronic).

- [19] D. J. GRYNKIEWICZ, *Sumsets, Zero-sums and Extremal Combinatorics*. Ph. D. Dissertation, Caltech (2005).
- [20] D. J. GRYNKIEWICZ, *A Step Beyond Kemperman's Structure Theorem*. Preprint (2007).
- [21] Y. O. HAMIDOUNE AND A. PLAGNE, *A new critical pair theorem applied to sum-free sets in abelian groups*. *Comment. Math. Helv.* **79** (2004), no. 1, 183–207.
- [22] Y. O. HAMIDOUNE, *On weighted sequence sums*. *Comb. Prob. Comput.* **4** (1995), 363–367.
- [23] Y. O. HAMIDOUNE, *On weighted sums in abelian groups*. *Discrete Math.* **162** (1996), 127–132.
- [24] T. HUNGERFORD, *Algebra*. Springer-Verlag, New York, 1974.
- [25] J. H. B. KEMPERMAN, *On Small Sumsets in an Abelian Group*. *Acta Math.* **103** (1960), 63–88.
- [26] M. KNESER, *Abschätzung der asymptotischen Dichte von Summenmengen*. *Math. Z.* **58** (1953), 459–484.
- [27] M. KNESER, *Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen*. *Math. Z.* **64** (1955), 429–434.
- [28] S. LANG, *Algebra*. Third edition, Yale University, New Haven, CT, 1993.
- [29] V. LEV, *Critical pairs in abelian groups and Kemperman's structure theorem*. *Int. J. Number Theory* **2** (2006), no. 3, 379–396.
- [30] M. NATHANSON, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. *Graduate Texts in Mathematics* **165**, Springer-Verlag, New York, 1996.
- [31] J. E. OLSON, *An addition theorem for finite abelian groups*. *J. Number Theory* **9** (1977), no. 1, 63–70.
- [32] O. ORDAZ AND D. QUIROZ, *Representation of group elements as subsequences sums*. *Discrete Mathematics* **308** (2008), no. 15, 3315–3321.
- [33] T. TAO AND V. VU, *Additive Combinatorics*. *Cambridge Studies in Advanced Mathematics* **105**, Cambridge University Press, Cambridge, 2006.

David J. GRYNKIEWICZ
 Institut für Mathematik und Wissenschaftliches Rechnen
 Karl-Franzens-Universität Graz
 Heinrichstraße 36
 8010 Graz, Austria.

Luz E. MARCHAN
 Departamento de Matemáticas
 Decanato de Ciencias y Tecnologías
 Universidad Centroccidental Lisandro Alvarado
 Barquisimeto, Venezuela.

Oscar ORDAZ
 Departamento de Matemáticas y Centro ISYS
 Facultad de Ciencias
 Universidad Central de Venezuela
 Ap. 47567
 Caracas 1041-A, Venezuela.