Abstract

Let $A, B$ be subsets of a finite abelian group $G$ such that $A + B$ does not contain a unique sum, i.e., there is no $g \in G$ with a unique representation $g = a + b$, $a \in A$, $b \in B$. Under the condition that $|A| + |B|$ is small compared to the order of $G$, we obtain detailed information on the structure of $A$ and $B$ by studying the Smith Normal Form of the linear relations the elements of $A$ and $B$ have to satisfy. As a consequence, we are able to substantially improve and generalize previously known results which provide sufficient conditions for the existence of unique sums and
differences. The case $B = -A$, i.e., the problem of unique differences in a subset of a finite abelian group, is relevant to the theory of weighing matrices and Weil numbers. In particular, our result on the structure of sets with no unique differences is surprisingly well suited to determine the structure of group invariant weighing matrices of small weight. Using this connection, we prove that, for fixed $n$, the set of all weighing matrices of weight $n$, which are invariant under an abelian group, is finitely generated. We also obtain a result on Weil numbers that improves a result of Loxton and implies new bounds on the orders of certain explicitly given subgroups of class groups of cyclotomic fields.

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 $g = a + a'$.

The main objective in studying these problems is to find sufficient conditions for the existence of unique sums and unique differences. Such results are relevant in a variety of contexts, for instance, cyclotomic integers of small modulus [10, 11], field extensions [3], spectral gaps of subsets of $\mathbb{F}_p$ [4], balanced sets [12, 13, 14], and circulant weighing matrices [8].

We denote the cyclic group of order $v$ by $C_v$. 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 in [3], where the following was proved.

**Result 1** Let $p$ be a prime and $A, B \subset C_p$. If $p > \min\{2^{|A|+|B|-2}, |A||B|-1, |B||A|-1\}$, then $A + B$ contains a unique sum. Furthermore, if $p > 2^{|A|-1}$, then $A$ has a unique difference.
and a unique sum.

Lev [9] generalized and partially strengthened Result 1 and obtained the following.

**Result 2** Let $A, B$ be subsets of a finite abelian group $G$. If all prime divisors of $|G|$ are larger than $2^{|A|+|B|-3}$, then $A + B$ contains a unique sum.

In this paper, one of our aims is to improve and generalize Results 1 and 2. In this vain, we obtain Theorems 3 and 4 stated below. For a subset $A$ of a group $G$, we write $\langle A \rangle$ for the subgroup of $G$ generated by $A$.

**Theorem 3** Let $G$ be a finite abelian group, and let $A, B$ be subsets of $G$ with $0 \in A \cap B$. Let $p$ be the smallest prime divisor of the order of $G$.

(a) If $p > (\sqrt[3]{12})^{|A|+|B|-2}$, then $A + B$ contains a unique sum.

(b) If $p > (\sqrt[3]{12})^{|A|+|B|-2}$ and both $|\langle A \rangle|$ and $|\langle B \rangle|$ are not prime, then $A + B$ contains a unique sum.

**Theorem 4** Let $G$ be a finite abelian group and let $A$ be a subset of $G$ with $0 \in A$. Let $p$ be the smallest prime divisor of the order of $G$.

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

(b) If $p > (\sqrt[3]{12})^{|A|}$ and $|\langle A \rangle|$ is not a prime, then $A$ has a unique difference.

But our motivation also stems from the study of group invariant weighing matrices and Weil numbers. In this context, we need to deal with subsets of abelian groups which do not have unique differences and need detailed information on their structure. To explain this connection, we introduce some notation. We will write groups multiplicatively now to distinguish the group operation from the addition in the group ring.

Let $G$ be a finite multiplicative group of order $v$ and let $\mathbb{Z}[G]$ denote the corresponding integral group ring. Any $X \in \mathbb{Z}[G]$ can be written as $X = \sum_{g \in G} a_g g$ with $a_g \in \mathbb{Z}$. The integers $a_g$ are called the **coefficients** of $X$. We write $|X| = \sum_{g \in G} a_g$ and $X^{-1} =$
\[ \sum a_g g^{-1} \]. We identify a subset \( S \) of \( G \) with the group ring element \( \sum_{g \in S} g \). For the identity element \( 1_G \) of \( G \) and an integer \( s \), we write \( s \) for the group ring element \( s1_G \). The set \( \text{supp}(X) = \{ g \in G : a_g \neq 0 \} \) is called the support of \( X \).

A weighing matrix \( W(v, n) \) is a \( v \times v \) matrix \( M \) with entries \( 0, \pm 1 \) only such that \( MM^T = n \). The integer \( v \) is called the order of \( M \) and \( n \) its weight. We say that a \( v \times v \) matrix \( H = (h_{f,g})_{f,g \in G} \), indexed with the elements of \( G \), is \( G \)-invariant if \( h_{f,kg} = h_{f,g} \) for all \( f, g, k \in G \).

The following is well known, see [16, Lem. 1.3.9].

**Lemma 5** Let \( G \) be a finite group of order \( v \). The existence of \( G \)-invariant weighing matrix \( W(v, n) \) is equivalent to the existence of \( X \in \mathbb{Z}[G] \) with coefficients \( 0, \pm 1 \) only such that \( XX^{-1} = n \).

In view of Lemma 5, we will always view \( G \)-invariant weighing matrices as elements of \( \mathbb{Z}[G] \). The main connection between group invariant weighing matrices and unique differences is given by the following.

**Lemma 6** Suppose that \( X \in \mathbb{Z}[G] \) is a solution of \( XX^{-1} = n \) and that \( |\text{supp}(X)| > 1 \). Then \( \text{supp}(X) \) has no unique difference.

**Proof** Write \( X = \sum_{g \in S} a_g g \) where \( S = \text{supp}(X) \), \( a_g \in \mathbb{Z} \), and \( a_g \neq 0 \) for all \( g \in S \). Suppose that \( \text{supp}(X) \) has a unique difference. Then there is \( k \in G \) such that there is exactly one pair \((c, d)\), \( c, d \in \text{supp}(X) \), with \( k = cd^{-1} \) (recall that we write \( G \) multiplicatively). Note that the identity element of \( G \) is not a unique difference of \( \text{supp}(X) \), as \( |\text{supp}(X)| > 1 \). Hence \( k \) is not the identity element of \( G \). But the coefficient of \( k \) in \( XX^{-1} \) is \( a_c a_d \neq 0 \), as \( k = cd^{-1} \) is the only representation of \( k \) as a difference of elements of \( \text{supp}(X) \). This contradicts \( XX^{-1} = n \). Q.E.D.

To formulate our main result on group invariant weighing matrices, we need the following notion.

**Definition 7** Let \( G \) be a finite abelian group and let \( H \) be a subgroup of \( G \). We say that \( X \in \mathbb{Z}[G] \) is decomposable over \( H \) if there exist an integer \( K \geq 1 \), \( X_1, ..., X_K \in \mathbb{Z}[H] \), and \( g_1, g_2, ..., g_K \in G \) such that \( X = \sum_{i=1}^K X_i g_i \) and

\[ a \]
(i) \( \text{supp}(X_i g_i) \cap \text{supp}(X_j g_j) = \emptyset \) whenever \( i \neq j \),

(ii) \( X_i X_j = 0 \) whenever \( i \neq j \).

A weighing matrix \( W(v, n) \) invariant under a cyclic group is called a \textbf{circulant weighing matrix} and denoted by \( CW(v, n) \). The main result of \cite{8} is the following.

\textbf{Result 8} Let \( n \) be a positive integer. There is a constant \( F(n) \), only depending on \( n \), such that every circulant weighing matrix \( CW(v, n) \) is decomposable over a group of order at most \( F(n) \).

Though the constant \( F(n) \) can be computed for any given \( n \), it is huge even for moderately sized \( n \). In particular, all primes \( \leq 4^n + 1 \) are divisors of \( F(n) \). In Section 5, we prove the following result which generalizes and dramatically improves Result 8.

\textbf{Theorem 9} Let \( n \) be a positive integer. Every weighing matrix of weight \( n \) invariant under an abelian group is decomposable over a group \( H \) of \( G \) with \( |H| \leq 2^{n-1} \).

A \( G \)-invariant weighing matrix \( X \in \mathbb{Z}[G] \) is \textbf{proper} if there is no \( g \in G \) and no proper subgroup \( U \) of \( G \) such that \( Xg \in \mathbb{Z}[U] \). Together with results from \cite{8}, Theorem 9 implies the following.

\textbf{Corollary 10} Suppose there exists a proper circulant weighing matrix \( CW(v, n) \) where \( n \) is an odd prime power. Then \( v \leq 2^{n-1} \).

Our approach also can be used to improve known results on cyclotomic integers. Write \( \zeta_m = \exp(2\pi i/m) \). The elements of the ring \( \mathbb{Z}[\zeta_m] \) are called \textbf{cyclotomic integers}. A cyclotomic integer \( Y \) is called an \textbf{\( n \)-Weil number} if \( |Y|^2 = n \). We say that \( Y \) is \textbf{trivial} if \( Y = \zeta \sqrt{n} \) for some root of unity \( \zeta \).

Weil numbers are essential for the study of difference sets and similar structures in finite abelian groups and are closely related to the structure of ideal class groups of cyclotomic fields. Necessary conditions for the existence of nontrivial Weil numbers are of particular interest. The following essentially is contained in Loxton’s work \cite[pp. 171–172]{11}. 

5
**Result 11** Let \( p \) be a prime and let \( n \) be a positive integer. Suppose that \( Y \in \mathbb{Z}[\zeta_p] \) is an \( n \)-Weil number. If \( p > 4^n \), then \( n \) is a square and \( Y \) is trivial.

It can be shown that under certain conditions the existence of an \( n \)-Weil number implies the existence of solutions to group ring equations \( XX^{(-1)} = n \). Hence, by Lemma 6, results on unique differences yield information on Weil numbers. Using this approach, we prove the following theorem in Section 6. It improves and generalizes Result 11.

**Theorem 12** Let \( p \) be a prime and let \( n, r \) be positive integers. Suppose that \( Y \in \mathbb{Z}[\zeta_p^r] \) is an \( n \)-Weil number. If \( p > \max\{4n^2 - 2n + 2, 2^{n-1}\} \), then \( n \) is a square and \( Y \) is trivial.

At the end of Section 6, to illustrate the applications of our results to class groups, we give an example of a new bound on the order of a certain subgroup of the class groups of a cyclotomic field.

All our results are based on the theorems in Section 2. These give detailed information on the structure of subsets \( A, B \) of finite abelian group for which \( A + B \) does not contain a unique sum, going beyond mere sufficient conditions for the existence of unique sums. An essential tool for the work in Section 2 will be the Smith Normal Form of the coefficient matrix corresponding to the linear equations such subsets \( A, B \) have to satisfy. This approach is similar to the construction and investigation of universal ambient groups as described in [5, Chapter 20] or [19, Chapter 5]. Our approach in Section 2, however, yields deeper results on the structure of sumsets without unique sums which require techniques different from those in [5, 19]. Moreover, the determinant bounds we establish in Section 3 for sumsets without unique sums are stronger than those used in [5, 19] for general sumsets.

For the convenience of reader, we recall the following known results which will be used later.

**Result 13 (Fourier Inversion Formula)** Let \( G \) be a finite abelian group and let \( \hat{G} \) denote the group of complex characters of \( G \). Let \( X = \sum_{g \in G} a_g g \in \mathbb{Z}[G] \). Then

\[
a_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(X g^{-1})
\]
for all $g \in G$. In particular, if $\chi(X) = 0$ for all $\chi \in \hat{G}$, then $X = 0$.

For a proof of Result 13, see [1, Section VI.3], for instance. The following determinant bound is due to Schinzel [15].

**Result 14** Let $A = (A_{ij})$ be a real $n \times n$ matrix. For $i = 1, \ldots, n$, let

$$R^+_i(A) = \sum_{j=1}^{n} \max(0, A_{ij}),$$

$$R^-_i(A) = \sum_{j=1}^{n} \max(0, -A_{ij}).$$

We have

$$|\det(A)| \leq \prod_{i=1}^{n} \max\{R^+_i(A), R^-_i(A)\}.$$ 

## 2 Main Results

In this section, we study subsets $A, B$ of a finite abelian group $G$ such that there is no unique sum in $A + B$. We will write groups additively in this section and use $0$ to denote their identity elements.

Let $a \in A$ and $b \in B$ be arbitray. Note that $A + B$ contains a unique sum if and only if $(A-a) + (B-b)$ contains a unique sum. Hence, without loss of generality, we may assume that both $A$ and $B$ contain $0$. We may also assume $\langle A \cup B \rangle = G$ as $A + B \subset \langle A \cup B \rangle$. Here $\langle C \rangle$ denotes the subgroup of $G$ generated by a subset $C$ of $G$.

All our results are based on the following theorem, which provides detailed information on the structure of subsets $A, B$ of finite abelian groups such that $A + B$ does not contain a unique sum.

**Theorem 15** Let $G$ be a finite abelian group, and let $A, B$ be subsets of $G$ with $0 \in A \cap B$ and assume that $\langle A \cup B \rangle = G$. 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 $|H| \leq (\sqrt[4]{12})^{|A|+|B|-3}$, 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 \( A_1, \ldots, A_N \) 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 \(N \geq 2\).

Before we start with the proof of Theorem 15, we set up some notation and make some preliminary observations. Write \(A = \{a_0, \ldots, a_{|A|-1}\}\) and \(B = \{b_0, \ldots, b_{|B|-1}\}\). We may assume \(a_0 = b_0 = 0\). As in the proof of Theorem 1 in [3], 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).

As \(A + B\) does not contain a unique sum, for each pair \((a_i, b_j)\), there exists at least one pair \((i', j')\) with \(i' \neq i\) and \(j' \neq j\) such that \(a_i + b_j = a_{i'} + b_{j'}\). To any such equation, we associate an equation

\[x_i + y_j = x_{i'} + y_{j'}\]  

(1)

Note that all the equations (1) are homogeneous. Furthermore, for a given pair \((i, j)\), there may be more than one pair \((i', j')\) which satisfies (1). Observe that there are \(n := |A| + |B| - 2\) variables involved (\(x_0\) and \(y_0\) do not count as variables). Set

\[\mathcal{E} = \{x_i + y_j = x_{i'} + y_{j'} : 0 \leq i, i' \leq |A| - 1, 0 \leq j, j' \leq |B| - 1, i \neq i', j \neq j', a_i + b_j = a_{i'} + b_{j'}\}\]

and \(a_i + b_j = a_{i'} + b_{j'}\) (note that there may be more than one such equation for fixed \((i, j)\)). We identify \(\mathcal{E}\) with the set of corresponding coefficient row vectors in \(\mathbb{Q}^n\). Let \(M(\mathcal{E})\) be the coefficient matrix corresponding to the equations in \(\mathcal{E}\). Note that \(M(\mathcal{E})\) is an integral matrix with entries 0, \pm 1 only. Furthermore, each row of \(M(\mathcal{E})\) has \(n = |A| + |B| - 2\) entries, at most four of which are nonzero.
Note that there are rows of $M(\mathcal{E})$ which contain less than four nonzero entries. For instance, an equation $x_0 + y_j = x_{i'} + y_{i'}$ corresponds to a row of $M(\mathcal{E})$ with at most three nonzero entries, as $x_0 = 0$ and thus this equation is equivalent to $y_j = x_{i'} + y_{i'}$. Write $z_0 = (a_1, ..., a_{|A|-1}, b_1, ..., b_{|B|-1})^t$. Then

$$M(\mathcal{E})z_0 = 0$$

by the definition of $M(\mathcal{E})$. For a subset $\mathcal{C}$ of $\mathcal{E}$, let $M(\mathcal{C})$ denote the coefficient matrix corresponding to the equations in $\mathcal{C}$. Recall that $n = |A| + |B| - 2$. The following property of $\mathcal{E}$ is crucial for the proof of Theorem 15.

**Lemma 16** There is a subset $\mathcal{B}$ of $\mathcal{E}$ with the following properties.

(a) $\mathcal{B}$ is a basis of $\text{span}_\mathbb{Q}(\mathcal{E})$.

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

(c) If $\text{rank}_\mathbb{Q}(M(\mathcal{B})) < n$, then $|\det(M')| \leq (\sqrt[4]{12})^{|A|+|B|-3}$ for every invertible submatrix $M'$ of $M(\mathcal{B})$.

As the proof of Lemma 16 is quite complicated, we postpone it to Section 3.

**Remark 17** A weaker version of Lemma 16 can be proved easily: Choose any subset $\mathcal{B}$ of $\mathcal{E}$ which is a basis of $\text{span}_\mathbb{Q}(\mathcal{E})$. Note that all row vectors in $\mathcal{E}$ and thus in $\mathcal{B}$ have Euclidean norm at most 2. Thus, if $\text{rank}_\mathbb{Q}(M(\mathcal{B})) = n$, then $|\det(M(\mathcal{B}))| \leq 2^{|A|+|B|-2}$ by Hadamard’s inequality. Moreover, if $\text{rank}_\mathbb{Q}(M(\mathcal{B})) < n$, then $|\det(M')| \leq 2^{|A|+|B|-3}$ for every invertible submatrix $M'$ of $M(\mathcal{B})$, again by Hadamard’s inquality. In summary, this proves Lemma 16 with $\sqrt[4]{12}$ replaced by 2.

**Proof of Theorem 15** Let $\mathcal{B}$ be a subset of $\mathcal{E}$ with the properties stated in Lemma 16. Clearly, $|\mathcal{B}| \leq n$. Let $M = M(\mathcal{B})$ be the coefficient matrix corresponding to the equations in $\mathcal{B}$. 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 $A = \{a_0, ..., a_{|A|-1}\}$, $B = \{b_0, ..., b_{|B|-1}\}$, and that

$$Mz_0 = 0 \text{ for } z_0 = (a_1, ..., a_{|A|-1}, b_1, ..., b_{|B|-1})^t. \quad (2)$$
Let $D$ be the Smith Normal Form of $M$. Then $D$ is a diagonal matrix with diagonal entries $d_1, d_2, \ldots, d_n \in \mathbb{Z}$ such that $d_i | d_j$ whenever $i < j$. Let $S$ and $T$ be unimodular matrices with $SMT = D$. Write $s = \text{rank}_0(M)$. Note that $d_1, \ldots, d_s \neq 0$ and $d_{s+1} = d_{s+2} = \cdots = d_n = 0$. 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 \{ $Yf : f \in \mathbb{Z}^{n-s}$ \}.
(b) The solution set of $Mz = 0$, $z \in \mathbb{G}^n$, is

$$\{Xe + Yf : e \in \mathbb{G}^s, f \in \mathbb{G}^{n-s}, o(e_i)|d_i \text{ for } i = 1, \ldots, s\}.$$  

Here we write $e = (e_1, \ldots, e_s)^t$.

Proof of Claim 1: Let $R$ be either $\mathbb{Z}$ or $\mathbb{G}$. Note that $M = S^{-1}DT^{-1}$. Hence $Mz = 0$, $z \in R^n$, if and only if $DT^{-1}z = 0$. Write $T^{-1}z = \binom{e}{f}$ with $e \in R^s$, $f \in R^{n-s}$. Recall that that $d_1, \ldots, d_s \neq 0$ and $d_{s+1} = d_{s+2} = \ldots = d_n = 0$. Thus $DT^{-1}z = D\binom{e}{f} = 0$ if and only if

$$d_i e_i = 0 \text{ for } i = 1, \ldots, s. \quad (3)$$

If $R = \mathbb{Z}$, then (3) holds if and only if $e = 0$. Hence, in this case, the general solution of $Mz = 0$ is $z = T\binom{e}{f} = (X,Y)\binom{e}{f} = Yf$, $f \in \mathbb{Z}^{n-s}$. This proves part (a) of Claim 1. If $R = \mathbb{G}$, then (3) holds if and only if $o(e_i)|d_i$ for $i = 1, \ldots, s$. Hence the general solution of $Mz = 0$, $z \in \mathbb{G}^n$, is as stated in part (b) of Claim 1. This completes the proof of Claim 1.

Claim 2 $M$ does not have full rank over $\mathbb{Q}$.

Proof of Claim 2: If $M$ has full rank over $\mathbb{Q}$, then $s = n$. By (2) we have $Mz_0 = 0$ where $z_0 = (a_1, \ldots, a_{|A|-1}, b_1, \ldots, b_{|B|-1})^t \in \mathbb{G}^n$. Hence $z_0 = Xe$, $e \in \mathbb{G}^n$, and $o(e_i)|d_i$ for $i = 1, \ldots, s$ by Claim 1 (note that there is no term $Yf$ in $z_0 = Xe$, as $s = n$). Let $\langle e_1, \ldots, e_n \rangle$ denote the subgroup of $G$ generated by $e_1, \ldots, e_n$. As $z_0 = Xe$ and $X$ is an integer matrix, we conclude that all $a_i$’s and $b_i$’s are contained in $\langle e_1, \ldots, e_n \rangle$. As $o(e_i)|d_i$ for $i = 1, \ldots, s$, we have $|\langle e_1, \ldots, e_n \rangle| \leq \prod_{i=1}^n d_i$. Note that $\det(M) = \prod_{i=1}^n d_i$, since $SMT = D$ and $S, T$ are unimodular matrices. Furthermore, $\det(M) \leq (\sqrt{12})^{|A|+|B|} - 2$ by Lemma 16. Hence

$$|\langle A \cup B \rangle| \leq |\langle e_1, \ldots, e_n \rangle| \leq \det(M) \leq (\sqrt{12})^{|A|+|B|} - 2.$$
This contradicts the assumptions $\langle A \cup B \rangle = G$ and $|G| > (\sqrt{12})^{|A|+|B|-2}$ of Theorem 15. Claim 2 is proved.

Now suppose that $\text{rank}_Q(M) = s < n$. Recall that, by Claim 1, the general solution of $Mz = 0$, $z \in \mathbb{Z}^n$, is $z = Yf$, $f \in \mathbb{Z}^{n-s}$. Let $Y_1, \ldots, Y_n$ be the rows of $Y$.

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

If $\gamma_i = 0$, then $Y_i = 0$, and if $\gamma_i = \gamma_k$, then $Y_i = Y_k$. 

Proof of Claim 3: For each $i$ with $Y_i \neq 0$, the set $H_i := \{x \in \mathbb{R}^{n-s} : Y_ix = 0\}$ is a hyperplane in $\mathbb{R}^{n-s}$, and for each pair $(i, k)$ with $Y_i \neq Y_k$, the set $H_{ik} := \{x \in \mathbb{R}^{n-s} : (Y_i - Y_k)x = 0\}$ is also a hyperplane in $\mathbb{R}^{n-s}$. If $f \in \mathbb{Z}^{n-s}$ does not satisfy (4), then $Y_if = \gamma_i = 0$ for some $i$ with $Y_i \neq 0$ or $(Y_i - Y_k)f = \gamma_i - \gamma_k = 0$ for some pair $(i, k)$ with $Y_i \neq Y_k$. This means that every $f$ which does not satisfy (4) lies on at least one of the hyperplanes $H_i$ or $H_{ik}$. But any union of finitely many hyperplanes of $\mathbb{R}^{n-s}$ does not cover $\mathbb{Z}^{n-s}$. Hence there is $f \in \mathbb{Z}^{n-s}$ satisfying (4). This proves Claim 3.

Now we fix a $f \in \mathbb{Z}^{n-s}$ satisfying (4), set $\gamma = Yf$, and write

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

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

**Claim 4** For all $i, j, i', j'$ with $0 \leq i, i' \leq |A| - 1$ and $0 \leq j, j' \leq |B| - 1$ we have the following. If $a_i + b_j = a_{i'} + b_{j'}$, then $u_i + v_j = v_{i'} + v_{j'}$.

Proof of Claim 4: By the definition of $\mathcal{E}$, if $a_i + b_j = a_{i'} + b_{j'}$, then $x_i + y_j = x_{i'} + y_{j'}$ is an equation in $\mathcal{E}$. Recall that $\gamma$ satisfies $M\gamma = 0$. As $M$ is a basis of $\text{span}_\mathbb{Q}(\mathcal{E})$, we conclude that $(u_1, \ldots, u_{|A|-1}, v_1, \ldots, v_{|B|-1})^t = \gamma$ satisfies all equations in $\mathcal{E}$. Thus $x_i + y_j = x_{i'} + y_{j'}$ implies $u_i + v_j = v_{i'} + v_{j'}$ (note that the argument is still correct if $i$ or $j$ is 0, as $x_i$ or $y_j$ 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

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

for $i = 1, \ldots, K$ and $k = 1, \ldots, N$. Clearly, $A$ and $B$ are disjoint unions of the $A_i$’s and $B_k$’s, respectively. This proves part (i) of Theorem 15.

We now prove part (ii) of Theorem 15. 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, $\alpha_i + \beta_j = u_r + v_t = u_r' + v_t' = \alpha_i' + \beta_j'$. This proves part (ii) of Theorem 15.

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, $(A_1 + B_1) \cap (A_1 + B_1) = \emptyset$ 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 15.

We now proceed to part (iv) of Theorem 15. 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 $z_0 = Xe + Yf$ with $e \in G^s$, $f \in G^{n-s}$, and $o(e_i)|d_i$ 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 $H = \langle e_1, \ldots, e_s \rangle$. We will show $a_k - a_t \in H$. Recall that $\gamma = Yf$ 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 $z_0 = Xe + Yf$. Let $X_1, \ldots, X_n$ be the rows of $X$. Since $Y_k = Y_t$, we conclude

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

$$a_k - a_t = 0 - a_t = -(z_0)_t = -X_t e - Y_t f = -X_t e,$$

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 15, it remains to show

$$|H| \leq (\sqrt[4]{12})^{(|A|+|B|)-3}.$$

Note that $|H| \leq \prod_{i=1}^s d_i$, as $o(e_i)\vert d_i$ 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 Lemma 16, we have $|D_s| \leq (\sqrt[4]{12})^{(|A|+|B|)-3}$. Thus $|H| \leq (\sqrt[4]{12})^{(|A|+|B|)-3}$. Part (iv) of Theorem 15 is proved.

To prove part (v) of Theorem 15, 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, $|G| = |H| \leq (\sqrt[4]{12})^{(|A|+|B|)-3}$. 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 15. Q.E.D.

**Remark 18** If we are content with a weaker version of Theorem 15, we can avoid using Lemma 16 (whose proof is complicated and given in Section 3) by replacing $\sqrt[4]{12}$ by $2$ in the relevant bounds. Remark 17 together with the proof of Theorem 15 shows that the following weakened version of Theorem 15 is true with no need to use Lemma 16.

*Let $G$ be a finite abelian group, and let $A, B$ be subsets of $G$ with $0 \in A \cap B$ and assume that $\langle A \cup B \rangle = G$. 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 15 hold.

Next, we deal with the case of unique differences.

**Theorem 19** 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 $|H| \leq 2^{|A|-2}$, 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 $i = 1, \ldots, K$.

**Proof** We only give a short description of the proof, as it essentially uses the same arguments as the proof of Theorem 15. We may assume $a_0 = 0$. To each $a_i$, $i = 1, \ldots, |A|-1$, we associate a variable $x_i$. Furthermore, we set $x_0 = 0$ and do not view $x_0$ as a variable. As $A$ does not have a unique difference, for every pair $(i, j)$, $0 \leq i, j \leq |A|-1$, $i \neq j$, there are $i' \neq i$ and $j' \neq j$ with $a_i - a_j = a_{i'} - a_{j'}$. Let

$$\mathcal{E}' \setminus \{x_i - x_j = x_{i'} - x_{j'} : 0 \leq i, i', j, j' \leq |A|-1, i \neq i', j \neq j', and a_i - a_j = a_{i'} - a_{j'}\}.$$

As before, let $n$ denote the number of variables involved and identify $\mathcal{E}'$ with the set of corresponding coefficient row vectors in $\mathbb{Q}^n$. Note that $n = |A| - 1$. This time, it is possible that there are entries $\pm 2$ in these vectors. For instance, if $i = j' \neq 0$, then the vector corresponding to the equation $x_i - x_j = x_{i'} - x_{j'}$ has an entry $\pm 2$, as the equation is equivalent to $2x_i - x_j - x_{i'} = 0$ in this case. But note that all vectors in $\mathcal{E}'$ have entries...
0, ±1, ±2 only. Furthermore, the sum of the positive entries in each vector in \( \mathcal{E}' \) is at most 2, and the sum of the negative entries in each vector is at least −2.

Let \( \mathcal{B}' \) be any subset of \( \mathcal{E}' \) which is a basis of the vector space spanned by \( \mathcal{E}' \) over \( \mathbb{Q} \). Then \( |\mathcal{B}'| \leq n \). Let \( M' \) be the coefficient matrix corresponding to the equations in \( \mathcal{B}' \). Using Result 14, we see that \( \det(M') \leq 2^{|A|-1} \). A similar argument as in the proof of Theorem 15 shows that the assumption \(|\langle A \rangle| = |G| > 2^{|A|-1}\) implies that \( M' \) is not of full rank over \( \mathbb{Q} \).

We can then apply a similar argument as in the proof of Theorem 15 to get a solution \( \gamma = (\gamma_1, \ldots, \gamma_n)^t \in \mathbb{Z}^n \) of \( M' \gamma = 0 \) as before. Now we have \( \gamma = (u_1, \ldots, u_n)^t \) and there are no \( v_j \)'s. We define \( u_0 = 0 \). Again, we can show that \( a_i - a_j = a'_r - a'_s \) implies \( u_i - u_j = u'_r - u'_s \). Let \( \alpha_1 < \cdots < \alpha_K \) be the distinct values in the set \( \{u_i : i = 0, \ldots, n\} \) and let

\[
A_i = \{a_j : 0 \leq j \leq n, u_j = \alpha_i\}
\]

for \( i = 1, \ldots, K \), as before. Then part (i) of Theorem 19 obviously holds.

For part (ii), suppose that \( a_r - a_s = a'_r - a'_s \) for some \( a_r \in A_i \), \( a_s \in A_j \), \( a'_r \in A'_r \), \( a'_s \in A'_s \). Then there is an equation \( x_r - x_s = x'_r - x'_s \) in \( \mathcal{E}' \). As \( \gamma = (u_1, \ldots, u_n)^t \) satisfies \( M' \gamma = 0 \), the vector \( (u_1, \ldots, u_n)^t \) satisfies all equation in \( \mathcal{E}' \). Hence \( u_r - u_s = u'_r - u'_s \). As \( a_r \in A_i \), \( a_s \in A_j \), \( a'_r \in A'_r \), and \( a'_s \in A'_s \), we have \( u_r = \alpha_i \), \( u_s = \alpha_j \), \( u'_r = \alpha'_r \), and \( u'_s = \alpha'_s \). Thus \( \alpha_i - \alpha_j = \alpha'_r - \alpha'_s \). This proves part (ii).

For part (iii), recall that \( \alpha_1 < \cdots < \alpha_K \). Hence \( (A_K - A_1) \cap (A_i - A_j) = \emptyset \) for all pairs \( (i, j) \neq (K, 1) \) by part (ii), since \( \alpha_K - \alpha_1 > \alpha_i - \alpha_j \). Thus, as \( A \) has no unique difference, \( A_K - A_1 \) has no unique difference as well. Part (iii) is proved.

To prove part (iv), we proceed in the same way as in the proof of Theorem 15. Thus, for fixed \( i \), any two elements of \( A_i \) are contained in the same coset of a subgroup \( H \) of \( G \) with \( |H| \leq \det(M'') \) where \( M'' \) is an invertible submatrix of \( M' \) of order at most \( n - 1 = |A| - 2 \). Result 14 implies \( \det(M'') \leq 2^{|A|-2} \). Hence \( |H| \leq 2^{|A|-2} \) which completes the proof of part (iv).

It remains to show \( K \geq 2 \). Suppose that \( K = 1 \). Then \( A \subset H \) by part (iv), as \( 0 \in A \). But this contradicts the assumption \( \langle A \rangle = G \). Q.E.D.
The following can be proved in the same way a Theorem 19.

**Theorem 20** 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 sum, then there exists a subgroup $H$ of $G$ with $|H| \leq 2^{|A| - 2}$, an integer $K \geq 2$, integers $\alpha_1 < \cdots < \alpha_K$, and nonempty subsets $A_1, \ldots, A_K$ of $G$ such that

(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) $A_1$ and $A_K$ both do not have a unique sums.

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

3 Proof of Lemma 16

We use the notation introduced before Lemma 16. Recall that $n = |A| + |B| - 2$. To prove Lemma 16, we need to find a basis $B \subset E$ of $\text{span}_\mathbb{Q}(E)$ such that the following hold. If $\text{rank}_\mathbb{Q}(M(B)) = n$, then

$$\left| \det(M(B)) \right| \leq (\sqrt{12})^{|A|+|B|-2}. \quad (5)$$

If $\text{rank}_\mathbb{Q}(M(B)) < n$, then

$$\left| \det(M') \right| \leq (\sqrt{12})^{|A|+|B|-3} \quad (6)$$

for every invertible submatrix $M'$ of $M$.

In the following, we consider the equations in $E$ as row vectors in $\mathbb{Q}^n$. Recall that $a_0 = x_0 = 0$. By the definition of $E$, for every $i$ with $0 \leq i \leq |B| - 1$, there is an equation $y_i + x_0 = y_j + x_k$ in $E$ with $i \neq j$ and $k \neq 0$. As $x_0 = 0$, this simplifies to $y_i = y_j + x_k$. Hence, for every $i$ with $0 \leq i \leq |B| - 1$, there exist $\tau(i) \neq i$ and $\sigma(i) \neq 0$ such that the equation

$$y_i = y_{\tau(i)} + x_{\sigma(i)} \quad (7)$$
is in $E$.

Note that the row vectors corresponding to the equations (7) have Euclidean norm at most $\sqrt{3}$ while equations in $E$ involving four nonzero terms correspond to rows of Euclidean norm 2. Our first goal is to include as many equations of type (7) in the prospective basis $B$ as possible. The effect is that, for the subsequent application of Hadamard’s inequality to $\det(M(B))$ and $\det(M')$, a substantial number of factors 2 are reduced to $\sqrt{3}$ compared to the application of Hadamard’s inequality to an arbitrary basis. In addition to this improvement, we will also include as many equations of the form $x_i = y_j + x_k$ in $B$ as possible and so strengthen the bounds further.

Let us start with considering equations of type (7). Note that $\tau(i)$ and $\sigma(i)$ may not be unique. But from now on, we fix one pair $(\tau(i), \sigma(i))$ satisfying (7) for each $i$. We may then view $\tau$ and $\sigma$ as functions

$$
\tau : \{0, 1, \ldots, |B| - 1\} \to \{0, 1, \ldots, |B| - 1\},
$$

$$
\sigma : \{0, 1, \ldots, |B| - 1\} \to \{1, 2, \ldots, |A| - 1\}.
$$

We now recursively construct subsets $B_1, B_2, \ldots, B_R$ of $E$ which contain $|B| - 1$ equations of type (7) in total. These subsets will be used to build up the required basis $B$. Our goal is to maximize $\dim_{\mathbb{Q}}(\text{span}(\bigcup_{i=1}^R B_i))$. This is beneficial for the subsequent application of Hadamard’s inequality, as rows corresponding to equations of type (7) have Euclidean norm at most $\sqrt{3}$. First of all, we will choose the $B_i$’s such that each $B_i$ is linearly independent over $\mathbb{Q}$. Hence, if $\dim_{\mathbb{Q}}(\text{span}(\bigcup_{i=1}^R B_i))$ is comparatively small, this must be due to linear dependencies between different $B_i$’s. But we will show that such linear dependencies imply that we can include a comparatively large number of equations of the form $x_i = y_j + x_k$ in $B$. Thus a comparatively small number of equations (7) in $B$ fortunately can be compensated by a comparatively large number of equations of the form $x_i = y_j + x_k$. This will be enough to prove Lemma 16.

Now let us proceed to the construction of the sets $B_i$. Let $r_1 \geq 1$ be the smallest integer such that $\tau^{r_1}(1) \in \{\tau^i(1) : i = 1, \ldots, r_1\} \cup \{0\}$. Then $1, \tau(1), \ldots, \tau^{r_1-1}(1)$ are distinct nonzero integers. Renumbering the $b_i$’s, if necessary, we may assume $\tau^i(1) = i + 1$
for $i = 1, \ldots, r_1 - 1$, that is, $\tau(i) = i + 1$ for $i = 1, \ldots, r_1 - 1$. Hence, by (7), the equations $y_i = y_{i+1} + x_{\sigma(i)}$, $i = 1, \ldots, r_1 - 1$, are in $\mathcal{E}$. Moreover, the equation $y_{r_1} = y_{\tau(r_1)} + x_{\sigma(r_1)}$ is in $\mathcal{E}$ by (7). Thus

$$\mathcal{B}_1 := \{y_i = y_{i+1} + x_{\sigma(i)} : i = 1, \ldots, r_1 - 1\} \cup \{y_{r_1} = y_{\tau(r_1)} + x_{\sigma(r_1)}\} \subset \mathcal{E}.$$ 

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

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

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

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

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

Hence, by definition of $j_1$, we have

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

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

$$\tau(j) = j + 1 \text{ for } r_1 + 1 \leq j < r_2 \text{ and } \tau(r_2) < r_2. \quad (8)$$

We denote the set of equations in $\mathcal{E}$ corresponding to (8) by $\mathcal{B}_2$, i.e.,

$$\mathcal{B}_2 := \{y_i = y_{i+1} + x_{\sigma(i)} : i = r_1 + 1, \ldots, r_2 - 1\} \cup \{y_{r_2} = y_{\tau(r_2)} + x_{\sigma(r_2)}\}.$$ 

If $r_2 \neq |B| - 1$, we repeat the above argument and replace $r_1 + 1$ by $r_2 + 1$. For convenience, we set $r_0 = 0$. It is not difficult to prove inductively that there exist integers $r_0 < r_1 < r_2 < \cdots < r_R$ with $r_R = |B| - 1$ such that, after a possible renumbering of the $b_i$’s, we have

$$\tau(r_{j-1} + \ell) = r_{j-1} + \ell + 1 \text{ and } \tau(r_{j}) \leq r_{j} - 1.$$
for \( j = 1, \ldots, R \) and \( \ell = 1, \ldots, r_j - r_{j-1} - 1 \).

We thus obtain \( R \) sets \( \mathcal{B}_1, \ldots, \mathcal{B}_R \) of equations in \( E \) with

\[
\mathcal{B}_i = \{ y_j = y_{j+1} + x_{\sigma(j)} : r_{i-1} + 1 \leq j \leq r_i - 1 \} \cup \{ y_{r_i} = y_{\tau(r_i)} + x_{\sigma(r_i)} \}
\]

and \( \sum_{i=1}^{R} |\mathcal{B}_i| = |\mathcal{B}| - 1. \)

We now need to compute \( \dim_{\mathbb{Q}}(\text{span}(\bigcup_{i=1}^{R} \mathcal{B}_i)) \). We first prove two claims as a preparation. For \( j = 1, \ldots, |\mathcal{B}| - 1 \), set

\[
G_j = -y_j + y_{j+1} + x_{\sigma(j)} \text{ if } r_{i-1} + 1 \leq j \leq r_i - 1,
\]

\[
G_j = -y_{r_i} + y_{\tau(r_i)} + x_{\sigma(r_i)} \text{ if } j = r_i
\]

for some \( i \in \{1, \ldots, R\} \).

**Claim 1** Suppose there are scalars \( \lambda_{r_{i-1}+1}, \ldots, \lambda_{r_i} \in \mathbb{Q} \), not all zero, such that in \( S = \sum_{j=r_{i-1}+1}^{r_i} \lambda_j G_j \) the coefficients of \( y_{r_{i-1}+1}, y_{r_{i-1}+2}, \ldots, y_{r_i} \) all vanish. Then \( \lambda_{r_i} \neq 0 \), \( r_i \geq r_{i-1} + 2 \), and \( r_{i-1} + 1 \leq \tau(r_i) \leq r_i - 1 \). Furthermore,

\[
S = \lambda_{r_i} \sum_{j=\tau(r_i)}^{r_i} x_{\sigma(j)}. \tag{9}
\]

Proof of the Claim: We first show \( r_i \geq r_{i-1} + 2 \). Recall that \( r_i > r_{i-1} \) by definition. Suppose that \( r_i = r_{i-1} + 1 \). Then \( S = \lambda_{r_i} G_{r_i} = \lambda_{r_i} (-y_{r_i} + y_{\tau(r_i)} + x_{\sigma(r_i)}) \) and \( \lambda_{r_i} \neq 0 \). Since \( \tau(r_i) \neq r_i \), the coefficient of \( y_{r_i} \) in \( S \) does not vanish, contradicting the assumptions. Hence \( r_i \geq r_{i-1} + 2 \).

For the proof of (9), note that

\[
S = \lambda_{r_i} (-y_{r_i} + y_{\tau(r_i)} + x_{\sigma(r_i)}) + \sum_{j=r_{i-1}+1}^{r_i-1} \lambda_j (-y_j + y_{j+1} + x_{\sigma(j)}).
\]

If \( \lambda_j = 0 \) for \( j = r_{i-1} + 1, \ldots, r_i - 1 \), then \( \lambda_{r_i} \neq 0 \) and the coefficient of \( y_{r_i} \) in \( S \) does not vanish, a contradiction. Thus there is at least one \( j \) with \( r_{i-1} + 1 \leq j \leq r_i - 1 \) and \( \lambda_j \neq 0 \). Let \( j_0 \) the smallest such \( j \). Then

\[
S = \lambda_{r_i} (-y_{r_i} + y_{\tau(r_i)} + x_{\sigma(r_i)}) + \sum_{j=j_0}^{r_i-1} \lambda_j (-y_j + y_{j+1} + x_{\sigma(j)}). \tag{10}
\]
Note that, in the sum on the right hand side of (10), the variable $y_{j_0}$ only occurs for $j = j_0$. Furthermore, $y_{j_0}$ occurs with a nonzero coefficient in the sum, as $\lambda_{j_0} \neq 0$. Since the coefficient of $y_{j_0}$ in $S$ vanishes by assumption, $y_{j_0}$ also occurs with a nonzero coefficient in the first term on the right hand side of (10), i.e., in

$$\lambda_{r_i}(-y_{r_i} + x_{\tau(r_i)}).$$

This implies $\lambda_{r_i} \neq 0$. Furthermore, as $j_0 < r_i$, we must have $\tau(r_i) = j_0$. Hence we have

$$S = \lambda_{r_i}(-y_{r_i} + y_{j_0} + x_{\sigma(r_i)}) + \sum_{j=j_0}^{r_i-1} \lambda_j(-y_j + y_{j+1} + x_{\sigma(j)}). \quad (11)$$

Since the coefficient of $y_{j_0}$ in $S$ vanishes, we get $\lambda_{r_i} = \lambda_{j_0}$. As the coefficient of $y_{j_0+1}$ in $S$ vanishes, we have $\lambda_{j_0} = \lambda_{j_0+1}$. Continuing in this way, we get $\lambda_{r_i} = \lambda_{j_0} = \lambda_{j_0+1} = \cdots = \lambda_{r_i-1}$. Thus $S = \lambda_{r_i} \sum_{j=j_0}^{r_i} x_{\sigma(j)}$. This proves Claim 1.

For $i = 2, 3, \ldots, R$, we define

$$\delta_i := \dim_Q \text{span}(B_i) \cap \text{span}(B_1 \cup \cdots \cup B_{i-1}).$$

**Claim 2** We have $\delta_i \in \{0, 1\}$ for all $i$. Furthermore,

$$|\{\sigma(j) : j = 1, \ldots, r_i\}| \leq |\{\sigma(j) : j = 1, \ldots, r_{i-1}\}| + |B_i| - 2\delta_i \quad (12)$$

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

Proof of Claim 2: We identify $B_i$ with $\{G_{r_{i-1}+1}, \ldots, G_{r_i}\}$. If $\delta_i = 0$, then (12) holds. Thus suppose $\delta_i > 0$. We first show $\delta_i = 1$. Suppose $T \in \text{span}(B_i) \cap \text{span}(B_1 \cup \cdots \cup B_{i-1})$, $T \neq 0$. We can write $T = \sum_{j=r_{i-1}+1}^{r_i} \lambda_j G_j$ with $\lambda_j \in Q$, since $T \in \text{span}(B_i)$. Furthermore, not all $\lambda_j$’s are zero. Note that, by definition, the equations in $B_1, \ldots, B_{i-1}$ do not involve any of the variables $y_{r_{i-1}+1}, \ldots, y_{r_i}$. Thus, as $T \in \text{span}(B_1 \cup \cdots \cup B_{i-1})$, the coefficients of $y_{r_{i-1}+1}, \ldots, y_{r_i}$ in $T$ all vanish. By Claim 1, this implies $\lambda_{r_i} \neq 0$, $r_i \geq r_{i-1} + 2$, and

$$T = \lambda_{r_i} \sum_{j=\tau(r_i)}^{r_i} x_{\sigma(j)} \quad (13)$$

20
where \( r_{i-1} + 1 \leq \tau(r_i) \leq r_i - 1 \). Hence \( \text{span}(B_i) \cap \text{span}(B_1 \cup \cdots \cup B_{i-1}) \) is spanned by \( T \) and thus \( \delta_i = 1 \).

It remains to prove (12). Note that the sum in (13) has \( r_i - \tau(r_i) + 1 \) terms. Since \( T \in \text{span}(B_1 \cup \cdots \cup B_{i-1}) \), each variable \( x_{\sigma(j)}, \tau(r_i) \leq j \leq r_i \), must occur in at least one equation in \( B_1 \cup \cdots \cup B_{i-1} \). Note that \( |B_i| - (r_i - \tau(r_i) + 1) \leq 2 \), as \( r_i - \tau(r_i) \geq 1 \). This proves (12) and the proof of Claim 2 is completed.

Now we are ready to compute \( \dim_Q(\text{span}(\bigcup_{i=1}^R B_i)) \). Recall that \( \sum_{i=1}^R |B_i| = |B| - 1 \). First note that Claim 1 shows that each \( B_i \) is linearly independent. By the definition of the \( \delta_i \)'s, this implies

\[
\dim_Q(\text{span}(\bigcup_{i=1}^R B_i)) = |B_i| + \sum_{i=2}^R (|B_i| - \delta_i) = |B| - 1 - \sum_{i=2}^R \delta_i.
\]

On the other hand, by (12), we have

\[
|\{\sigma(j) : j = 1, \ldots, r_R\}| \leq |\{\sigma(j) : j = 1, \ldots, r_{R-1}\}| + |B_R| - 2\delta_R
\]

\[
\leq |\{\sigma(j) : j = 1, \ldots, r_{R-2}\}| + |B_R| + |B_{R-1}| - 2(\delta_R + \delta_{R-1})
\]

\[
\vdots
\]

\[
\leq |\{\sigma(j) : j = 1, \ldots, r_1\}| + \sum_{i=2}^R (|B_i| - 2\delta_i)
\]

\[
\leq |B_1| + \sum_{i=2}^R (|B_i| - 2\delta_i)
\]

\[
= |B| - 1 - 2 \sum_{i=2}^R \delta_i.
\]

Recall that \( r_R = |B| - 1 \). Write \( L = |\{\sigma(j) : j = 1, \ldots, |B| - 1\}| \) and \( k = \sum_{i=2}^R \delta_i \). Then, by what we have shown, \( \dim_Q(\text{span}(\bigcup_{i=1}^R B_i)) = |B| - k - 1 \) and \( L \leq |B| - 2k - 1 \).

Renumbering the \( a_i \)'s, if necessary, we may assume \( \{\sigma(j) : j = 1, \ldots, |B| - 1\} = \{1, \ldots, L\} \). 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 $a_i = a_j + b_k$ instead of $b_i = a_j + b_k$. We obtain functions

$$
\alpha : \{0, 1, \ldots, |A| - 1\} \rightarrow \{0, 1, \ldots, |A| - 1\},$
$$
$$
\beta : \{0, 1, \ldots, |A| - 1\} \rightarrow \{1, 2, \ldots, |B| - 1\}.
$$

such that

$$a_i = a_{\alpha(i)} + b_{\beta(i)},$$

$\alpha(i) \neq i$, and $\beta(i) \neq 0$ for $i = 0, \ldots, |A| - 1$. Hence, by the definition of $\mathcal{E}$, the equations $x_i = x_{\alpha(i)} + y_{\beta(i)}$ are in $\mathcal{E}$ for $i = 0, \ldots, |A| - 1$.

Let $\mathcal{C}$ be a basis of $\text{span}(\bigcup_{i=1}^{R} \mathcal{B}_i)$. Note that $|\mathcal{C}| = |B| - k - 1$. Let

$$\mathcal{D} = \{x_i = x_{\alpha(i)} + y_{\beta(i)} : L + 1 \leq i \leq |A| - 1\}.$$

Note that $\mathcal{D}$ is disjoint from $\mathcal{C}$, as the variables $x_i$, $L + 1 \leq i \leq |A| - 1$, do not occur in any of the equations in $\bigcup_{i=1}^{R} \mathcal{B}_i$ and thus not in any of the equations in $\mathcal{C}$. Let $\mathcal{F}$ be a subset of $\mathcal{D}$ such that $\mathcal{C} \cup \mathcal{F}$ is a basis of $\text{span}_Q(\mathcal{C} \cup \mathcal{D})$. We claim that

$$|\mathcal{C} \cup \mathcal{F}| \geq (|A| + |B| - 1)/2.$$

Since $\mathcal{D} \subset \text{span}_Q(\mathcal{C} \cup \mathcal{F})$, every $x_i$ with $L + 1 \leq i \leq |A| - 1$ must appear in at least one equation in $\mathcal{B} \cup \mathcal{F}$. Since none of these $x_i$’s appears in any of the equations in $\mathcal{C}$, they all must occur in equations in $\mathcal{F}$. Since there are $|A| - 1 - L$ such $x_i$’s and each equation in $\mathcal{F}$ involves at most two $x_i$’s, the set $\mathcal{F}$ must contain at least $(|A| - 1 - L)/2$ equations. Recall that $L \leq |B| - 2k - 1$ and $|\mathcal{C}| = |B| - k - 1$. Hence

$$|\mathcal{C} \cup \mathcal{F}| = |\mathcal{C}| + |\mathcal{F}|$$
$$\geq |B| - k - 1 + (|A| - 1 - L)/2$$
$$\geq |B| - k - 1 + [(|A| - 1) - (|B| - 2k - 1)]/2$$
$$= (|A| + |B| - 1)/2.$$

Recall that $\text{dim span}(\mathcal{E}) \leq |A| + |B| - 2$. Hence we can extend $\mathcal{C} \cup \mathcal{F}$ to a basis $\mathcal{B}$ of $\text{span}(\mathcal{E})$ by adjoining at most $(|A| + |B| - 3)/2$ further equations from $\mathcal{E}$ to $\mathcal{C} \cup \mathcal{F}$. 

22
Let $M(B)$ be the coefficient matrix corresponding to the equations in $B$. Note that the Euclidean norm of the row vectors of $M(B)$ corresponding to equations in $C \cup F$ is at most $\sqrt{3}$ and the Euclidean norm of the row vectors corresponding to equations in $B \setminus (C \cup F)$ is at most 2. Recall that $n = |A| + |B| - 2$. Hence, if rank$_Q(M(B)) = n$, then

$$|\det(M(B))| \leq 2^{(|A|+|B|-3)/2} \sqrt{3}^{[(|A|+|B|-1)/2]} < \sqrt{12}^{(|A|+|B|-2)/2},$$

using Hadamard’s inequality. This proves (5).

Now suppose rank$_Q(M(B)) < n$, say, rank$_Q(M(B)) = n - t$ with $t \geq 1$. Let $M'$ be an invertible submatrix of $M(B)$. Then at least $(|A| + |B| - 1)/2 - t$ rows of $M'$ correspond to equations in $C \cup F$. Hence, again using Hadamard’s inequality,

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

This proves (6). The proof of Lemma 16 is complete. Q.E.D.

Remark 21 The bounds in Lemma 16 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 $B$ of span($E$) such that $\det(M') \leq \min(|A|^{|B|'-1}, |B|^{|A|'-1})$ for every invertible submatrix $M'$ of the coefficient matrix corresponding to $B$.

4 Proofs of Theorems 3 and 4

We now prove the first two theorems stated in the introduction.

Proof of Theorem 3 Suppose that $A + B$ contains no unique sum. We are going to apply Theorem 15 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 15 then. Thus we may assume $\langle A \cup B \rangle = G$. Recall that $p$ is the smallest prime divisor of $|G|$. If $p > \sqrt[4]{12}^{(|A|+|B|-2)}$ 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 $|G| > \sqrt[12]{2^{(|A|+|B|)-2}}$. By Theorem 15, 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 15. Recall that $|H| \leq \sqrt[12]{2^{(|A|+|B|)-3}}$. Note that $|H| = 1$ is impossible, as $|A_1| = |B_1| = 1$ then and $A_1 + B_1$ would not contain a unique sum. Thus $|H| > 1$.

(a) Let $q$ be a prime divisor of $|H|$. Then $q \leq |H| \leq \sqrt[12]{2^{(|A|+|B|)-3}}$, which contradicts the assumption $p > \sqrt[12]{2^{(|A|+|B|)-2}}$, as $p$ is the smallest prime divisor of $|G|$. This completes the proof of part (a).

(b) As $|H| \leq \sqrt[12]{2^{(|A|+|B|)-3}}$ and $p > \sqrt[12]{2^{(|A|+|B|)-2}}$ 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 $N \geq 2$.

It follows that $A_1, A_K$ are disjoint subsets of $A$ and $B_1, B_N$ are disjoint subsets of $B$. In particular, $|A_1| + |B_1| \leq (|A| + |B|)/2$ 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 $|H| > \sqrt[12]{2^{(|A_1|+|B_1|)-2}}$. Then applying Theorem 15 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

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

But this is impossible, as $p > \sqrt[12]{2^{(|A|+|B|)-2}}$ 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).

Q.E.D.

**Proof of Theorem 4** Suppose that $A$ does not have a unique difference. We apply Theorem 19 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 19 then. Thus we may assume $\langle A \rangle = G$. 

24
(a) Theorem 19 shows that there is a subgroup $H$ of $G$ with $|H| \leq 2^{|A|-2}$ and disjoint nonempty subsets $A_1, \ldots, A_K$ of $G$, $K \geq 2$, such that conditions (i)-(iv) in Theorem 19 hold. In particular, $A_K - A_1$ contains no unique difference. As $|H| \leq 2^{|A|-2}$ and $|G|$ has no prime divisor $\leq 2^{|A|-2}$, we have $|H| = 1$. Hence $|A_1| = |A_K| = 1$ by condition (iv) of Theorem 19. But this contradicts the fact that $A_K - A_1$ contains no unique difference. This proves part (a).

(b) Since, by assumption, $|G|$ is not a prime and $p > (\sqrt[4]{12})^{|A|}$ is the smallest prime divisor of $|G|$, we conclude $|G| \geq p^2 > (\sqrt[4]{12})^{|A|} > 2^{|A|-1}$. Hence we can apply Theorem 19 again and we get a subgroup $H$ of $G$ with $|H| \leq 2^{|A|-2}$ and disjoint nonempty subsets $A_1, \ldots, A_K$ of $G$, $K \geq 2$, such that conditions (i)-(iv) in Theorem 19 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 19. Moreover, by condition (iv) of Theorem 19, 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 15 to the subsets $X$ and $-Y$ of $H$. This yields disjoint sets $X_1, \ldots, X_S$ and $Y_1, \ldots, Y_T$ with $X = \bigcup X_i$ and $-Y = \bigcup Y_j$ such that $X_i + Y_j$ does not contain a unique sum. Note that $|X_i| = |Y_j| = 1$, 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 $X_i + Y_j$ contains a unique sum. Part (b) is proved.

Q.E.D.

5 Group Invariant Weighing Matrices

Theorem 19 is surprisingly well suited to determine the structure of group invariant weighing matrices with small weights. It not only shows that, for fixed weight $n$, all weighing matrices $W(v, n)$ invariant under an abelian group can be generated from a finite set of finite subsets of group rings. It also implies that the relevant group ring elements satisfy a strong orthogonality relation. In this way, we obtain a generalization and substantial improvement of the main result of [8].
We begin with a general result concerning the decomposition of group ring elements satisfying equations of the form $XX^{(-1)} = n$ where $n$ is an integer. We will write groups multiplicatively in this section, since we are working with group rings. The identity element of a group will be denoted by $1$.

**Theorem 22** Let $G$ be a finite abelian group and let $n$ be a positive integer. Suppose $X \in \mathbb{Z}[G]$ satisfies $XX^{(-1)} = n$. Write $A = \text{supp}(X)$. Suppose that $1 \in A$ and $|\langle A \rangle| > 2^{n-1}$. Then there exist a subgroup $H$ with $|H| \leq 2^{n-2}$, nonzero elements $X_1, \ldots, X_K$ of $\mathbb{Z}[H]$, $g_1, \ldots, g_K \in G$, $K \geq 2$, such that

(i) $X = \sum_{i=1}^{K} X_i g_i$;

(ii) $\text{supp}(X_i g_i) \cap \text{supp}(X_j g_j) = \emptyset$ whenever $i \neq j$;

(iii) $X_i X_j = 0$ whenever $i \neq j$.

**Proof** Write $X = \sum_{g \in G} a_g g$ with $a_g \in \mathbb{Z}$. Recall that $A = \text{supp}(X) = \{g \in G : a_g \neq 0\}$. As $XX^{(-1)} = n$ by assumption, $A$ does not have a unique difference by Lemma 6. Furthermore, $XX^{(-1)} = n$ implies $\sum a_g^2 = n$ and thus $|A| \leq n$.

As $|\langle A \rangle| > 2^{n-1}$ by assumption, Theorem 19 shows that there is a subgroup $H$ of $G$ with $|H| \leq 2^{n-2}$, integers $\alpha_1 < \cdots < \alpha_K$, $K \geq 2$, and nonempty disjoint subsets $A_1, \ldots, A_K$ of $G$ such that conditions (i)-(iv) in Theorem 19 hold. By condition (iv) of Theorem 19, there are $g_1, \ldots, g_k \in G$ such that $A_i g_i^{-1} \in H$ for all $i$.

Define $X_i = g_i^{-1} \sum_{g \in A_i} a_g g$ for $i = 1, \ldots, K$. Note that $X_i \in \mathbb{Z}[H]$ and $X_i \neq 0$ for all $i$, as the $A_i$'s are nonempty. Note that $a_g \neq 0$ for all $g \in A_i$, as $A_i \subseteq \text{supp}(X)$. We have $\sum_{i=1}^{K} X_i g_i = \sum_{i=1}^{K} \sum_{g \in A_i} a_g g = \sum_{g \in \text{supp}(X)} a_g g = X$. Thus condition (i) of Theorem 22 holds. Note that $\text{supp}(X_i g_i) = \text{supp}(\sum_{g \in A_i} a_g g) = A_i$. As the $A_i$'s are disjoint, condition (ii) of Theorem 22 holds.

It remains to prove (iii). Let $\alpha$ be any real number. We define

$$Y_{\alpha} = \sum_{i,j=1 \atop \alpha_i - \alpha_j \leq \alpha}^{K} X_i X_j^{(-1)} g_i g_j^{-1} \text{ and } Z_{\alpha} = \sum_{i,j=1 \atop \alpha_i - \alpha_j > \alpha}^{K} X_i X_j^{(-1)} g_i g_j^{-1}.$$
Note that, by condition (ii) of Theorem 19, for any \(i, j, i', j'\) with \(1 \leq i, j, i', j' \leq K\), the intersection of \(\text{supp}(A_i A_j^{-1})\) and \(\text{supp}(A_{i'} A_{j'}^{-1})\) can only be nonempty if \(\alpha_i - \alpha_j = \alpha_{i'} - \alpha_{j'}\).

Recall that \(a_g \neq 0\) for all \(g \in A_i\) and all \(i\). Thus

\[
\text{supp} \left( X_i X_j^{(-1)} g_i g_j^{-1} \right) = \text{supp} \left( (X_i g_i)(X_j g_j)^{(-1)} \right)
\]

\[
= \text{supp} \left( \left( \sum_{g \in A_i} a_g g \right) \left( \sum_{h \in A_j} a_h h^{-1} \right) \right)
\]

\[
= \text{supp} \left( \sum_{g \in A_i} \sum_{h \in A_j} g h^{-1} \right)
\]

\[
= \text{supp} \left( A_i A_j^{(-1)} \right). \quad (14)
\]

This implies that

\[
\text{supp} \left( X_i X_j^{(-1)} g_i g_j^{-1} \right) \cap \text{supp} \left( X_{i'} X_{j'}^{(-1)} g_{i'} g_{j'}^{-1} \right) \neq \emptyset \text{ only if } \alpha_i - \alpha_j = \alpha_{i'} - \alpha_{j'}. \quad (15)
\]

Thus

\[
\text{supp}(Y_\alpha) \cap \text{supp}(Z_\alpha) = \emptyset \quad (16)
\]

for all \(\alpha \in \mathbb{R}\).

Note that

\[
n = XX^{(-1)} = \sum_{i,j=1}^{K} X_i X_j^{(-1)} g_i g_j^{-1} = Y_\alpha + Z_\alpha. \quad (17)
\]

In view of (16), this implies \(Y_\alpha = 0\) or \(Y_\alpha = n\). Note that, if \(\alpha_i - \alpha_j < 0\), then \(\alpha_i - \alpha_j \neq \alpha_i - \alpha_i\) and thus \(1 \not\in \text{supp}(A_i A_j^{(-1)})\) by (15), since \(1 \in \text{supp}(A_i A_i^{(-1)})\). Note that

\[
\text{supp}(Y_\alpha) = \bigcup_{i,j=1}^{K} \text{supp}(A_i A_j^{(-1)})
\]

by (14). Suppose \(\alpha < 0\). Then \(1 \not\in \text{supp}(Y_\alpha)\), since \(1 \not\in \text{supp}(A_i A_j^{(-1)})\) if \(\alpha_i - \alpha_j < 0\). As \(Y_\alpha \in \{0, n\}\), we conclude

\[
\sum_{i,j=1}^{K} X_i X_j^{(-1)} g_i g_j^{-1} = Y_\alpha = 0 \text{ if } \alpha < 0. \quad (18)
\]
We are going to use (18) to show that \( X_i X_j = 0 \) for all \( i \neq j \). First of all, setting \( \alpha = \alpha_1 - \alpha_K \) in (18), we get \( X_K^{(-1)} = 0 \), as \( \alpha_i - \alpha_j > \alpha_1 - \alpha_K \) for all pairs \((i, j) \neq (1, K)\). Now we prove by induction that

\[
X_1 X_K^{(-1)} = X_1 X_{K-1}^{(-1)} = \cdots = X_1 X_2^{(-1)} = 0. \tag{19}
\]

Suppose we have

\[
X_1 X_K^{(-1)} = X_1 X_{K-1}^{(-1)} = \cdots = X_1 X_\ell^{(-1)} = 0 \tag{20}
\]

with \( \ell \geq 3 \). To prove (19) by induction, it suffices to show

\[
X_1 X_\ell^{(-1)} = 0 \tag{22}
\]

Recall that \( \alpha_1 < \cdots < \alpha_K \). Suppose a pair \((i, j)\) satisfies \( \alpha_i - \alpha_j \leq \alpha' = \alpha_1 - \alpha_{\ell-1} \). Then \( \alpha_j \geq (\alpha_i - \alpha_1) + \alpha_{\ell-1} \). As \( \alpha_i - \alpha_1 \geq 0 \), this implies \( j \geq \ell - 1 \). Furthermore, if \( j = \ell - 1 \), then \( \alpha_i - \alpha_1 = 0 \) and thus \( i = 1 \). Hence all pairs \((i, j)\) with \( \alpha_i - \alpha_j \leq \alpha' \) satisfy \((i, j) = (1, \ell - 1)\) or \( j \geq \ell \). Thus (21) is equivalent to

\[
X_1 X_\ell^{(-1)} + \sum_{\substack{i, j = 1 \\
\alpha_i - \alpha_j \leq \alpha'}} \sum_{j \geq \ell} X_i X_j^{(-1)} g_i g_j^{-1} = 0. \tag{22}
\]

Recall that \( X_1 X_j^{(-1)} = 0 \) for \( j = \ell, \ldots, K \) by the inductive assumption (20). Thus, multiplying (21) by \( X_1 \), we get

\[
(X_1)^2 X_{\ell-1}^{(-1)} = 0. \tag{23}
\]

Let \( \chi \) be any complex character of \( G \). Note that (23) implies \( \chi(X_1)^2 \chi(X_{\ell-1}^{(-1)}) = 0 \) and thus \( \chi(X_1 X_{\ell-1}^{(-1)}) = \chi(X_1) \chi(X_{\ell-1}^{(-1)}) = 0 \). Therefore, \( X_1 X_{\ell-1}^{(-1)} = 0 \) by Result 13. This completes the proof of (19).

Note that the term \( X_1 X_1^{(-1)} \) does not occur in (18), as \( 1 \not\in \text{supp}(Y_\alpha) \). Hence (18) and (19) imply

\[
\sum_{\substack{i, j = 2 \\
\alpha_i - \alpha_j \leq \alpha}} X_i X_j^{(-1)} g_i g_j^{-1} = 0 \quad \text{if } \alpha < 0.
\]
Now a similar argument as above with \( X_1 \) replaced by \( X_2 \) shows that \( X_2X_j^{(-1)} = 0 \) for \( j = 3, \ldots, K \). Continuing in this way, we see that \( X_iX_j^{(-1)} = 0 \) for all \( i \neq j \). Hence \( \chi(X_i)\chi(X_j) = 0 \) for all complex characters \( \chi \) of \( G \) and all \( i \neq j \). This implies \( \chi(X_i)\chi(X_j) = 0 \) for all complex characters \( \chi \) of \( G \) and thus \( X_iX_j = 0 \) for all \( i \neq j \) by Result 13. This completes the proof of part (iii) of Theorem 22. Q.E.D.

We now show how Theorem 22 can be applied in the study of weighing matrices. We first use Theorem 22 to prove Theorem 9 and then prove Corollary 10.

**Proof of Theorem 9** Let \( n \) be a positive integer and let \( X \) be a weighing matrix \( W(v, n) \) invariant under an abelian group \( G \). By Lemma 5, we can view \( X \) as an element of \( \mathbb{Z}[G] \) satisfying \( XX^{(-1)} = n \). We need to show that \( X \) is decomposable over a subgroup \( H \) of \( G \) with \( |H| \leq 2^{n-1} \).

Write \( A = \text{supp}(X) \). Replacing \( X \) by \( Xg \) for some \( g \in G \), if necessary, we can assume \( 1 \in A \). If \( |\langle A \rangle| \leq 2^{n-1} \), then there is nothing to show since \( X \) trivially is decomposable over \( \langle A \rangle \) (in this case \( K = 1 \) and \( X_1 = X \) gives the required decomposition). Thus we may assume \( |\langle A \rangle| > 2^{n-1} \). But then \( X \) is decomposable over a subgroup \( H \) of \( G \) with \( |H| \leq 2^{n-1} \) by Theorem 22. Q.E.D.

**Remark 23** Theorem 9 implies that, for fixed \( n \), up to group isomorphisms, all weighing matrices of weight \( n \) invariant under an abelian group can be generated from a finite set of finite subsets of group rings:

Let \( \mathcal{G}(n) \) be a set whose elements are abelian groups of order at most \( 2^{n-1} \) such that each isomorphism type of abelian groups of order at most \( 2^{n-1} \) is represented exactly once. For instance,

\[
\mathcal{G}(4) = \{ C_1, C_2, C_3, C_4, C_2 \times C_2, C_5, C_6, C_7, C_8, C_4 \times C_2, C_2 \times C_2 \times C_2 \times C_2 \}.
\]

It is straightforward to show, that, for each \( H \in \mathcal{G}(n) \), there are only finitely many subsets \( \{X_1, \ldots, X_K\} \) of \( \mathbb{Z}[H] \) satisfying the conditions of Theorem 22 (the necessary arguments
are contained in the proof of Theorem 2.4 of [8]; note that $K$ may vary from subset to subset). Let $\mathcal{X}(n)$ be the set of all these sets $\{X_1, \ldots, X_K\} \subset \mathbb{Z}[H]$ where $H$ ranges over all groups in $\mathcal{G}(n)$. Note that $\mathcal{X}(n)$ is finite.

Now let $X$ be a weighing matrix of weight $n$ invariant under an abelian group $G$. We may assume $1 \in \text{supp}(X)$. By Theorem 9, there is a subgroup $H$ of $G$ with $|H| \leq 2^{n-1}$ such that $X$ is decomposable over $H$. Note $H \in \mathcal{G}(n)$ (up to isomorphism). Hence there is a set $\{X_1, \ldots, X_K\} \in \mathcal{X}(n)$ such that

$$X = \sum_{i=1}^{K} X_i g_i$$

with $g_1, \ldots, g_K \in G$. This shows that, up to group isomorphisms, all weighing matrices of weight $n$ invariant under an abelian group can be generated from $\mathcal{X}(n)$ by formula (24).

**Proof of Corollary 10** Suppose there exists a proper circulant weighing matrix $X \in \mathbb{Z}[C_v]$ of weight $n$ where $n$ is an odd prime power. We need to show $v \leq 2^{n-1}$.

Suppose $v > 2^{n-1}$. We may assume $1 \in \text{supp}(X)$. Since $X$ is proper by assumption, we have $\langle \text{supp}(X) \rangle = C_v$ and thus $|\langle \text{supp}(X) \rangle| > 2^{n-1}$. By Theorem 22, there is a proper subgroup $H$ of $C_v$ such that $X$ is decomposable over $H$. Hence $X = \sum_{i=1}^{K} X_i g_i$, $X_i \in \mathbb{Z}[H], g_i \in C_v, \ K \geq 2$, such that the conditions (i)-(iii) of Theorem 22 are satisfied. But this is impossible by [8, Thm. 2.6]. Thus $v \leq 2^{n-1}$. Q.E.D.

6  Weil Numbers

Our aim for this section is to demonstrate how Theorem 22 can be used to improve and generalize Loxton’s Result 11 mentioned in the introduction. We also show how our new result can be used to obtain information on class groups of cyclotomic fields.

**Theorem 24** Let $p$ be a prime and let $n, r$ be positive integers. Suppose that $YY = n$ for some $Y \in \mathbb{Z}[\zeta_p^r]$ and that $p > 4n^2 - 2n + 2$. Then $n$ is a square. Moreover, there exists $j \in \mathbb{Z}$ such that $Y \zeta_p^j \in \mathbb{Z}[\zeta_p^r]$ with $p^s \leq 2^{n-1}$. 30
Proof Write \( Y = \sum_{i=0}^{p^r - 1} a_i \zeta_{p^r}^i \) with \( a_0, \ldots, a_{p^r - 1} \in \mathbb{Z} \). By a result of Loxton [10, Lemma 9], we may assume \( |\{i : a_i \neq 0\}| \leq 2n \). Furthermore, we may assume that for any \( \mathcal{I} \subset \{0, \ldots, p^r - 1\} \), if there exists \( j \in \mathcal{I} \) with \( a_j \neq 0 \), then

\[
\sum_{i \in \mathcal{I}} a_i \zeta_{p^r}^i \neq 0
\]  

(25)

(if \( \sum_{i \in \mathcal{I}} a_i \zeta_{p^r}^i = 0 \), then we just remove this term from \( Y \)).

Let \( g \) be a generator of \( C_{p^r} \) and set \( X = \sum_{i=0}^{p^r - 1} a_i g^i \). Let \( K \) be the kernel of the ring homomorphism \( \phi : \mathbb{Z}[C_{p^r}] \to \mathbb{Z}[\zeta_{p^r}] \) determined by \( g \mapsto \zeta_{p^r} \). It is known [7, Thm. 2.2] that

\[
K = \{ PZ : Z \in \mathbb{Z}[C_{p^r}] \}
\]

where \( P \) is the subgroup of order \( p \) of \( C_{p^r} \). Since \( \phi(X) = Y \) and \( Y = n \), we have

\[
XX^{-1} = n + PZ
\]  

(26)

for some \( Z \in \mathbb{Z}[C_{p^r}] \). Suppose \( PZ \neq 0 \). Then \( |\text{supp}(PZ)| \geq p \), as the coefficients of \( PZ \) are constant an each coset of \( P \). Recall that \( |\text{supp}(X)| \leq 2n \). Write \( X = \sum_{j=1}^{s} b_j g^{a_j} \) with \( s \leq 2n \) and \( a_j, b_j \in \mathbb{Z} \). Then

\[
XX^{-1} = \sum_{j,k=1}^{s} b_j b_k g^{a_j-a_k} = \left( \sum_{j=1}^{s} b_j^2 \right) + \left( \sum_{j,k=1}^{s} b_j b_k g^{a_j-a_k} \right).
\]

Hence \( |\text{supp}(XX^{-1})| \leq 1 + s(s - 1) \leq 1 + 2n(2n - 1) = 4n^2 - 2n + 1 \). This contradicts (26), as \( |\text{supp}(n + PZ)| \geq p - 1 > 4n^2 - 2n + 1 \) (recall that \( p > 4n^2 - 2n + 2 \) by assumption).

We conclude that \( PZ = 0 \) and

\[
XX^{-1} = n
\]  

(27)

In particular, \( |X|^2 = n \) and thus \( n \) is a square.

Replacing \( X \) by \( Xg \) for some \( g \in G \), if necessary, we may assume \( 1 \in \text{supp}(X) \). Note that \( |\text{supp}(X)| = p^s \) for some nonnegative integer \( s \), as \( G \) is a \( p \)-group. In other words, \( X \in \mathbb{Z}[C_{p^r}] \) where \( C_{p^r} \) is the subgroup of \( C_{p^r} \) of order \( p^s \). If \( p^s \leq 2^{n-1} \), we are done, as \( Y = \phi(X) \in \mathbb{Z}[\zeta_{p^r}] \) in this case.
Now suppose $p^s > 2^{n-1}$. By Theorem 22 there are a subgroup $H$ of $C_{pr}$ with $|H| \leq 2^{n-2}$ and nonzero elements $X_1, \ldots, X_K$ of $\mathbb{Z}[H]$, $K \geq 2$, such that $X = \sum_{i=1}^{K} X_i g_i$, $g_i \in C_{pr}$, and the conditions (ii) and (iii) of Theorem 22 are satisfied.

By condition (iii) of Theorem 22, we have $X_1 X_2 = 0$. Thus $\phi(X_1) = 0$ or $\phi(X_2) = 0$. Without loss of generality, we may assume $\phi(X_1) = 0$. Note that $\text{supp}(X_1 g_1) \cap \text{supp}(X_2 g_2) = \emptyset$ by condition (ii) of Theorem 22. Note that $\phi(X_1 g_1) = \phi(X_1)(g_1) = 0$. Let $I = \{ j : g^j \in \text{supp}(X_1 g_1) \}$. Then $I \neq \emptyset$, as $X_1 \neq 0$. Furthermore,

$$0 = \phi(X_1 g_1) = \sum_{j \in I} a_j \zeta_{p^r}^j.$$

Note that $a_j \neq 0$ for all $j \in I$ by the definition of $I$. This contradicts (25). Therefore, $p^s \leq 2^{n-1}$. \[ \text{Q.E.D.} \]

Now we are ready to prove Theorem 12 stated in the introduction.

**Proof of Theorem 12** Suppose that $p > \max(4n^2 - 2n + 2, 2^{n-1})$ and that $|Y|^2 = n$ for some $Y \in \mathbb{Z}[\zeta_{pr}]$. Then $n$ is a square by Theorem 24 and there exists $j \in \mathbb{Z}$ such that $Y \zeta_{pr}^j \in \mathbb{Z}[\zeta_{pr}]$ with $p^s \leq 2^{n-1}$. As $p > 2^{n-1}$ by assumption, this implies $s = 0$. Hence $Y \zeta_{pr}^j \in \mathbb{Z}$. Together with $|Y|^2 = n$, this implies $Y \zeta_{pr}^j = \pm \sqrt{n}$. This shows that $Y$ is trivial. \[ \text{Q.E.D.} \]

Similar to [16, Thm. 3.7, Cor. 3.8], Theorem 15 can be used to derive lower bounds on sizes of subgroups of ideal class groups of cyclotomic fields generated by certain explicitly given prime ideals. We just give one example of such a bound to keep the technicalities at minimum.

**Example 25** For this example, we assume basic algebraic number theory as treated in [2, 6], for instance. Let $p = 3511$. Note that $\text{ord}_{p^2}(2) = (p - 1)/2$ and thus the ideal $(2)$ factors in $\mathbb{Z}[\zeta_{p^2}]$ as $(2) = \prod_{i=1}^{p} \pi_i \bar{\pi}_i$ where the $\pi_i$'s are distinct prime ideals. Let

$$T = \{ \prod_{i=1}^{p} \pi_i^{a_i} : 0 \leq a_i \leq 1 \}.$$
Suppose that two distinct ideals $\prod \pi_i^{a_i}$ and $\prod \pi_i^{b_i}$ in $T$ represent the same ideal class in the ideal class group of $\mathbb{Q}(\zeta_{p^2})$. Then there is $Y \in \mathbb{Q}(\zeta_{p^2})$ with

$$\prod_{i=1}^{p} \pi_i^{a_i-b_i} = (Y).$$

Write $c_i = a_i - b_i$, $-1 \leq c_i \leq 1$, $i = 1, \ldots, p$. Note that $-1 \leq c_i \leq 1$ for all $i$, as $0 \leq a_i, b_i \leq 1$. Furthermore, since $\prod \pi_i^{a_i} \neq \prod \pi_i^{b_i}$, there is $j \in \{1, \ldots, p\}$ with $c_j \neq 0$. Set $Y_1 = 2Y/Y$. Note that $Y_1 \in \mathbb{Z}[\zeta_{p^2}]$, since $c_i \geq -1$ for all $i$. Furthermore,

$$(Y_1) = \prod_{i=1}^{p} \pi_i^{1+a_i-b_i} \pi_i^{1-a_i+b_i} = \prod_{i=1}^{p} \pi_i^{1+c_i} \pi_i^{1-c_i}.$$  \hfill (28)

As $c_j \neq 0$, one of the prime ideals $\pi_j$, $\pi_j$ occurs in (28) with exponent 0. Thus $X \not\equiv 0 \pmod{2}$. Moreover, $XX = 4$. Note that $X \not\equiv 0 \pmod{2}$ implies that $X$ is nontrivial. But by Theorem 12, there is no nontrivial $X \in \mathbb{Z}[\zeta_{p^2}]$ with $XX = 4$, a contradiction.

Hence the ideals in $T$ represent pairwise distinct ideal classes. Thus the order of the subgroup of the ideal class group of $\mathbb{Q}(\zeta_{p^2})$ generated by the classes of the prime ideals above 2 is at least $|T| = 2^p = 2^{3511}$.

References


