Unique Sums and Differences in Finite Abelian Groups

Ka Hin Leung
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore [*]

Bernhard Schmidt
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371
Republic of Singapore [†]

May 13, 2021

[*] Ka Hin Leung's research is supported by grant No. R-146-000-158-112, Ministry of Education, Singapore

[†] This research is supported by the Ministry of Education, Singapore, under its Academic Research Fund Tier 1 (RG27/18)

Abstract

Let A, B be subsets of a finite abelian group G. Suppose that $A + B$ does not contain a unique sum, i.e., there is no $g \in G$ with a unique representation $g = a+b$, $a \in A$, $b \in B$. From such sets A, B, sparse linear systems over the rational numbers arise. We obtain a new determinant bound on invertible submatrices of the coefficient matrices of these linear systems. Under the condition that $|A|+|B|$ is small compared to the order of G, these bounds provide essential information on the Smith Normal Form of these coefficient matrices. We use this information to prove that A and B admit coset partitions whose parts have properties resembling those of A and B. As a consequence, we improve previously known sufficient conditions for the existence of unique sums in $A + B$ and show how our structural results can be used to classify sets A and B for which $A + B$ does not contain a unique sum when $|A| + |B|$ is relatively small. Our method also can be applied to subsets of abelian groups which have no unique differences.

Keywords: Finite abelian groups, sumsets, sparse linear systems, Smith Normal Form

Mathematics Subject Classification: 11B13 (primary), 15A15 (secondary)

1 Introduction

Let A, B be subsets of a finite abelian group G. If there is $g \in G$ such that there is exactly one pair (a, b), $a \in A$, $b \in B$ with $g = a + b$, we say that $A + B$ *contains a unique sum*. Here $A + B = \{a + b : a \in A, b \in B\}$. Unique differences in $A - B$ are defined similarly. In the case of a single set A, if there is $g \in G$ such that there is exactly one pair (a, a'), $a, a' \in A$, with $g = a - a'$, we say that *A has a unique difference*. Similarly, *A has a unique sum* if there is $g \in G$ such that there is exactly one pair (a, a'), $a, a' \in A$, with $g = a + a'$.

Sets with *no* unique sum or difference arise in a variety of contexts, for instance, cyclotomic integers of small modulus [12, 13], field extensions [3], spectral gaps of subsets of $\mathbb{F}_p$ [4], balanced sets [14, 15, 16], and circulant weighing matrices [9]. Thus the main objective of the investigation of these objects is to understand the structure of sets with *no* unique sum or difference and to find necessary conditions for their existence. In fact, in Sections 2 and 3, we obtain such structural results based on a detailed analysis of the arising sparse equations by employing methods from linear algebra. In Section 4, we derive new necessary conditions for the existence of sets with no unique sum or difference. Section 5 contains an application of our main result to circulant weighing matrices. Finally, in Section 6, we provide an example that demonstrates how our structural results can be used to classify sets A and B for which $A+B$ does not contain a unique sum when $|A|+|B|$ is relatively small.

We usually will assume that the sets A and B under consideration both contain the identity element of G. This assumption is not restrictive: Let $a,b \in G$ be arbitrary. Then $A+B$ contains a unique sum if and only if $(A-a)+(B-b)$ contains a unique sum. Similarly, A has a unique difference if and only if $A-a$ has a unique difference. We denote the cyclic group of order v by C_v and identify C_v with $\{0,\ldots,v-1\}$ (with addition modulo v as group operation).

It seems that the problem of unique differences was first mentioned by Straus [18], who in turn attributed it to W. Feit. Straus proved that, for a prime p, a subset A of C_p has a unique difference if $p \geq 4^{|A|}+1$. His result was generalized and strengthened by Browkin, Divis, and Schinzel [3] who proved the following.

Result 1. *Let p be a prime and $A, B \subset C_p$.*

(a) If $p > \min\{2^{|A|+|B|-2}, |A|^{|B|-1}, |B|^{|A|-1}\}$, then $A+B$ contains a unique sum.

(b) If $p > 2^{|A|-1}$, then A has a unique difference and a unique sum.

Lev [11] generalized and partially strengthened Result 1 as follows.

Result 2. *Let A, B be subsets of a finite abelian group G and let p be smallest prime divisor of $|G|$.*

(a) If $p > 2^{|A|+|B|-3}$, then $A+B$ contains a unique sum.

(b) If $p > 2^{|A|-1}$, then A has a unique difference.

Our aim is to improve Results 1 and 2 in the case where G is not of prime power order. In this vein, we obtain the following theorem. For a subset A of a group G, let $\langle A\rangle$ denote the subgroup of G generated by A.

Theorem 3. *Let G be a finite abelian group, and let A, B be subsets of G that both contain the identity element of G. Let p be the smallest prime divisor of the order of G.*

(a) *If $p > (\sqrt[4]{12})^{|A|+|B|-2}$, then $A + B$ contains a unique sum.*

(b) *If $p > (\sqrt[8]{12})^{|A|+|B|-2}$ and both $|\langle A\rangle|$ and $|\langle B\rangle|$ are not prime, then $A + B$ contains a unique sum.*

(c) *If $p > (\sqrt[4]{12})^{|A|}$ and $|\langle A\rangle|$ is not a prime, then A has a unique difference.*

The proof of Theorem 3 has two key ingredients:

(i) A determinant bound on coefficient matrices of linear systems arising from A and B.

(ii) Viewing the arising linear systems as equations over $\mathbb{Q}$ and use of the Smith Normal Form of the corresponding coefficient matrices to obtain information on their solution set.

We take care of (i) in the next section and of (ii) in Section 3. This approach is similar to the construction and investigation of universal ambient groups as described in [7, Chapter 20] or [19, Chapter 5]. Our approach in Section 3, however, yields deeper results on the structure of sumsets without unique sums and requires techniques different from those in [7, 19]. Moreover, the determinant bound we establish in Section 2 for sumsets without unique sums is stronger than those used in [7, 19] for general sumsets.

The proof of Theorem 3 will be given in Section 4. We remark that the bounds given in Theorem 3 are certainly not sharp, since the basis $\mathcal{B}$ constructed in Theorem 4 can be replaced by a more refined basis. However, based on our investigations, we are convinced that a substantial improvement in this direction would require much more complicated arguments than the proof on Theorem 3.

2 Determinant Bound

In this section, we investigate determinants arising from linear systems that correspond to subsets A, B of finite abelian groups for which $A+B$ does not contain a unique difference. We first set up some notation and make some preliminary observations.

Let A, B be subsets of a finite abelian group G such that $A+B$ does not contain a unique sum and write $A = \{a_0, \ldots, a_{|A|-1}\}$ and $B = \{b_0, \ldots, b_{|B|-1}\}$. As pointed out in the introduction, we may assume $a_0 = b_0 = 0$. Similar to the proof of [3, Thm. 1], we assign variables x_i and y_j to the nonzero a_i's and b_j's, respectively. We set $x_0 = y_0 = 0$ (and do not view x_0 and y_0 as variables). Let

$$\mathcal{Q} = \{(i, j, i', j') : a_i + b_j = a_{i'} + b_{j'},\ 0 \le i, i' \le |A| - 1, 0 \le j, j' \le |B| - 1, i \neq i'\}.$$

We remark that $i \neq i'$ implies $j \neq j'$ here and thus the condition $j \neq j'$ is ommited in the definition of $\mathcal{Q}$. We will study the linear system

$$x_i + y_j = x_{i'} + y_{j'},\ (i, j, i', j') \in \mathcal{Q}, \tag{1}$$

over the field of rational numbers. As $A+B$ does not contain a unique sum, for each pair (i, j), there exists at least one pair (i', j') with $(i, j, i', j') \in \mathcal{Q}$. Note that all equations in (1) are homogeneous. Furthermore, for a given pair (i, j), there may be more than one pair (i', j') such that $(i, j, i', j') \in \mathcal{Q}$. Observe that there are $|A| + |B| - 2$ variables involved in (1) (x_0 and y_0 do not count as variables).

We consider (1) as a system of equations for $(x_1, \ldots, x_{|A|-1}, y_1, \ldots, y_{|B|-1})^T \in \mathbb{Q}^{|A|+|B|-2}$. Let e_i be the unit row vector of length $|A|+|B|-2$ with a 1 in position i, $1 \le i \le |A|-1$, and let f_j be the unit row vector of length $|A| + |B| - 2$ with a 1 in position $|A| - 1 + j$, $1 \le j \le |B| - 1$. For convenience, we set $e_0 = f_0 = 0$ (the all-zero vector in $\mathbb{Q}^{|A|+|B|-2}$). In this notation, the coefficient vector of an equation $x_i + y_j = x_{i'} + y_{j'}$ is

$$e_i - e_{i'} + f_j - f_{j'}. \tag{2}$$

Let $\mathcal{R}(A, B)$ be the set of all vectors (2), $(i, j, i', j') \in \mathcal{Q}$, and let $M(A, B)$ be a matrix whose rows are the vectors in $\mathcal{R}(A, B)$. Then (1) is equivalent to

$$M(A, B)(x_1, \ldots, x_{|A|-1}, y_1, \ldots, y_{|B|-1})^T = 0. \tag{3}$$

Note that an equation $x_i + y_j = x_{i'} + y_{j'}$ corresponds to the the coefficient vector $v = e_i - e_{i'} + f_j - f_{j'}$ and the equivalent equation $x_{i'} + y_{j'} = x_i + y_j$ to $e_{i'} - e_i + f_{j'} - f_j = -v$. Hence, if v is a row of $M(A, B)$, then $-v$ is also a row of $M(A, B)$.

For instance, if $G = C_4 = \{0,1,2,3\}$, $A = B = \{0,1,2\}$, we can take

$$M(A,B) = \begin{pmatrix} 0 & -1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 1 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & 1 & 0 \\ 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ -1 & 1 & -1 & 0 \\ -1 & 1 & 1 & -1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Here the columns of $M(A,B)$ correspond to x_1, x_2, y_1, y_2 (note that $x_0 = y_0 = 0$ are not variables and thus there are no columns of $M(A,B)$ associated to them). For example, the equation $a_1 + b_2 = 1 + 2 = a_2 + b_1$ corresponds to the row $e_1 - e_2 + f_2 - f_1 = (1,-1,-1,1)$ of $M(A,B)$.

Note that $M(A,B)$ is an integral matrix with entries 0, ± 1 only. Furthermore, each row of $M(A,B)$ has $|A| + |B| - 2$ entries, at most four of which are nonzero. Moreover, there are rows of $M(A,B)$ which contain less than four nonzero entries. For instance, an equation $x_0 + y_j = x_{i'} + y_{i'}$ corresponds to a row of $M(A,B)$ with at most three nonzero entries, as $x_0 = 0$ and thus this equation is equivalent to $y_j = x_{i'} + y_{i'}$.

For $\mathcal{F} \subset \mathcal{R}(A,B)$, let $M(\mathcal{F})$ be the submatrix of $M(A,B)$ consisting of the rows in $\mathcal{F}$. The following is the central result of this section.

Theorem 4. *There is a subset $\mathcal{B}$ of $\mathcal{R}(A,B)$ with the following properties.*

(a) *$\mathcal{B}$ is a basis of the rowspace of $M(A,B)$.*

(b) *If $\operatorname{rank}_{\mathbb{Q}}(M(\mathcal{B})) = |A| + |B| - 2$, then $|\det(M(\mathcal{B}))| \le (\sqrt[4]{12})^{|A|+|B|-2}$.*

(c) *If $\operatorname{rank}_{\mathbb{Q}}(M(\mathcal{B})) < |A| + |B| - 2$, then $|\det(M')| \le 2\sqrt[4]{12}^{|A|+|B|-4}$ for every invertible submatrix M' of $M(\mathcal{B})$.*

Proof. Recall that $a_0 = b_0 = 0$ and $e_0 = f_0 = 0$. Since $A + B$ does not contain a unique sum, for every i with $0 \leq i \leq |A| - 1$, there are j, k, $0 \leq j \leq |A| - 1$, $0 \leq k \leq |B| - 1$, $j \neq i$, with $a_i + b_0 = a_j + b_k$. Thus $e_i - e_j + f_0 - f_k = e_i - e_j - f_k$ is a row of $M(A, B)$. Hence, for every i with $1 \leq i \leq |A| - 1$, there exist $\sigma(i), \tau(i)$ with $0 \leq \sigma(i) \leq |A| - 1$, $\sigma(i) \neq i$, $1 \leq \tau(i) \leq |B| - 1$ such that

$$e_i - e_{\sigma(i)} - f_{\tau(i)} \tag{4}$$

is a row of $M(A, B)$.

Note that the row vectors corresponding to (4) have Euclidean norm at most $\sqrt{3}$ while rows of $M(A, B)$ with four nonzero entries have Euclidean norm 2. Our first goal is to include as many rows of type (4) in the targeted set $\mathcal{B}$ as possible. The only restriction we have to abide by in this process is to make sure that the set of chosen rows remains linearly independent over $\mathbb{Q}$. The effect is that, for the subsequent application of Hadamard's inequality to $\det(M(\mathcal{B}))$, respectively $\det(M')$, a substantial number of factors 2 are reduced to $\sqrt{3}$ compared to the application of Hadamard's inequality to an arbitrary basis of the rowspace of $M(A, B)$. In addition to this improvement, we will also include as many rows of the form $e_i - e_0 + f_j - f_k = e_i + f_j - f_k$ in $\mathcal{B}$ as possible and so strengthen the bounds further.

Let us start with considering row vectors of type (4) in detail. Note that $\sigma(i)$ and $\tau(i)$ may not be unique. But from now on, for each i, we fix one pair $(\sigma(i), \tau(i))$ such that (4) is a row of $M(A, B)$. We may then view σ and τ as functions

$$\begin{aligned} \sigma: \quad & \{1, \ldots, |A| - 1\} \to \{0, 1, 2, \ldots, |A| - 1\}, \\ \tau: \quad & \{1, \ldots, |A| - 1\} \to \{1, \ldots, |B| - 1\}. \end{aligned}$$

We now recursively construct subsets $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_R$ of $\mathcal{R}(A, B)$ such that $\bigcup_{i=1}^{R} \mathcal{B}_i$ consists of $|A| - 1$ rows of type (4). These subsets will be used to build up the required set $\mathcal{B}$. Our goal is to maximize $\dim_{\mathbb{Q}}(\operatorname{span}(\bigcup_{i=1}^{R} \mathcal{B}_i))$. First of all, we will choose the $\mathcal{B}_i$'s such that, for each i, the rows in $\mathcal{B}_i$ are linearly independent. Hence, if $\dim_{\mathbb{Q}}(\operatorname{span}(\bigcup_{i=1}^{R} \mathcal{B}_i))$ is relatively small, this must be due to linear dependencies between different $\mathcal{B}_i$'s. But we will show that the existence such linear dependencies implies that we can include a comparatively large number of equations of the form $e_i + f_j - f_k$ in $\mathcal{B}$. Thus a comparatively small number of rows (4) in $\mathcal{B}$ fortunately can be compensated by a comparatively large number of rows of the form $e_i + f_j - f_k$. This will be enough to prove Theorem 4.

Now let us proceed to the construction of the sets $\mathcal{B}_i$. For a positive integer t and $c \in \{0, 1, \ldots, |A| - 1\}$, let $\sigma^t(c)$ denote the image of c under the t-fold iteration of σ, that is, $\sigma^1(c) = \sigma(c)$, $\sigma^2(x) = \sigma(\sigma(c))$, etc. Let $r_1 \geq 1$ be the smallest integer such that $\sigma^{r_1}(1) \in \{\sigma^i(1) : i = 1, \ldots, r_1 - 1\} \cup \{0\}$. Then $1, \sigma(1), \ldots, \sigma^{r_1-1}(1)$ are pairwise distinct positive integers. Renumbering the a_i's, if necessary, we may assume $\sigma^i(1) = i + 1$ for $i = 1, \ldots, r_1 - 1$, that is, $\sigma(i) = i + 1$ for $i = 1, \ldots, r_1 - 1$. Hence, by (4), the rows $e_i - e_{i+1} - f_{\tau(i)}$, $i = 1, \ldots, r_1 - 1$, are in $\mathcal{R}(A, B)$. Moreover, the row $e_{r_1} - e_{\sigma(r_1)} - f_{\tau(r_1)}$ is in $\mathcal{R}(A, B)$ by (4). Thus

$$\mathcal{B}_1 := \{e_i - e_{i+1} - f_{\tau(i)} : i = 1, \ldots, r_1 - 1\} \cup \{e_{r_1} - e_{\sigma(r_1)} - f_{\tau(r_1)}\} \subset \mathcal{R}(A, B).$$

Furthermore, $\sigma(r_1) \in \{0, 1, \ldots, r_1\}$ by the definition of r_1.

Note that $|\mathcal{B}_1| = r_1$. If $r_1 = |A| - 1$, we set $R = 1$ and are done with the construction of the $\mathcal{B}_i$'s. Suppose $r_1 < |A| - 1$. Then there is a smallest integer $j_1 \geq 1$ such that

$$\sigma^{j_1}(r_1 + 1) \in \{0, \ldots, r_1\} \cup \{\sigma^j(r_1 + 1) : 1 \leq j \leq j_1 - 1\}.$$

Then $\sigma(r_1 + 1), \ldots, \sigma^{j_1-1}(r_1 + 1)$ are distinct and not in $\{0, \ldots, r_1\}$. Set $r_2 = r_1 + j_1$. After renumbering the a_i's, if necessary, we may assume $\sigma(r_1 + 1) = r_1 + 2, \sigma^2(r_1 + 1) = r_1 + 3, \ldots, \sigma^{j_1-1}(r_1 + 1) = r_1 + j_1 = r_2$. Thus after the possible renumbering we have

$$\{0, \ldots, r_1\} \cup \{\sigma^j(r_1 + 1) : 1 \leq j \leq j_1 - 1\} = \{0, 1, \ldots, r_2\}.$$

Hence, by definition of j_1, we have

$$\sigma^{j_1}(r_1 + 1) = \sigma(\sigma^{j_1-1}(r_1 + 1)) = \sigma(r_2) \in \{0, 1, \ldots, r_2\}.$$

Recall that $\sigma(i) \neq i$ for all i. Thus $\sigma(r_2) < r_2$. In summary, we have

$$\sigma(j) = j + 1 \text{ for } r_1 + 1 \leq j < r_2 \text{ and } \sigma(r_2) < r_2.$$

We set

$$\mathcal{B}_2 = \{e_i - e_{i+1} - f_{\tau(i)} : i = r_1 + 1, \ldots, r_2 - 1\} \cup \{e_{r_2} - e_{\sigma(r_2)} - f_{\tau(r_2)}\}.$$

If $r_2 < |A| - 1$, we repeat the process with r_1, r_2 replaced by r_2, r_3, etc.

For convenience, we set $r_0 = 0$. We repeat the process above until we reach $r_i = |A| - 1$ for some i. Hence we obtain integers $r_0 < r_1 < r_2 < \cdots < r_R$ with $r_R = |A| - 1$ such that, after a possible renumbering of the a_i's, we have

$$\sigma(j) = j + 1 \text{ for } r_{i-1} + 1 \leq j \leq r_i - 1 \text{ and } \sigma(r_i) \leq r_i - 1 \tag{5}$$

for $i = 1, \ldots, R$. This yields subsets $\mathcal{B}_1, \ldots, \mathcal{B}_R$ of $\mathcal{R}(A, B)$ with

$$\mathcal{B}_i = \{e_j - e_{j+1} - f_{\tau(j)} : r_{i-1} + 1 \leq j \leq r_i - 1\} \cup \{e_{r_i} - e_{\sigma(r_i)} - f_{\tau(r_i)}\} \tag{6}$$

and $\sum_{i=1}^{R} |\mathcal{B}_i| = |A| - 1$. Note that $|\mathcal{B}_i| = r_i - r_{i-1}$. We now need to compute $\dim_{\mathbb{Q}}(\operatorname{span}(\bigcup_{i=1}^{R} \mathcal{B}_i))$. As a preparation, we prove the following.

Lemma 5. *Each set $\mathcal{B}_i$ is linearly independent. For $i = 2, 3, \ldots, R$, write*

$$\delta_i = \dim_{\mathbb{Q}} \left(\operatorname{span}(\mathcal{B}_i) \cap \operatorname{span}(\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{i-1})\right).$$

Then $\delta_i \in \{0, 1\}$ for all i. Furthermore,

$$|\{\tau(j) : j = 1, \ldots, r_i\}| \leq |\{\tau(j) : j = 1, \ldots, r_{i-1}\}| + |\mathcal{B}_i| - 2\delta_i \tag{7}$$

for $i = 2, \ldots, R$.

Proof. To prove this lemma, we mainly work with the support of vectors. For $w = (w_1, \ldots, w_{|A|+|B|-2})^T$, we call $\{i : w_i \neq 0, 1 \leq i \leq |A| - 1\}$ the *e-support* of w and $\{i : w_i \neq 0, |A| \leq i \leq |A| + |B| - 2\}$ the *f-support* of w.

For $j = 1, \ldots |A| - 1$ and $i = 1, \ldots, R$, set

$$\begin{aligned} v_j &= e_j - e_{j+1} - f_{\tau(j)} \quad \text{if } r_{i-1} + 1 \leq j \leq r_i - 1, \\ v_j &= e_{r_i} - e_{\sigma(r_i)} - f_{\tau(r_i)} \;\; \text{if } j = r_i. \end{aligned} \tag{8}$$

Note that the v_j's are well defined, as every $j \in \{1, \ldots, |A| - 1\}$ satisfies exactly one of the conditions on the right hand side of (8). Note that $\mathcal{B}_i = \{v_j : r_{i-1} + 1 \leq j \leq r_i\}$.

We first show that each $\mathcal{B}_i$ is linearly independent. Suppose that $\sum_{j=r_{i-1}+1}^{r_i} \lambda_j v_j = 0$ with $\lambda_j \in \mathbb{Q}$, not all of which are zero. In particular, the e-support and f-support of

$\sum_{j=r_{i-1}+1}^{r_i} \lambda_j v_j$ are both empty. By (8), the e-support of $\sum_{j=r_{i-1}+1}^{r_i} \lambda_j v_j$ can only be empty if the nonzero λ_j's are all equal. But then the f-support of $\sum_{j=r_{i-1}+1}^{r_i} \lambda_j v_j$ is nonempty, a contradiction. Hence $\mathcal{B}_i$ is linearly independent.

Suppose that w is a nonzero vector in $\mathrm{span}(\mathcal{B}_i) \cap \mathrm{span}(\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{i-1})$. As $w \in \mathrm{span}(\mathcal{B}_i)$, there are $\lambda_j \in \mathbb{Q}$ with $w = \sum_{j=r_{i-1}+1}^{r_i} \lambda_j v_j$. Since $w \in \mathrm{span}(\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{i-1})$, the e-support of w is contained in $\{1, \ldots, r_{i-1}\}$ by (5). By (8) this is only possible if the the e-support of $\sum_{j=r_{i-1}+1}^{r_i} \lambda_j v_j$ is empty, i.e., all contributions from unit vectors e_k with $r_{i-1} + 1 \leq k \leq r_i$ in $\sum_{j=r_{i-1}+1}^{r_i} \lambda_j v_j$ cancel out. This means that either all λ_j's are zero or there is $j_0 \in \{r_{i-1} + 1, \ldots, r_i - 1\}$ with $\lambda_j = 0$ for $j < j_0$, $\lambda_{j_0} = \cdots = \lambda_{r_i} \neq 0$, and $\sigma(r_i) = j_0$. The former case cannot occur, since $w \neq 0$. Hence $\sigma(r_i) = j_0$ and

$$w \in \mathrm{span}\left(\sum_{j=j_0}^{r_i} v_j\right) = \mathrm{span}\left(\sum_{j=j_0}^{r_i} f_{\tau(j)}\right). \tag{9}$$

This implies $\delta_i \in \{0, 1\}$.

It remains to prove (7). If $\delta_i = 0$, then (7) holds, since $|\mathcal{B}_i| = r_i - r_{i-1}$. Thus suppose that $\delta_i = 1$. Then, by (9), the f-support of w is $\{\tau(j) : j_0 \leq j \leq r_i\}$. On the other hand, since $w \in \mathrm{span}(\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{i-1})$, the f-support of w is contained in $\{\tau(j) : j = 1, \ldots, r_{i-1}\}$ by (6). We conclude $\{\tau(j) : j_0 \leq j \leq r_i\} \subset \{\tau(j) : j = 1, \ldots, r_{i-1}\}$. Using $j_0 \leq r_i - 1$, we get

$$\begin{aligned} |\{\tau(j) : j = 1, \ldots, r_i\}| - |\{\tau(j) : j = 1, \ldots, r_{i-1}\}| &\leq |\{\tau(j) : j = r_{i-1} + 1, \ldots, j_0 - 1\}| \\ &\leq j_0 - r_{i-1} - 1 \\ &\leq r_i - 1 - r_{i-1} - 1 = |\mathcal{B}_i| - 2. \end{aligned}$$

This completes the proof of Lemma 5. □

We continue with the proof of Theorem 4. Now we are ready to compute $\dim_{\mathbb{Q}}(\mathrm{span}(\bigcup_{i=1}^R \mathcal{B}_i))$. Recall that $\sum_{i=1}^R |\mathcal{B}_i| = |A| - 1$. As the $\mathcal{B}_i$'s are linearly independent, we have $\dim_{\mathbb{Q}}(\mathrm{span}(\mathcal{B}_i)) = |\mathcal{B}_i|$ for all i. Moreover,

$$\dim_{\mathbb{Q}}(\mathrm{span}(\bigcup_{i=1}^{k} \mathcal{B}_i)) = \dim_{\mathbb{Q}}(\mathrm{span}(\bigcup_{i=1}^{k-1} \mathcal{B}_i)) + \dim_{\mathbb{Q}}(\mathrm{span}(\mathcal{B}_k)) - \delta_k \tag{10}$$

for $k = 2, \ldots, R$ by the dimension formula and the definition of the δ_i's. Applying (10) repeatedly, we get

$$\dim_{\mathbb{Q}}(\mathrm{span}(\bigcup_{i=1}^{R-1} \mathcal{B}_i)) = |\mathcal{B}_1| + \sum_{i=2}^{R} (|\mathcal{B}_i| - \delta_i) = |A| - 1 - \sum_{i=2}^{R} \delta_i.$$

We now show that a comparatively large number of rows of the form $e_i + f_j - f_k$ can be included in the targeted set $\mathcal{B}$ if $\sum_{i=2}^{R} \delta_i$ is large. Using (7) repeatedly, we get

$$\begin{aligned} |\{\tau(j) : j = 1, \ldots, r_R\}| &\leq |\{\tau(j) : j = 1, \ldots, r_{R-1}\}| + |\mathcal{B}_R| - 2\delta_R \\ &\leq |\{\tau(j) : j = 1, \ldots, r_{R-2}\}| + |\mathcal{B}_R| + |\mathcal{B}_{R-1}| - 2(\delta_R + \delta_{R-1}) \\ &\ldots \\ &\leq |\{\tau(j) : j = 1, \ldots, r_1\}| + \sum_{i=2}^{R} (|\mathcal{B}_i| - 2\delta_i) \\ &\leq |\mathcal{B}_1| + \sum_{i=2}^{R} (|\mathcal{B}_i| - 2\delta_i) \\ &= |A| - 1 - 2\sum_{i=2}^{R} \delta_i. \end{aligned}$$

Recall that $r_R = |A| - 1$. Write $L = |\{\tau(j) : j = 1, \ldots, |A| - 1\}|$ and $k = \sum_{i=2}^{R} \delta_i$. Then, by what we have shown,

$$\dim_{\mathbb{Q}}(\mathrm{span}(\bigcup_{i=1}^{R} \mathcal{B}_i)) = |A| - k - 1 \text{ and } L \leq |A| - 2k - 1. \tag{11}$$

Renumbering the b_i's, if necessary, we may assume $\{\tau(j) : j = 1, \ldots, |A| - 1\} = \{1, \ldots, L\}$. We now use a similar argument as above, but reverse the roles of A and B, i.e., this time we work with equations of the form $b_i = a_j + b_k$ instead of $a_i = a_j + b_k$. We obtain functions

$$\begin{aligned} \alpha : &\ \{1, \ldots, |B| - 1\} \to \{1, \ldots, |A| - 1\}, \\ \beta : &\ \{1, \ldots, |B| - 1\} \to \{0, \ldots, |B| - 1\}. \end{aligned}$$

such that

$$f_i - e_{\alpha(i)} - f_{\beta(i)} \in \mathcal{R}(A, B) \text{ for } i = 1, \ldots, |B| - 1$$

and $\beta(i) \neq i$ for all i.

Set

$$\mathcal{D} = \{f_i - e_{\alpha(i)} - f_{\beta(i)} : L+1 \leq i \leq |B|-1\}.$$

Considering the f-support of the vectors in $\mathcal{D}$, it is straightforward to see that there is a subset $P = \{p_1, \ldots, p_t\}$ of $\{L+1, \ldots, |B|-1\}$ with $|P| \geq |\mathcal{D}|/2$ such that

$$p_j \notin \{p_1, \ldots, p_{j-1}\} \cup \{\beta(p_1), \ldots, \beta(p_{j-1})\} \text{ for } j = 2, \ldots, t. \tag{12}$$

Set

$$\mathcal{E} = \{f_i - e_{\alpha(i)} - f_{\beta(i)} : i \in P\}.$$

Note that (12) implies that $\mathcal{E}$ is linearly independent. Thus $\dim_{\mathbb{Q}}(\operatorname{span}(\mathcal{E})) \geq |\mathcal{D}|/2 = (|B| - L - 1)/2$. Moreover, since none of the f_i, $i \in P$, occurs in any of the sets $\mathcal{B}_i$, we have

$$\operatorname{span}(\mathcal{E}) \cap \operatorname{span}(\bigcup_{i=1}^{R} \mathcal{B}_i) = \{0\}.$$

Using (11) and $\dim_{\mathbb{Q}}(\operatorname{span}(\mathcal{E})) \geq (|B| - L - 1)/2$, we conclude

$$\begin{aligned}\dim_{\mathbb{Q}}\left(\operatorname{span}(\mathcal{E}) \cup \bigcup_{i=1}^{R} \mathcal{B}_i\right) &\geq \frac{|B| - L - 1}{2} + |A| - k - 1 \\ &\geq \frac{|B| - (|A| - 2k - 1) - 1}{2} + |A| - k - 1 \\ &= \frac{|A| + |B| - 2}{2}.\end{aligned} \tag{13}$$

Let $\mathcal{C}$ be linearly independent subset of $\mathcal{E} \cup \bigcup_{i=1}^{R} \mathcal{B}_i$ of maximal cardinality. Then $|\mathcal{C}| \geq (|A| + |B| - 2)/2$ by (13). Note that $\dim_{\mathbb{Q}}(\operatorname{span}(\mathcal{R}(A,B))) \leq |A| + |B| - 2$, since $\mathcal{R}(A,B) \subset \mathbb{Q}^{|A|+|B|-2}$. Hence there is a subset $\mathcal{F}$ of $\mathcal{R}(A,B)$ with $|\mathcal{F}| \leq (|A| + |B| - 2)/2$ such that $\mathcal{B} := \mathcal{C} \cup \mathcal{F}$ is a basis of the rowspace of $M(A,B)$. Recall that $M(\mathcal{B})$ is the submatrix of $M(A,B)$ that consists of the rows in $\mathcal{B}$. Note that the Euclidean norm of the row vectors of $M(\mathcal{B})$ corresponding to elements of $\mathcal{C}$ is at most $\sqrt{3}$ and the Euclidean norm of the row vectors corresponding to equations in $\mathcal{B} \setminus \mathcal{C}$ is at most 2. Hence, if $\operatorname{rank}_{\mathbb{Q}}(M(\mathcal{B})) = |A| + |B| - 2$, then

$$|\det(M(\mathcal{B})| \leq 2^{(|A|+|B|-2)/2} \sqrt{3}^{(|A|+|B|-2)/2} = \sqrt[4]{12}^{|A|+|B|-2}$$

by Hadamard's inequality. This proves part (b) of Theorem 4.

Now suppose $\operatorname{rank}_{\mathbb{Q}}(M(\mathcal{B})) < |A|+|B|-2$, say, $\operatorname{rank}_{\mathbb{Q}}(M(\mathcal{B})) = |A|+|B|-2-t$ with $t \geq 1$. Let M' be an invertible submatrix of $M(\mathcal{B})$. Then at least $(|A|+|B|-1)/2-t$ rows of M' correspond to rows in $\mathcal{C}$. Hence, again using Hadamard's inequality,

$$\begin{aligned} |\det(M')| &\leq 2^{(|A|+|B|-2)/2}\sqrt{3}^{(|A|+|B|-2)/2-t} \\ &\leq 2^{(|A|+|B|-2)/2}\sqrt{3}^{(|A|+|B|-2)/2-1} \\ &\leq 2\sqrt[4]{12}^{|A|+|B|-4}. \end{aligned}$$

This proves part (c) of Theorem 4. □

Remark 6.
(a) The bounds in Theorem 4 can be improved further if $|A|$ or $|B|$ is small by applying arguments used in the proof of [3, Thm. 1]. In this way, we can prove that there is a basis $\mathcal{B}$ of $\operatorname{span}(\mathcal{E})$ such that $\det(M') \leq \min(|A|^{|B|-1}, |B|^{|A|-1})$ for every invertible submatrix M' of the coefficient matrix corresponding to $\mathcal{B}$.

(b) A weaker version of Theorem 4 can be proved easily: Choose *any* subset $\mathcal{B}$ of $\mathcal{E}$ which is a basis of $\operatorname{span}_{\mathbb{Q}}(\mathcal{E})$. Note that all row vectors in $\mathcal{E}$ and thus in $\mathcal{B}$ have Euclidean norm at most 2. Thus, if $\operatorname{rank}_{\mathbb{Q}}(M(\mathcal{B})) = n$, then $|\det(M(\mathcal{B}))| \leq 2^{|A|+|B|-2}$ by Hadamard's inequality. Moreover, if $\operatorname{rank}_{\mathbb{Q}}(M(\mathcal{B})) < n$, then $|\det(M')| \leq 2^{|A|+|B|-3}$ for every invertible submatrix M' of $M(\mathcal{B})$, again by Hadamard's inequality. In summary, this proves Theorem 4 with $\sqrt[4]{12}$ replaced by 2.

3 Structure of Sets with no Unique Sum

Let A be a subset of a finite abelian group and let H be a subgroup of G. If $A = \cup_{i=1}^{t} A_i$ for pairwise disjoint subsets A_i of G and $A_i \subset H + g_i$ for all i for some $g_i \in G$, then $\cup_{i=1}^{t} A_i$ is called an *H-coset decomposition* of A (see [7, p. 17]). One of the themes of structural additive number theory is to provide sufficient conditions for the existence of H-coset decompositions with certain properties. For instance, the theorem of Green and Ruzsa [6] shows that a subset of an abelian group that has a relatively small sumset $A+A$

necessarily admits an H-coset decomposition such that the cosets involved arise from an arithmetic progression.

In this section, following the theme just mentioned, we show that subsets A, B of a finite abelian group G admit a highly structured H-coset decomposition if $A+B$ does not contain a unique sum and $|A|, |B|$ are relatively small compared to $|G|$. This provides insights into the nature of such sets and will lead to new sufficient conditions for the existence of unique sums and differences.

Theorem 7. *Let G be a finite abelian group, and let A, B be subsets of G with $0 \in A \cap B$ and $\langle A \cup B \rangle = G$. Suppose that $A + B$ does not contain a unique sum and that $|G| > (\sqrt[4]{12})^{|A|+|B|-2}$. Then there exist a subgroup H of G with $|H| \leq 2\sqrt[4]{12}^{|A|+|B|-4}$, integers $K \geq 1$, $N \geq 1$, integers $\alpha_1 < \cdots < \alpha_K$, $\beta_1 < \cdots < \beta_N$, and nonempty subsets $A_1, \ldots, A_K$, $B_1, \ldots, B_N$ of G such that the following hold.*

(i) *A is the disjoint union of $A_1, \ldots, A_K$ and B is the disjoint union of $B_1, \ldots, B_N$.*

(ii) *If $(A_i + B_j) \cap (A_{i'} + B_{j'})$ is nonempty for any i, j, i', j' with $1 \leq i, i' \leq K$, $1 \leq j, j' \leq N$, then $\alpha_i + \beta_j = \alpha_{i'} + \beta_{j'}$.*

(iii) *$A_1 + B_1$ and $A_K + B_N$ both do not contain unique sums.*

(iv) *$A_i \subset H + g_i$ and $B_j \subset H + h_j$ for some $g_i, h_j \in G$ for all i, j.*

(v) *If $\langle A \rangle = G$, then $K \geq 2$. Similarly, if $\langle B \rangle = G$, then $N \geq 2$.*

Proof. Write $n = |A| + |B| - 2$. Let $\mathcal{B}$ be a subset of $M(A, B)$ with the properties stated in Theorem 4, write $M = M(\mathcal{B})$ and $s = \operatorname{rank}_{\mathbb{Q}}(M)$. Note that s is the number of rows of M, since the rows of M are linearly independent. We now consider the linear system $Mz = 0$, $z = (z_1, ..., z_n)^T$, for both $z \in \mathbb{Z}^n$ and $z \in G^n$. Recall that $A = \{a_0, \ldots, a_{|A|-1}\}$, $B = \{b_0, \ldots, b_{|B|-1}\}$, and that

$$Mz_0 = 0 \text{ for } z_0 = (a_1, \ldots, a_{|A|-1}, b_1, \ldots, b_{|B|-1|})^T. \tag{14}$$

Let D be the Smith Normal Form of M (over the principal ideal domain $\mathbb{Z}$). Then D is a diagonal $s \times n$ matrix with diagonal entries $d_1, d_2, \ldots, d_s \in \mathbb{Z}$ such that $d_i | d_j$ whenever

$i < j$. Note that $d_1, \ldots, d_s \neq 0$, as M has rank s. Let S and T be unimodular matrices with $SMT = D$. Write $T = (X, Y)$ where X consists of the first s columns of T and Y of the remaining columns. By $o(g)$ we denote the order of an element g of G.

Claim 1
(a) The solution set of $Mz = 0$, $z \in \mathbb{Z}^n$, is $\{Yw : w \in \mathbb{Z}^{n-s}\}$.
(b) The solution set of $Mz = 0$, $z \in G^n$, is

$$\{Xc + Yw : c \in G^s, w \in G^{n-s},\ o(c_i)|d_i \text{ for } i = 1, \ldots, s\}.$$

Here we write $c = (c_1, \ldots, c_s)^T$.

Proof of Claim 1: Let R be either $\mathbb{Z}$ or G. Note that $M = S^{-1}DT^{-1}$. Hence $Mz = 0$, $z \in R^n$, if and only if $DT^{-1}z = 0$. Write $T^{-1}z = \binom{c}{w}$ with $c \in R^s$, $w \in R^{n-s}$. Recall that that $d_1, \ldots, d_s \neq 0$. Thus $DT^{-1}z = D\binom{c}{w} = 0$ if and only if

$$d_i c_i = 0 \text{ for } i = 1, \ldots, s. \tag{15}$$

If $R = \mathbb{Z}$, then (15) holds if and only if $c = 0$. Hence, in this case, the general solution of $Mz = 0$ is $z = T\binom{0}{w} = (X, Y)\binom{0}{w} = Yw$, $w \in \mathbb{Z}^{n-s}$. This proves part (a) of Claim 1. If $R = G$, then (15) holds if and only if $o(c_i)|d_i$ for $i = 1, \ldots, s$. Hence the general solution of $Mz = 0$, $z \in G^n$, is as stated in part (b) of Claim 1. This completes the proof of Claim 1.

Claim 2 We have $s < n$.

Proof of Claim 2: Clearly, $s \leq n$. Suppose that $s = n$. By (14) we have $Mz_0 = 0$ where $z_0 = (a_1, ..., a_{|A|-1|}, b_1, ..., b_{|B|-1})^T \in G^n$. Hence $z_0 = Xc$, $c \in G^n$, and $o(c_i)|d_i$ for $i = 1, \ldots, s$ by Claim 1 (note that there is no term Yw in z_0, as $s = n$). Let $\langle c_1, \ldots, c_n \rangle$ denote the subgroup of G generated by $c_1, \ldots, c_n$. As $z_0 = Xc$ and X is an integer matrix, we conclude that all a_i's and b_i's are contained in $\langle c_1, \ldots, c_n \rangle$. As $o(c_i)|d_i$ for $i = 1, \ldots, s$, we have $|\langle c_1, \ldots, c_n \rangle| \leq \prod_{i=1}^n d_i$. Note that $\det(M) = \prod_{i=1}^n d_i$, since $SMT = D$ and S, T are unimodular matrices. Furthermore, $\det(M) \leq (\sqrt[4]{12})^{|A|+|B|-2}$ by Theorem 4. Hence

$$|\langle A \cup B \rangle| \leq |\langle c_1, \ldots, c_n \rangle| \leq \det(M) \leq (\sqrt[4]{12})^{|A|+|B|-2}.$$

This contradicts the assumptions $\langle A \cup B \rangle = G$ and $|G| > (\sqrt[4]{12})^{|A|+|B|-2}$ of Theorem 7. Claim 2 is proved.

From now on we assume $s < n$. Recall that, by Claim 1, the general solution of $Mz = 0$, $z \in \mathbb{Z}^n$, is $z = Yw$, $w \in \mathbb{Z}^{n-s}$. Let $Y_1, \ldots, Y_n$ be the rows of Y. The following claim can be generalized to arbitrary real matrices instead of Y, but we only state it for Y to minimize the required notation.

Claim 3 There is $w \in \mathbb{Z}^{n-s}$ such that $\gamma := Yw$ satisfies the following conditions for all i, k with $1 \leq i, k \leq n$.

$$\text{If } \gamma_i = 0, \text{ then } Y_i = 0, \text{ and if } \gamma_i = \gamma_k, \text{ then } Y_i = Y_k. \tag{16}$$

Proof of Claim 3: For each i with $Y_i \neq 0$, the set $E_i := \{x \in \mathbb{R}^{n-s} : Y_i x = 0\}$ is a hyperplane in $\mathbb{R}^{n-s}$, and for each pair (i, k) with $Y_i \neq Y_k$, the set $E_{ik} := \{x \in \mathbb{R}^{n-s} : (Y_i - Y_k)x = 0\}$ is also a hyperplane in $\mathbb{R}^{n-s}$. If $w \in \mathbb{Z}^{n-s}$ does not satisfy (16), then $Y_i w = \gamma_i = 0$ for some i with $Y_i \neq 0$ or $(Y_i - Y_k)w = \gamma_i - \gamma_k = 0$ for some pair (i, k) with $Y_i \neq Y_k$. This means that every w which does not satisfy (16) lies on at least one of the hyperplanes E_i or E_{ik}. But any union of finitely many hyperplanes of $\mathbb{R}^{n-s}$ does not cover $\mathbb{Z}^{n-s}$. Hence there is $w \in \mathbb{Z}^{n-s}$ satisfying (16). This proves Claim 3.

Now we fix a $w \in \mathbb{Z}^{n-s}$ satisfying (16), set $\gamma = Yw$, and write

$$(u_1, \ldots, u_{|A|-1}, v_1, \ldots, v_{|B|-1}) = (\gamma_1, \ldots, \gamma_n).$$

Recall that we assume $a_0 = b_0 = 0$ and have the corresponding values $x_0 = y_0 = 0$. Accordingly, we set $u_0 = v_0 = 0$.

Claim 4 Suppose that $a_i + b_j = a_{i'} + b_{j'}$ where $0 \leq i, i' \leq |A| - 1$ and $0 \leq j, j' \leq |B| - 1$. Then $u_i + v_j = v_{i'} + v_{j'}$.

Proof of Claim 4: By the definition of $\mathcal{R}(A, B)$, if $a_i + b_j = a_{i'} + b_{j'}$, then $e_i + f_j - e_{i'} - f_{j'} \in \mathcal{R}(A, B)$. Recall that $M\gamma = 0$. As the rows of M form a basis of $\operatorname{span}_{\mathbb{Q}}(\mathcal{R}(A, B))$, we conclude that $(u_1, \ldots, u_{|A|-1}, v_1, \ldots, v_{|B|-1})^T = \gamma$ satisfies all equations (1). Thus $a_i + b_j = a_{i'} + b_{j'}$ implies $u_i + v_j = v_{i'} + v_{j'}$ (note that the argument is still correct if i or j is 0, as a_i or b_j is 0 in this case, and we have $u_0 = v_0 = 0$ by definition). This proves Claim 4.

Let $\alpha_1 < \cdots < \alpha_K$ be the distinct values in the set $\{u_i : i = 0, \ldots, |A| - 1\}$ and $\beta_1 < \cdots < \beta_N$ be the distinct values in the set $\{v_i : i = 0, \ldots, |B| - 1\}$. Define

$$\begin{aligned} A_i &= \{a_j : 0 \leq j \leq |A| - 1, u_j = \alpha_i\}, \\ B_k &= \{b_j : 0 \leq j \leq |B| - 1, v_j = \beta_k\} \end{aligned}$$

for $i = 1, \ldots, K$ and $k = 1, \ldots, N$. Clearly, A and B are disjoint unions of the A_i's and B_i's, respectively. This proves part (i) of Theorem 7.

We now prove part (ii) of Theorem 7. Suppose $(A_i + B_j) \cap (A_{i'} + B_{j'}) \neq \emptyset$. Then there exist $a_r \in A_i$, $b_t \in B_j$, $a_{r'} \in A_{i'}$, and $b_{t'} \in B_{j'}$ such that $a_r + b_t = a_{r'} + b_{t'}$. By Claim 4, we conclude $u_r + v_t = u_{r'} + v_{t'}$. As $a_r \in A_i$, $b_t \in B_j$, $a_{r'} \in A_{i'}$, and $b_{t'} \in B_{j'}$, we have $u_r = \alpha_i$, $v_t = \beta_j$, $u_{r'} = \alpha_{i'}$, and $v_{t'} = \beta_{j'}$ by the definition of the A_i's and B_k's. Therefore, $\alpha_i + \beta_j = u_r + v_t = u_{r'} + y_{t'} = \alpha_{i'} + \beta_{j'}$. This proves part (ii) of Theorem 7.

For (iii), observe that $\alpha_1 + \beta_1 \neq \alpha_i + \beta_j$ if $(i, j) \neq (1, 1)$, since $\alpha_1 < \cdots < \alpha_K$ and $\beta_1 < \cdots < \beta_N$. Therefore, $(A_1 + B_1) \cap (A_i + B_j) = \emptyset$ if $(i, j) \neq (1, 1)$ by part (ii). As $A + B$ does not contain a unique sum, this implies that $A_1 + B_1$ does not contain a unique sum. By a similar argument, we conclude that $A_K + B_N$ does not contain a unique sum as well. This proves part (iii) of Theorem 7.

We now proceed to part (iv) of Theorem 7. Recall that

$$z_0 = (a_1, \ldots, a_{|A|-1}, b_1, \ldots, b_{|B|-1})^T \in G^n$$

is a solution of $Mz_0 = 0$. By Claim 1, we have $z_0 = Xc + Yw$ with $c \in G^s$, $w \in G^{n-s}$, and $o(c_i)|d_i$ for $i = 1, \ldots, s$. Now suppose that $a_k, a_t \in A_i$ for some fixed i and some integers k, t with $0 \leq k < t \leq |A| - 1$. Then $u_k = u_t = \alpha_i$ by the definition of A_i. Let $H = \langle c_1, \ldots, c_s \rangle$. We will show $a_k - a_t \in H$. Recall that $\gamma = Yw$ and

$$(u_1, \ldots, u_{|A|-1}, v_1, \ldots, v_{|B|-1}) = (\gamma_1, \ldots, \gamma_n).$$

First suppose that both k and t are positive. Then $u_k = u_t$ implies $\gamma_k = \gamma_t$. Thus $Y_k = Y_t$ by Claim 3. Recall that $z_0 = Xc + Yw$. Let $X_1, \ldots, X_n$ be the rows of X. Since $Y_k = Y_t$, we conclude

$$a_k - a_t = (z_0)_k - (z_0)_t = (X_k - X_t)c + (Y_k - Y_t)w = (X_k - X_t)c.$$

As the entries of X_k and X_t are integers, we conclude $a_k - a_t \in H$.

Now suppose that $k = 0$. Then $a_k = 0$ and $u_k = 0$ by definition and thus $u_t = \alpha_i = u_k = 0$. As $t > 0$, this implies $\gamma_t = u_t = 0$. By Claim 3, we conclude $Y_t = 0$. Hence

$$a_k - a_t = 0 - a_t = -(z_0)_t = -X_t c - Y_t w = -X_t c,$$

as $Y_t = 0$. Thus $a_k - a_t \in H$ in this case, too.

In summary, we have shown that, for every i, any two elements of A_i are in the same coset of H. In the same way, we can prove that for every k, any two elements of B_k are in the same coset of H.

To complete the proof of part (iv) of Theorem 7, it remains to show

$$|H| \leq 2\sqrt[4]{12}^{|A|+|B|-4}.$$

Note that $|H| \leq \prod_{i=1}^{s} d_i$, as $o(c_i)|d_i$ for $i = 1, \ldots, s$. It is a well known fact concerning the Smith Normal Form that $d_j = D_j/D_{j-1}$ for $j = 1, \ldots, s$ where D_j is the greatest common divisor of all $j \times j$ minors of M (with the convention $D_0 = 1$). Hence $D_s = \prod_{i=1}^{s} d_i$. By Theorem 4, we have $|D_s| \leq 2\sqrt[4]{12}^{|A|+|B|-4}$. Thus $|H| \leq 2\sqrt[4]{12}^{|A|+|B|-4}$. Part (iv) of Theorem 7 is proved.

To prove part (v) of Theorem 7, we need to show $K \geq 2$ if $\langle A \rangle = G$. If $K = 1$, then $A = A_1$ and thus $0 \in A_1$, since $0 \in A$ by assumption. As $0 \in A_1$, we have $A_1 \subset H$ by part (iv). Thus $G = \langle A \rangle = \langle A_1 \rangle \subset H$. In particular, $|G| = |H| \leq 2\sqrt[4]{12}^{|A|+|B|-4}$. This contradicts the assumption $|G| > (\sqrt[4]{12})^{|A|+|B|-2}$. Similarly, we see that $N \geq 2$ if $\langle B \rangle = G$, which proves part (v). This completes the proof of Theorem 7. □

Remark 8. If we are content with a weaker version of Theorem 7, we can avoid using Theorem 4 by replacing $\sqrt[4]{12}$ by 2 in the relevant bounds. Remark 6 (b) together with the proof of Theorem 7 shows that the following weakened version of Theorem 7 is true with no need to use to Theorem 4.

Let G be a finite abelian group, and let A, B be subsets of G with $0 \in A \cap B$ and $\langle A \cup B \rangle = G$. Suppose that $A+B$ does not contain a unique sum and that $|G| > 2^{|A|+|B|-2}$. Then there exist a subgroup H of G with $|H| \leq 2^{|A|+|B|-3}$, integers $\alpha_1 < \cdots < \alpha_K$, $\beta_1 <$

$\cdots < \beta_N$, and nonempty subsets $A_1, \ldots, A_K$, $B_1, \ldots, B_N$ of G such that the conclusions (i)-(v) *of Theorem* 7 *hold.*

For unique differences we obtain the following result similar to Theorem 7. We skip the proof, as it is straightforward adaption of the proof of Theorem 7. More details can be found in [10, Thm. 13, Cor. 16].

Theorem 9. *Let G be a finite abelian group and A be a subset of G with $0 \in A$ and $\langle A \rangle = G$. Suppose that $|G| > 2^{|A|-1}$. If A does not have a unique difference, then there exist a subgroup H of G with $|H| \leq 2^{|A|-1}$, an integer $K \geq 2$, integers $\alpha_1 < \cdots < \alpha_K$, and nonempty subsets $A_1, \ldots, A_K$ of G such that the following hold.*

(i) *A is the disjoint union of $A_1, \ldots, A_K$.*

(ii) *If $(A_i - A_j) \cap (A_{i'} - A_{j'})$ is nonempty for any i, j, i', j' with $1 \leq i, j, i', j' \leq K$, then $\alpha_i - \alpha_j = \alpha_{i'} - \alpha_{j'}$.*

(iii) *$A_K - A_1$ does not have a unique difference.*

(iv) *$A_i \subset H + g_i$ for some $g_i \in G$ for $i = 1, \ldots, K$.*

4 Proof of Theorem 3

We now prove our main result stated in the introduction.

Proof of Theorem 3. Suppose that $A + B$ contains no unique sum. We are going to apply Theorem 7 to derive a contradiction. If $\langle A \cup B \rangle$ is a proper subgroup of G, then we replace G by $\langle A \cup B \rangle$ and apply Theorem 7 then. Thus we may assume $\langle A \cup B \rangle = G$. Recall that p is the smallest prime divisor of $|G|$. If $p > \sqrt[8]{12}^{|A|+|B|-2}$ and $|\langle A \rangle|$ is not a prime, then $|G| \geq |\langle A \rangle| \geq p^2 > \sqrt[4]{12}^{|A|+|B|-2}$. Hence in both parts (a) and (b) of Theorem 3, the assumptions imply $|G| > \sqrt[4]{12}^{|A|+|B|-2}$. By Theorem 7, we get $A = A_1 \cup \cdots \cup A_K$ and $B = B_1 \cup \cdots \cup B_N$ where the A_i's and B_j's satisfy the conditions listed there. In particular, $A_1 + B_1$ does not contain a unique sum. Let H be the subgroup of G as specified in Theorem 7. Recall that $|H| \leq 2\sqrt[4]{12}^{|A|+|B|-4}$. If $|H| = 1$ then $|A_1| = |B_1| = 1$ and $A_1 + B_1$ would not contain a unique sum, which is impossible. Thus $|H| > 1$.

To prove part (a) of Theorem 3, suppose that $p > \sqrt[4]{12}^{|A|+|B|-2}$. As $|H| > 1$, there a is a prime q that divides $|H|$. Note that $q \leq |H| \leq 2\sqrt[4]{12}^{|A|+|B|-4}$, which contradicts the assumption $p > \sqrt[4]{12}^{|A|+|B|-2}$, as p is the smallest prime divisor of $|G|$. This completes the proof of part (a).

To prove part (b), suppose that $p > \sqrt[8]{12}^{|A|+|B|-2}$. As $|H| \leq 2\sqrt[4]{12}^{|A|+|B|-4}$ and p is the smallest prime divisor of $|G|$, the order of H must be prime. If $K = 1$, then $A = A_1 \subset H$, as $0 \in A$. Hence $\langle A \rangle \subset H$ and $|\langle A \rangle|$ is prime which contradicts the assumptions. Hence $K \geq 2$. Similarly, we obtain $N \geq 2$.

Note that A_1, A_K are disjoint subsets of A and B_1, B_N are disjoint subsets of B by Theorem 7 (i). This implies that $|A_1|+|B_1| \leq (|A|+|B|)/2$ or $|A_K|+|B_N| \leq (|A|+|B|)/2$.

First suppose $|A_1| + |B_1| \leq (|A| + |B|)/2$. Recall that $A_1 + B_1$ does not contain a unique sum. Note that we may assume $A_1 \subset H$ and $B_1 \subset H$ by replacing A_1 by $A_1 + g$ and B_1 by $B_1 + h$ for some $g, h \in G$, if necessary. Suppose $|H| > \sqrt[4]{12}^{|A_1|+|B_1|-2}$. Then applying Theorem 7 to $A_1 + B_1 \subset H$ yields $A_1' \subset A_1$ and $B_1' \subset B_1$ such that $A_1' + B_1'$ does not contain a unique sum. Furthermore, $|A_1'| = |B_1'| = 1$, as H is of prime order and thus the only proper subgroup of H is the trivial group. But $|A_1'| = |B_1'| = 1$ is impossible, as $A_1' + B_1'$ does not contain a unique sum, a contradiction. Hence

$$|H| \leq \sqrt[4]{12}^{|A_1|+|B_1|-2} \leq \sqrt[4]{12}^{(|A|+|B|)/2-2} < \sqrt[8]{12}^{|A|+|B|-2}.$$

But this is impossible, as $p > \sqrt[8]{12}^{|A|+|B|-2}$ is the smallest prime divisor of $|G|$. Similarly, we get a contradiction if $|A_K| + |B_N| \leq (|A| + |B|)/2$. This completes the proof of part (b).

For the proof of part (c), suppose that A does not have a unique difference. We apply Theorem 9 to obtain a contradiction. If $\langle A \rangle$ is a proper subgroup of G, then we replace G by $\langle A \rangle$ and apply Theorem 9 then. Thus we may assume $\langle A \rangle = G$. Since, by assumption, $|G|$ is not a prime and $p > (\sqrt[4]{12})^{|A|}$ is the smallest prime divisor of $|G|$, we conclude $|G| \geq p^2 > (\sqrt{12})^{|A|} > 2^{|A|-1}$. Hence Theorem 9 shows that there is a subgroup H of G with $|H| \leq 2^{|A|-1}$ and disjoint nonempty subsets $A_1, \ldots, A_K$ of G, $K \geq 2$, such that conditions (i)-(iv) in Theorem 9 hold. Note that $|H| < p^2$, as $p^2 > 2^{|A|-1}$. Therefore, $|H|$ is a prime. Recall that $A_K - A_1$ contains no unique difference by condition (iii) of Theorem 9. Moreover, by condition (iv) of Theorem 9, we have $A_1 \subset H + g_1$ and $A_K \subset H + g_K$ for some $g_1, g_K \in G$. We can write $A_1 = X + g_1$ and $A_K = Y + g_K$ where X, Y are subsets of H. It follows that $X - Y$ does not contain a unique difference. But $|X| + |Y| \leq |A|$ and $|H| \geq p > \sqrt[4]{12}^{|A|} > \sqrt[4]{12}^{|X|+|Y|-2}$ and thus we can apply Theorem 7 to the subsets X and $-Y$ of H. This yields disjoint sets $X_1, \dots, X_S$ and $Y_1, \dots, Y_T$ with $X = \bigcup X_i$ and $-Y = \bigcup Y_j$ such that $X_1 + Y_1$ does not contain a unique sum. Note that $|X_1| = |Y_1| = 1$, as each X_i and Y_j is contained in a coset of a proper subgroup of H and the only proper subgroup of H is the trivial group. But this contradicts the fact that $X_1 + Y_1$ contains a unique sum. This completes the proof of part (c). □

5 Application to Circulant Weighing Matrices

In this section, we briefly describe how Theorem 3 can be used to prove a necessary condition for the existence of circulant weighing matrices. We refer to [17, Section 1.3] for the necessary background. A *$CW(v, k)$ matrix* is a circulant $v \times v$ matrix H with entries $0, \pm 1$ only such that $HH^T = kI$ where I is the identity matrix of order v. There is an extensive literature on circulant weighing matrices, see [1, 2, 5, 8], for instance.

Let G be a cyclic group of order v. It can be shown that a $CW(v, k)$ matrix exists if and only if there are $a_g \in \{-1, 0, 1\}$ such that the element $X = \sum_{g \in G} a_g g$ of the group ring $\mathbb{Z}[G]$ satisfies $XX^{(-1)} = k$ (see [17, Lem. 1.3.9]). Write $\mathrm{supp}(X) = \{g \in G : a_g \neq 0\}$. The weighing matrix corresponding to X is called *proper* if there is no subgroup U of G, $U \neq G$, such that $\mathrm{supp}(X)$ is contained in a coset of U. It is straightforward to check that $XX^{(-1)} = k$ implies that $\mathrm{supp}(X)$ does not have a unique difference.

Using Theorem 3, we obtain the following new result on circulant weighing matrices.

Theorem 10. *Suppose that v is not a prime and let p be the smallest prime divisor of v. If a proper $CW(v, k)$ matrix exists, then*

$$p \leq 12^{k/4}.$$

Proof. Let G be a cyclic group of order v and let $X \in \sum_{g \in G} a_g g$ be the group element corresponding to a proper $CW(v, k)$ matrix. Write $A = \mathrm{supp}(X)$. The properness assumption guarantees that $\langle A \rangle = G$ and thus $|\langle A \rangle|$ is not a prime. Comparing the coefficient of the identity element on both sides of $XX^{(-1)} = k$, we get $\sum_{g \in G} a_g^2 = k$. As $a_g \in \{-1, 0, 1\}$ for all g, this implies $|A| = k$. Because A has no unique difference, Theorem 3 (c) shows that $p \leq \left(\sqrt[4]{12}\right)^{|A|} = 12^{k/4}$. $\square$

Theorem 10 compares favorably with the bound $p \leq 2^{k-1}$ that follows from Result 2.

6 An Example

Finally, we present an example that illustrates the techniques used in this paper. Since we can replace A, B by $A + g$, $B + h$, respectively, for some group elements g, h, without affecting the unique sum property, we can make certain assumptions on A and B. We indicate such assumptions by the phrase "up to translation".

6.1 Subsets of C_{49p} with No Unique Sums

Let $p > 31$ be a prime. The results of this paper can be used to find all subsets A, B of $G = C_{49p}$ with $|A| + |B| \leq 14$ and $\langle A \rangle = \langle B \rangle = G$, such that $A + B$ does not contain a unique sum. There are numerous other cases that can be treated similarly; we focus on C_{49p} here, since we find it particularly instructive. We spare the reader the tedious proof and only state the final result (details can be provided upon request). In the following, we identify the subgroup of G of order 7 with $\{0, \ldots, 6\}$. For an integer x, let $\overline{x}$ denote the unique integer with $\overline{x} \equiv x \pmod 7$ and $0 \leq x \leq 6$.

Theorem 11. *Let $p > 31$ be a prime and suppose that A, B are subsets of $G = C_{49p}$ with $|A| + |B| \leq 14$ and $\langle A \rangle = \langle B \rangle = G$, such that $A + B$ does not contain a unique sum. Then there are elements g, h of G order order $49p$ such that, up to translation and interchanging A and B, we have*

$$\begin{aligned} A = A_1 \cup (A_2' + g) &\text{ and } B = B_1 \cup (B_2' + h), \\ A_1 &= \{\overline{0}, \overline{c}, \overline{3c}\}, \\ B_1 &= \{\overline{0}, \overline{1}, \overline{2}, \overline{3c^3 + 1}\}, \\ \{A_2', B_2'\} &= \left\{ \{\overline{0}, \overline{d}, \overline{3d}\}, \{\overline{s}, \overline{s+1}, \overline{s+2}, \overline{s + 3d^3 + 1}\} \right\} \end{aligned} \tag{17}$$

for some integers c, d with $1 \leq c, d \leq 6$. Furthermore, one of the following holds.

(a) *g and h are in different cosets of H',*

$$A'_2 = \{\overline{0}, \overline{d}, \overline{3d}\}, B'_2 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3d^3+1}\} \textit{ and } d^3 \equiv c^3 \pmod 7.$$

(b) *$g = h$ and $|A'_2| = 3$.*

(c) *$g = h$, $|A'_2| = 4$ and the triple (c, d, s) is not one of the following.*
$(1,1,5), (1,1,6), (1,2,4), (1,4,2), (2,1,4), (2,2,3), (2,4,1), (3,3,4)(3,5,2), (3,6,1), (3,6,6),$
$(4,1,2), (4,2,1), (4,4,6), (5,3,2), (5,5,0), (5,5,6), (6,3,1), (6,3,6), (6,6,5)$

It is straightforward to check that $A+B$ does not contain a unique sum if the conditions in Theorem 11 are satisfied. Hence Theorem 11 provides a complete classification of the sets A, B we have been looking for.

6.2 Illustration of Theorem 7

We now pick one pair of sets A, B given by Theorem 11 and illustrate the decomposition of A and B given in Theorem 7 on this example. We take $p = 37$ and thus work in the group $G = C_{49 \cdot 37} = C_{1813}$. We represent the elements of G by integers in the range $0, \ldots, 1812$ and use addition modulo 1813 as group operation. Note that $H' = \{0, 259, \ldots, 6 \cdot 259\}$ in this notation. We take $g = 1$, $h = 2$, $c = d = 1$ in Theorem 11. In this case, we have

$$A = \{0, 1, 259, 260, 777, 778\}, \ B = \{0, 2, 259, 261, 518, 520, 1036, 1038\}.$$

Following the proof of Theorem 7 (and using its notation), we obtain $K = 2, N = 2$, $\alpha_1 = \beta_1 = 0$ and $\alpha_2 = \beta_2 = 1$. Moreover,

$$\begin{aligned} A_1 &= \{a_i : u_i = 0\} = \{a_0, a_4, a_5\} = \{0, 259, 777\}, \\ A_2 &= \{a_i : u_i = 1\} = \{a_1, a_2, a_3\} = \{1, 260, 778\}, \\ B_1 &= \{b_i : v_i = 0\} = \{b_0, b_1, b_2, b_3\} = \{0, 259, 518, 1036\}, \\ B_2 &= \{b_i : v_i = 1\} = \{b_4, b_5, b_6, b_7\} = \{2, 261, 520, 1038\}. \end{aligned}$$

It is straightforward to check that these sets A_i and B_i satisfy all conditions in Theorem 7.

Acknowledgment We thank the anonymous referee for his careful reading and thoughtful suggestions that helped to improve the readability of the paper.

References

[1] K. T. Arasu and J. F. Dillon: Perfect ternary arrays. *In: Difference Sets, Sequences, and their Correlation Properties.* NATO Science Series **542**, Kluwer 1999, 1–15.

[2] K.T. Arasu, J.F. Dillon, D. Jungnickel, A. Pott: The solution of the Waterloo problem. *J. Combin. Theory A* **71** (1995), 316–331.

[3] J. Browkin, B. Diviš, A. Schinzel: Addition of Sequences in General Fields. *Monatsh. Math.* **82** (1976), 261–268.

[4] E. Croot, T. Schoen: On sumsets and spectral gaps. *Acta Arith.* **136** (2009), 47–55.

[5] P. Eades: Circulant (v, k, λ)-designs. *In: Combinatorial Mathematics VII, Lecture Notes in Math.* **829**, Springer 1980, 83–93.

[6] B. J. Green and I. Z. Ruzsa: Freiman's theorem in an arbitrary Abelian group. *J. London Math. Soc.* **75** (2007), 163–175.

[7] D. J. Grynkiewicz: *Structural additive theory.* Developments in Mathematics **30**. Springer 2013.

[8] C. Koukouvinos, J. Seberry: Weighing matrices and their applications. *J. Stat. Plann. Inf.* **62** (1997), 91–101.

[9] K. H. Leung and B. Schmidt: Finiteness of circulant weighing matrices of fixed weight. *J. Combin. Theory Ser. A*, **116** (2011), 908–919.

[10] K. H. Leung and B. Schmidt: Structure of Group Invariant Weighing Matrices of Small Weight. *J. Comb. Theory Ser. A* **154** (2018), 114–128.

[11] V. F. Lev: The rectifiability threshold in abelian groups. *Combinatorica* **28** (2008) 491–497.

[12] J. H. Loxton: On the maximum modulus of cyclotomic integers. *Acta Arith.* **22** (1972), 69–85.

[13] J. H. Loxton: On two problems of E. M. Robinson about sums of roots of unity. *Acta Arith.* **26** (1974), 159–174.

[14] Z. Nedev: An algorithm for finding a nearly minimal balanced set in $\mathbb{F}_p$. *Math. Comp.* **268** (2009), 2259–2267.

[15] Z. Nedev: Lower bound for balanced sets. *Theoret. Comput. Sci.* **460** (2012), 89–93.

[16] Z. Nedev, A. Quas: Balanced sets and the vector game. *Int. J. Number Theory* **4** (2008), 339–347.

[17] B. Schmidt: *Characters and Cyclotomic Fields in Finite Geometry.* Lecture Notes in Mathematics **1797**, Springer 2002.

[18] E. G. Straus: Differences of residues mod *p*. *J. Number Theory* **8** (1976) 40–42.

[19] T. Tao, V. Vu: *Additive combinatorics.* Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press 2006.