Structure of Group Invariant Weighing Matrices of Small Weight

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

October 10, 2016

Abstract

We show that every weighing matrix of weight n invariant under a finite abelian group G can be generated from a subgroup H of G with $|H| \leq 2^{n-1}$. Furthermore, if n is an odd prime power and a proper circulant weighing matrix of weight n and order v exists, then $v \leq 2^{n-1}$. We also obtain a lower bound on the weight of group invariant matrices depending on the invariant factors of the underlying

group. These results are obtained by investigating the structure of subsets of finite abelian groups that do not have unique differences. Finally, our method can be used to improve multiplier theorems for difference sets.

1 Introduction

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 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 $\mathrm{supp}(X) = \{g \in G : a_g \neq 0\}$ is called the **support** of X.

A **weighing matrix** is a square matrix M with entries $0, \pm 1$ only such that $MM^T = nI$ where n is a positive integer and I is an identity matrix. The integer n is the **weight** of the matrix. Let G be a finite group and let $H = (h_{f,g})_{f,g \in G}$ be a $|G| \times |G|$ matrix, indexed with the elements of G. We say that H is ***G*-invariant** if $h_{fk,gk} = h_{f,g}$ for all $f, g, k \in G$. Weighing matrices invariant under cyclic groups are called **circulant weighing matrices**.

The existence of group invariant weighing matrices has been studied quite intensively, see [1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 19, 20], for instance. Interest in methods for the study of group invariant weighing matrices also stems from the multiplier conjecture for difference sets: The most powerful known approach to this conjecture due to McFarland [15] depends on nonexistence results for group ring elements which satisfy the same equation $XX^{(-1)} = n$ as group invariant weighing matrices. In fact, we will describe an application of our results to multipliers of difference sets in Section 6.

The following is well known, see [18, Lem. 1.3.9].

Lemma 1. *Let G be a finite group of order v. The existence of G-invariant weighing matrix of weight 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 1, we will always view G-invariant weighing matrices as elements of $\mathbb{Z}[G]$. The key to our results is the investigation of the support of group invariant weiging matrices in Section 3. As the support of such matrices does not contain a unique difference, we can use the Smith Normal Form of the matrix of the corresponding linear system to gain insights into the structure of the support.

Many group invariant weighing matrices can be constructed as follows. Let H be a subgroup of a finite abelian group G and let $g_1, \ldots, g_K \in G$ be representatives of distinct cosets of H in G. Suppose that $X_1, \ldots, X_K \in \mathbb{Z}[H]$ have coefficients $0, \pm 1$ only and that $\sum_{i=1}^{K} X_i X_i^{(-1)} = n$ and $X_i X_j = 0$ whenever $i \neq j$. It follows by straightforward computation ([2, Thm. 2.4]) that

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

is a G-invariant weighing matrix of weight n. If (1) holds, we say that X is **generated from H**.

Note that, indeed, the main conditions that make (1) a weighing matrix only involve equations over the group ring of H. These conditions are $\sum_{i=1}^{K} X_i X_i^{(-1)} = n$ and $X_i X_j = 0$ for $i \neq j$. The choice of the g_i's only makes sure that the coefficients of X are $0, \pm 1$. In fact, such g_i's exist in *any* abelian group which contains H as a subgroup of index at least K.

The following [1, Construction 3.10] provides examples of group invariant weighing matrices obtained via (1).

Result 2. Let $q = p^a$ where p is a prime and a is a positive integer. Let $d \geq 2$ be an integer and assume that d is even if p is odd. Set $r = q^d + q^{d-1} + \cdots + 1$. Let V be a $(d+1)$-dimensional vector space over $\mathbb{F}_q$ and let $U_1, \ldots, U_r$ be the d-dimensional subspaces of V. Let G be any abelian group containing V as a subgroup such that the index of V in G is at least $(r+1)/2$. Finally, let $g_1, \ldots, g_{(r-1)/2} \in G \setminus H$ be representatives of distinct cosets of H in G. Then

$$X = U_1 + \sum_{i=1}^{(r-1)/2} (U_{2i} - U_{2i+1}) g_i \tag{2}$$

is a G-invariant weighing matrix of weight q^{2d}.

The main aim of our work is to show that group invariant weighing matrices *necessarily* have the form (1) if their weight is small compared to order of the underlying group. Moreover, we show that the order of the group H which contains the "building blocks" X_i is bounded by a constant only depending on n. Some results in this direction concerning circulant weighing matrices previously were obtained in [12]. The main result of [12] is the following.

Result 3. For every positive integer n, there is a positive integer $F(n)$, only depending on n, such that every circulant weighing matrix of weight n is generated from a cyclic group of order $F(n)$.

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 substantially generalizes and improves Result 3.

Theorem 4. Let n be a positive integer. Every weighing matrix of weight n invariant under an abelian group G is generated from a subgroup H of G with $|H| \leq 2^{n-1}$.

A G-invariant weighing matrix $X \in \mathbb{Z}[G]$ is called **proper** if $\langle \mathrm{supp}(Xg) \rangle = G$ for all $g \in G$. Note that X is proper if and only if $Xg \notin \mathbb{Z}[U]$ for all proper subgroups U of G all $g \in G$.

Example 5. Let $q = 2^a$ where a is a positive integer. There exists a proper weighing matrix Y of weight q^2 invariant under a cyclic group, say U, of order q^2+q+1 (see [19]). Let $G = U \times \langle g \rangle \times \langle h \rangle$ where g is an element of order 2 and the order of h is coprime to $2(q^2 + q + 1)$. Note that G is a cyclic group of order $2(q^2 + q + 1)k$ where k is the order of h. Set

$$X = (1 + g)Y + (1 - g)hY.$$

Using $YY^{(-1)} = q^2$, $(1 + g)(1 - g) = 0$, and $(1 + g)^2 + (1 - g)^2 = 4$, it is straightforward to verify that X is a G-invariant weighing matrix of weight $4q^2 = 2^{2a+2}$. Furthermore, the fact that Y is proper implies that X is proper, too.

Note that the order of h in Example 5 can be arbitrarily large. Hence Example 5 shows that, for any fixed a, there exist proper circulant weighing matrices of weight 2^{2a+2} invariant under groups of arbitrarily large order. We will show that this cannot happen if the weight is an *odd* prime power. In fact, Theorem 4, together with results from [12], yields the following result.

Corollary 6. *Let n be an odd prime power. If there exists a proper circulant weighing matrix of weight n and order v, then $v \leq 2^{n-1}$.*

Example 7. We show that the statement of Corollary 6 does not hold any more if "circulant" is replaced by "group invariant". Let p be an odd prime and

$$G = (\mathbb{Z}/p\mathbb{Z})^3 \times \langle g_1 \rangle \times \cdots \times \langle g_{(r-1)/2} \rangle,$$

where $r = p^2+p+1$ and the g_i's are elements of order at least 2. Then (2) defines a proper G-invariant weighing matrix of weight p^4. As the order of the g_i's can be arbitrarily large, this shows that, for fixed p, there exist proper weighing matrices of weight p^4 invariant under arbitrarily large groups. Hence the conclusion of Corollary 6 does not hold for weighing matrices invariant under arbitrary abelian groups.

We will also obtain a lower bound on the weight of a G-invariant matrix depending on the invariant factors of G. We first give the necessary definitions. Let G be finite abelian group with $|G| \geq 2$. Then there are unique integers $k \geq 1$, $v_1, \ldots, v_k \geq 2$ with $v_1|v_2|\cdots|v_k$ such that G is isomorphic to $(\mathbb{Z}/v_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/v_k\mathbb{Z})$. The numbers $v_1, \ldots, v_k$ are called the **invariant factors** of G. The positive integer k is equal to the minimum number of generators of G and is denoted by $d(G)$.

Theorem 8. Let n be a positive integer. Let G be a finite abelian group with invariant factors v_i, $i = 1, \ldots, d(G)$, and suppose that $\prod_{i=1}^{m} v_i > 2^{n-1}$ for some $m \leq d(G)$. If a proper G-invariant weighing matrix of weight n exists, then

$$n \geq (d(G) - m + 2)^2 .$$

We will prove Theorem 8 in Section 5. The following example shows that the bound in Theorem 8 can be attained. For an element g of a group G, denote the order of g in G by $\mathrm{ord}(g)$.

Example 9. Let V be an elementary abelian group of order 2^{2a} and let

$$G = V \times \langle g_1 \rangle \times \cdots \times \langle g_{2^{a-1}} \rangle$$

be an abelian group such that $\mathrm{ord}(g_i)$ is even and larger than $2^{2^{2a}}$ for all i. Then (2) defines a G-invariant weighing matrix X of weight $n = 2^{2a}$ by Result 2. It is straightforward to check that X is proper.

Write $k = d(G)$ and note that $k = 2a + 2^{a-1}$. Let $v_1, v_2, \ldots, v_k$ be the invariant factors of G. By the assumptions above, we have $v_i = 2$ for $i = 1, \ldots, 2a$ and $v_{2a+1} > 2^{2^{2a}}$. Thus $\prod_{i=1}^{2a+1} v_i > v_{2a+1} > 2^{2^{2a}} > 2^{n-1}$. Applying Theorem 8 to this example, we get

$$n \geq \left(2a + 2^{a-1} - (2a+1) + 2\right)^2 = 2^{2a-2} + 2^a + 1.$$

In particular, the bound provided by Theorem 8 is best possible for $a = 1$.

2 Preliminaries

For the convenience of reader, we recall some known results which will be used later. Let G be a finite multiplicatively written abelian group. We denote the group of complex characters of G by $\hat{G}$. For $A = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$ and $\chi \in \hat{G}$, we set $\chi(A) = \sum_{g \in G} a_g \chi(g)$. A proof of the following result can be found in [8, Section VI.3], for instance.

Result 10 (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 $X = 0$.

The following determinant bound is due to Schinzel [17].

Result 11. *Let $A = (A_{ij})$ be a real $n \times n$ matrix. For $i = 1, \ldots, n$, write $R_i^+(A) = \sum_{j=1}^n \max(0, A_{ij})$ and $R_i^-(A) = \sum_{j=1}^n \max(0, -A_{ij})$. We have*

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

We will use the Smith Normal Form of integer matrices M to analyse the connection between the solution sets of $Mx = 0$ where, on the one hand, x is considered as an integer vector and, on the other hand, as a vector with entries from a finite abelian group. Lemma 12 below supplies some tools supporting these arguments.

At this point, a remark on notation is appropriate. When we are using group rings, we write groups multiplicatively to distinguish between the addition in the group ring and the group operation. When we consider linear systems of equations over ablian groups, however, we write groups additively, so that we can easily use matrix-vector notation.

Lemma 12. *Let G be an additive finite abelian group and let M be an $m \times n$ matrix with integer entries where $m \geq n$. Write $s = \operatorname{rank}_{\mathbb{Q}}(M)$. Let S and $T = (X|Y)$ be unimodular matrices such that $D = SMT$ is a Smith Normal Form of M. Note that X is an $n \times (n-s)$ matrix and Y is $n \times s$; and that D is a rectangular diagonal $m \times n$ matrix with diagonal entries $d_1, \ldots, d_n$ where $d_{s+1}, \ldots, d_n = 0$. Denote the rows of Y by $Y_1, \ldots, Y_n$. Then we have the following.*

(a) If $y \in G^n$ satisfies $My = 0$, then there is a subgroup H of G with $|H| \leq \prod_{j=1}^{s} d_j$ such that

$$y = Xe + Yf \text{ with } e \in H^s \text{ and } f \in G^{n-s}. \tag{3}$$

(b) Let $\mathbf{1}_n$ denote the vector with all entries 1 in $\mathbb{Z}^n$. If $M\mathbf{1}_n = 0$, then we can assume that Y contains $\mathbf{1}_n$ as a column.

(c) There is $\gamma \in \mathbb{Z}^{n-s}$ such that $Y_i\gamma \neq Y_j\gamma$ whenever $Y_i \neq Y_j$.

Proof. Since T is invertible, there is $w \in G^n$ such that $y = Tw$. We have $Dw = DT^{-1}y = 0$, since $S^{-1}(DT^{-1}y) = My = 0$. Write $w = \binom{e}{f}$ with $e = (e_1, \ldots, e_s)^T \in G^s$ and $f \in G^{n-s}$. We have $Dw = (e_1d_1, \ldots, e_sd_s, 0, \ldots, 0)^T = 0$. This implies that, for each i, the order of e_i in G divides d_i. Hence the subgroup H of G generated by $e_1, \ldots, e_s$ has order at most $\prod_{j=1}^{s} d_j$. As $e \in H^s$ and $y = Tw = Xe + Yf$, this proves (3).

Now suppose $M\mathbf{1}_n = 0$. Set $r = T^{-1}\mathbf{1}_n$. Then $Dr = DT^{-1}\mathbf{1}_n = 0$, since $M\mathbf{1}_n = S^{-1}DT^{-1}\mathbf{1}_n = 0$. Write $r = \binom{u}{v}$ with $u \in \mathbb{Z}^s$, $v \in \mathbb{Z}^{n-s}$. Then $u = 0$, since $Dr = 0$. Hence $\mathbf{1}_n = Tr = (X|Y)r = Yv$. As all entries in $\mathbf{1}_n$ are 1, this implies that the greatest

common divisor of the entries of v is 1. By [21, p. 336], there is an $(n-s)\times(n-s)$ unimodular matrix V which has v as its first column. Set

$$T' = T\begin{pmatrix} I_s & 0 \\ 0 & V \end{pmatrix},$$

where I_s is the $s\times s$ identity matrix and the zeros are zero blockmatrices of appropriate sizes. Then T' is unimodular, since T and V are unimodular. Furthermore,

$$SMT' = D\begin{pmatrix} I_s & 0 \\ 0 & V \end{pmatrix} = D,$$

since the last $n-s$ columns of D are all zero. Note that column $s+1$ of T' is first column of YV which is equal to $Yv = \mathbf{1}_n$ by the choice of V. Hence, replacing T by T', if necessary, we can assume that Y contains $\mathbf{1}_n$ as a column. This proves part (b).

If $Y_i \neq Y_j$, then $\{\gamma \in \mathbb{Z}^{n-s} : Y_i\gamma = Y_j\gamma\}$ is contained in a hyperplane of $\mathbb{Q}^{n-s}$. Since any union of finitely many hyperplanes of $\mathbb{Q}^{n-s}$ does not cover $\mathbb{Z}^{n-s}$, there exists $\gamma \in \mathbb{Z}^{n-s}$ which does not satisfy any of the equations $Y_i\gamma = Y_j\gamma$ for $Y_i \neq Y_j$. This proves part (c). □

3 Structure of Sets with no Unique Difference

Throughout this section, we write groups additively. Let A be a subset of a finite abelian group G. If there is $g \in G$ such that there is exactly one pair (a,b), $a,b \in A$, with $g = a-b$, we say that A has a **unique difference**.

Suppose that $A \subset G$ has *no* unique difference. Write $|A| = n$ and $A = \{a_1,\ldots,a_n\}$. To each a_i we associate a variable x_i. Consider the linear system

$$\begin{aligned}\mathcal{E} = \{&x_i - x_j = x_{i'} - x_{j'} : 0 \le i,i',j,j' \le |A|-1, i\neq i', j\neq j',\\ &\text{and } a_i - a_j = a_{i'} - a_{j'}\}.\end{aligned} \tag{4}$$

Since A does not have a unique difference, for every pair (i,j) with $i \neq j$, there is at least one pair (i',j') such that the equation $x_i - x_j = x_{i'} - x_{j'}$ is contained in $\mathcal{E}$ (note that for given (i,j), there might well be more than one such pair (i',j')).

Note that $\mathcal{E}$ is a homogeneous linear system and can be written in the form $Mx = 0$ where M is a coefficient matrix of the system. Note that M has entries 0, ± 1, and ± 2 only. It is indeed possible that M contains entries ± 2. For instance, if $i = j' \neq 0$, then the row of M corresponding to the equation $x_i - x_j = x_{i'} - x_{j'}$ has an entry ± 2, as the equation is equivalent to $2x_i - x_j - x_{i'} = 0$. Furthermore, note that the sum of the positive entries of each row of M is at most 2, and the sum of the negative entries of each row is at least -2.

Theorem 13. *Let G be a finite abelian group and A be a subset of G which has no unique difference. Let M be a coefficient matrix of the linear system (4) determined by A.*

Then there exist an integer $K \geq |A| - \mathrm{rank}_{\mathbb{Q}}(M)$ and a subgroup H of G with $|H| \leq 2^{|A|-1}$ such that the following hold. There are integers $\alpha_1 < \cdots < \alpha_K$ and nonempty subsets $A_1, \ldots, A_K$ of G satisfying the following conditions.

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

Proof. Write $n = |A|$ and $s = \mathrm{rank}_{\mathbb{Q}}(M)$. Note that $s \leq n - 1$, since the sum of all columns of M is zero. Let S and T be unimodular matrices such that $D = SMT$ is a Smith Normal Form of M. As in Lemma 12, we write $T = (X|Y)$ and $\mathbf{1}_n \in \mathbb{Z}_n$ is a vector with all entries 1. Obviously, if we set all x_i's to be 1, it is a solution for the linear system $\mathcal{E}$. Therefore, as M is the coefficient matrix of $\mathcal{E}$, $M\mathbf{1}_n = 0$. By Lemma 12 (b), we can assume that $\mathbf{1}_n$ is the first column of Y. Recall that D is a rectangular diagonal $m \times n$ matrix with diagonal entries $d_1, \ldots, d_n$ where $d_{s+1}, \ldots, d_n = 0$. Hence the last $n - s$ columns of D and thus of $S^{-1}D = MT$ are all zero. This shows

$$MY = 0. \tag{5}$$

Let $Y_1, \ldots, Y_n$ be the rows of Y and write $\{Y_1, \ldots, Y_n\} = \{Z_1, \ldots, Z_K\}$ where the Z_i's are pairwise distinct. Since the columns of Y are linearly independent, we have

$\operatorname{rank}_{\mathbb{Q}}(Y) = n - s$. Hence $K \geq n - s = |A| - \operatorname{rank}_{\mathbb{Q}}(M)$. By Lemma 12 (c), there is $\gamma \in \mathbb{Z}^{n-s}$ such that the values $\alpha_i = Z_i\gamma$, $i = 1, \ldots, K$, are pairwise distinct. In other words, $Y_i\gamma = Y_j\gamma$ if and only if $Y_i = Y_j$. By renumbering the Z_i's, if necessary, we may assume $\alpha_1 < \cdots < \alpha_K$. Write $A = \{a_1, \ldots, a_n\}$ and set $A_i = \{a_j : Y_j\gamma = \alpha_i\}$, $i = 1, \ldots, K$. Note that the A_i's form a partition of A. This proves part (i).

For part (ii), suppose that $a_r - a_s = a_{r'} - a_{s'}$ for some $a_r \in A_i$, $a_s \in A_j$, $a_{r'} \in A_{i'}$, $a_{s'} \in A_{j'}$. Then the equation $x_r - x_s = x_{r'} - x_{s'}$ is contained in the system (4). By considering the row vector associated with the equation and (5), this implies $Y_r - Y_s = Y_{r'} - Y_{s'}$. Note that $Y_r\gamma = \alpha_i$ by the definition of A_i and, similarly, $Y_s\gamma = \alpha_j$, $Y_{r'}\gamma = \alpha_{i'}$, and $Y_{s'}\gamma = \alpha_{j'}$. Thus $\alpha_i - \alpha_j = (Y_r - Y_s)\gamma = (Y_{r'} - Y_{s'})\gamma = \alpha_{i'} - \alpha_{j'}$. This proves part (ii).

It remains to prove (iii). Write $a = (a_1, \ldots, a_n)^T$. Since $Ma = 0$, we have

$$a = Xe + Yf \text{ with } e \in H^s \text{ and } f \in G^{n-s} \tag{6}$$

by Lemma 12 (a), where H is a subgroup of G with $|H| \leq \prod_{j=1}^{s} d_j$ and $d_1, \ldots, d_s$ are the nonzero diagonal entries of D. From the theory of the Smith Normal Form (see [16, p. 41], for instance), it is well known that $\prod_{i=1}^{s} d_i$ is the greatest common divisor of all $s \times s$ minors of M. Let N be such a minor of M. The sum of the positive entries of each row of N is at most 2, and the sum of the negative entries of each row is at least -2, since the same is true for M. Hence $|\det(N)| \leq 2^s$ by Result 11. Recall $s \leq n - 1$. Thus $|H| \leq \prod_{i=1}^{s} d_i \leq 2^{n-1}$.

Now let $a_r, a_s \in A_i$. To complete the proof of (iii), we have to show $a_r - a_s \in H$. By the definition of A_i, we have $Y_r\gamma = Y_s\gamma$, which implies $Y_r = Y_s$. Let $X_1, \ldots, X_n$ denote the rows of X. Using (6), we get

$$a_r - a_s = (X_r - X_s)e + (Y_r - Y_s)f = (X_r - X_s)e.$$

Since $e \in H^s$, this shows $a_r - a_s \in H$. □

For an abelian group G and $t \in \mathbb{Z}$, we write $tG = \{tg : g \in G\}$. Note that tG is a subgroup of G for all $t \in \mathbb{Z}$. The following is well known and straightforward to prove.

Lemma 14. *Let $G \cong (\mathbb{Z}/v_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/v_k\mathbb{Z})$ where $v_1, \ldots, v_k \geq 2$ are integers. Then*

$$|tG| = \frac{|G|}{\prod_{i=1}^{k} \gcd(t, v_i)}$$

for all positive integers t. In particular, $|tG| \geq |G|/t^k$.

For the application of Theorem 13, it is important to provide an upper bound on $\mathrm{rank}_{\mathbb{Q}}(M)$. This is the purpose of the following result. For a group G and $S \subset G$, let $\langle S \rangle$ denote the subgroup of G generated by S.

Theorem 15. *Let G be finite abelian group with invariant factors v_i, $i = 1, \ldots, d(G)$. Suppose A is a subset of G with $0 \in A$ and $\langle A \rangle = G$ that does not have a unique difference. Let M be a coefficient matrix of the linear system (4) determined by A. If $2^{|A|-1} < \prod_{i=1}^{m} v_i$ for some $m \leq d(G)$, then*

$$\mathrm{rank}_{\mathbb{Q}}(M) \leq |A| - d(G) + m - 2.$$

Proof. Let $s = \mathrm{rank}_{\mathbb{Q}}(M)$ and $k = d(G)$. As shown in the proof of Theorem 13, we have $s \leq |A| - 1$ and there is a subgroup H of G with $|H| \leq 2^{|A|-1}$ such that

$$a = Xe + Yf \text{ with } e \in H^s \text{ and } f \in G^{n-s}, \tag{7}$$

where $X \in \mathbb{Z}^{n \times s}$ and $Y \in \mathbb{Z}^{n \times (n-s)}$. Furthermore, all entries of the first column of Y are equal to 1. Write $f = (f_1, \ldots, f_{n-s})^T$ and $Y = (Y_{ij})$. Note that $Xe \in H^n$, since $e \in H^n$. Hence $A \subset H\langle f_1, \ldots, f_{n-s} \rangle$.

By assumption, we have $0 \in A$, say $a_t = 0$. Using (7), we get $0 = a_t = h + \sum_{j=1}^{n-s} Y_{tj} f_j$ for some $h \in H$. Note that $Y_{t1} = 1$, as all entries of the first column of Y are equal to 1. Hence $f_1 = -h - \sum_{j=2}^{n-s} Y_{tj} f_j$ and thus $H\langle f_1, \ldots, f_{n-s} \rangle = H\langle f_2, \ldots, f_{n-s} \rangle$. As $A \subset H\langle f_1, \ldots, f_{n-s} \rangle = H\langle f_2, \ldots, f_{n-s} \rangle$ and $\langle A \rangle = G$ by assumption, we conclude $d(G/H) \leq n - s - 1$.

Recall that $|H| \leq 2^{|A|-1} < \prod_{i=1}^{m} v_i$. Hence $|G/H| > \prod_{i=m+1}^{k} v_i$. We claim that $d(G/H) \geq k - m + 1$. To prove this, suppose $d(G/H) \leq k - m$. Then there is a positive integer $l \leq k - m$ such that

$$G/H = \langle Hg_1 \rangle \times \cdots \times \langle Hg_l \rangle. \tag{8}$$

for some $g_1, \ldots, g_l \in G$. Using (8), Lemma 14, $|G/H| > \prod_{i=m+1}^{k} v_i$, and $l \leq k-m$, we get

$$|v_m(G/H)| \geq \frac{|G/H|}{v_m^l} \geq \frac{|G/H|}{v_m^{k-m}} > \prod_{i=m+1}^{k} \frac{v_i}{v_m}.$$

This implies $|v_m\langle g_1, \ldots, g_l\rangle| > \prod_{i=m+1}^{k} \frac{v_i}{v_m}$. But we have $|v_m G| = \prod_{i=m+1}^{k} \frac{v_i}{v_m}$ by Lemma 14. This is a contradiction, since $v_m\langle g_1, \ldots, g_l\rangle$ is a subgroup of $v_m G$. This shows $d(G/H) \geq k-m+1$.

Combining this with $d(G/H) \leq n-s-1$, we get $s = \mathrm{rank}_{\mathbb{Q}}(M) \leq n-k+m-2$. □

Corollary 16. *Let G be a finite abelian group with invariant factors v_i, $i = 1, \ldots, d(G)$. Suppose A is a subset of G with $0 \in A$ and $\langle A\rangle = G$ that does not have a unique difference. Suppose $|G| > 2^{|A|-1}$ and let m be a positive integer such that $\prod_{i=1}^{m} v_i > 2^{|A|-1}$. Then the conclusions of Theorem 13 hold with*

$$K \geq d(G) - m + 2.$$

In particular, $K \geq 2$.

Proof. This follows from Theorems 13 and 15. □

4 Structure of Group Ring Elements Satisfying $XX^{(-1)} = n$

From now on, we write groups multiplicatively again. The following observation provides a connection between sets with no unique difference and group ring elements satisfying $XX^{(-1)} = n$.

Lemma 17. *Let G be a finite abelian group and let n be a positive integer. Suppose that $X \in \mathbb{Z}[G]$ is a solution of $XX^{(-1)} = n$ and that $|\mathrm{supp}(X)| > 1$. Then* supp(X) *has no unique difference.*

Proof. Write $X = \sum_{g \in S} a_g g$ where $S = \mathrm{supp(X)}$, $a_g \in \mathbb{Z}$, and $a_g \neq 0$ for all $g \in S$. Suppose that supp(X) has a unique difference. Then there is $k \in G$ such that

there is exactly one pair (c, d), $c, d \in \mathrm{supp(X)}$, with $k = cd^{-1}$ (recall that we write G multiplicatively). Note that the identity element of G is not a unique difference of $\mathrm{supp(X)}$, as $|\mathrm{supp(X)}| > 1$. 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 $\mathrm{supp(X)}$. This contradicts $XX^{(-1)} = n$. □

As for G-invariant weighing matrices, we call $X \in \mathbb{Z}[G]$ **proper** if $\langle \mathrm{supp}(Xg) \rangle = G$ for all $g \in G$. The condition for X to be proper in the following theorem is not restrictive. In fact, if $\langle \mathrm{supp}(Xg) \rangle \neq G$, then the theorem can be applied with X replaced by Xg and G replaced by $\langle \mathrm{supp}(Xg) \rangle$.

Theorem 18. *Let G be finite abelian group with invariant factors v_i, $i = 1, \ldots, d(G)$. Suppose that X is a proper element of $\mathbb{Z}[G]$ with $XX^{(-1)} = n$ where n is a positive integer and $|G| > 2^{n-1}$. Let m be a positive integer with $\prod_{i=1}^{m} v_i > 2^{n-1}$. Then there is an integer $K \geq d(G) - m + 2$ such that the following hold.*

There exist a subgroup H of G with $|H| \leq 2^{n-1}$, nonzero elements $X_1, \ldots, X_K$ of $\mathbb{Z}[H]$, and $g_1, \ldots, g_K \in G$, such that

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

(ii) $\mathrm{supp}(X_i g_i) \cap \mathrm{supp}(X_j g_j) = \emptyset$ *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 $A = \mathrm{supp}(X) = \{g \in G : a_g \neq 0\}$. As $XX^{(-1)} = n$ by assumption, A does not have a unique difference by Lemma 17. Furthermore, $XX^{(-1)} = n$ implies $\sum_{g \in G} a_g^2 = n$ and thus $|A| \leq n$.

Replacing X by Xg for some $g \in G$, if necessary, we can assume $1 \in A$. Since X is proper by assumption, we have $\langle A \rangle = G$. As $|G| > 2^{n-1}$ by assumption, Corollary 16 shows that there are $K \geq d(G) - m + 2$, a subgroup H of G with $|H| \leq 2^{n-1}$, integers $\alpha_1 < \cdots < \alpha_K$, and nonempty disjoint subsets $A_1, \ldots, A_K$ of G such that conditions (i)-(iii) in Theorem 13 hold. By condition (iii) of Theorem 13, there are $g_1, \ldots, g_k \in G$ such that $A_i g_i^{-1} \in H$ for all i.

Set $X_i = g_i^{-1} \sum_{g \in A_i} a_g g$ 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. Furthermore, $a_g \neq 0$ for all $g \in A_i$, as $A_i \subset \mathrm{supp}(X)$. We have $\sum_{i=1}^K X_i g_i = \sum_{i=1}^K \sum_{g \in A_i} a_g g = \sum_{g \in \mathrm{supp}(X)} a_g g = X$. Thus condition (i) of Theorem 18 holds. Note that $\mathrm{supp}(X_i g_i) = \mathrm{supp}(\sum_{g \in A_i} a_g g) = A_i$. As the A_i's are disjoint, this proves part (ii) of Theorem 18.

It remains to prove (iii). Recall that $a_g \neq 0$ for all $g \in A_i$ and all i. Thus

$$\begin{aligned}
\mathrm{supp}\left(X_i X_j^{(-1)} g_i g_j^{-1}\right) &= \mathrm{supp}\left((X_i g_i)(X_j g_j)^{(-1)}\right) \\
&= \mathrm{supp}\left(\left(\sum_{g \in A_i} a_g g\right)\left(\sum_{h \in A_j} a_h h^{-1}\right)\right) \\
&\subset \mathrm{supp}\left(\sum_{g \in A_i} \sum_{h \in A_j} g h^{-1}\right) \\
&= \mathrm{supp}\left(A_i A_j^{(-1)}\right). \qquad (9)
\end{aligned}$$

For any real number α, we set

$$Y_\alpha = \sum_{\substack{i,j=1 \\ \alpha_i - \alpha_j \leq \alpha}}^{K} X_i X_j^{(-1)} g_i g_j^{-1} \text{ and } Z_\alpha = \sum_{\substack{i,j=1 \\ \alpha_i - \alpha_j > \alpha}}^{K} X_i X_j^{(-1)} g_i g_j^{-1}.$$

Our strategy is to show $Y_\alpha = 0$ when $\alpha < 0$. Subsequently, we use some specific values for α and the condition $Y_\alpha = 0$ to show that (iii) holds.

Consider integers i, j, i', j' with $1 \leq i, j, i', j' \leq K$. By condition (ii) of Theorem 13, the intersection of $\mathrm{supp}(A_i A_j^{-1})$ and $\mathrm{supp}(A_{i'} A_{j'}^{-1})$ can only be nonempty if $\alpha_i - \alpha_j = \alpha_{i'} - \alpha_{j'}$. In view of (9), this implies that

$$\mathrm{supp}\left(X_i X_j^{(-1)} g_i g_j^{-1}\right) \cap \mathrm{supp}\left(X_{i'} X_{j'}^{(-1)} g_{i'} g_{j'}^{-1}\right) \neq \emptyset \text{ only if } \alpha_i - \alpha_j = \alpha_{i'} - \alpha_{j'}. \qquad (10)$$

Taking $i' = j'$ in (10), we conclude

$$1 \notin \mathrm{supp}(X_i X_j^{(-1)} g_i g_j^{-1}) \text{ whenever } i < j, \qquad (11)$$

since $1 \in \mathrm{supp}(X_{i'} X_{i'}^{(-1)})$ for all i' and $\alpha_i - \alpha_j \neq 0$ for $i < j$. Furthermore, (10) implies

$$\mathrm{supp}(Y_\alpha) \cap \mathrm{supp}(Z_\alpha) = \emptyset \qquad (12)$$

for all $\alpha \in \mathbb{R}$. Note that

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

We conclude $\mathrm{supp}(Y_\alpha + Z_\alpha) = \mathrm{supp}(n) = \{1\}$. Thus, in view of (12), we either have $Y_\alpha = 0$ or $\mathrm{supp}(Y_\alpha) = 1$. If $\alpha < 0$, then $i < j$ for all terms $X_i X_j^{(-1)} g_i g_j^{-1}$ occuring in Y_α. Hence $1 \notin \mathrm{supp}(Y_\alpha)$ by (11) and thus

$$Y_\alpha = 0 \text{ for } \alpha < 0. \tag{13}$$

We now consider some specific values of α. Recall that $\alpha_1 < \alpha_2 < \cdots < \alpha_K$. For any $1 \le t < \ell \le K$, we define $\alpha(t,\ell) = \alpha_t - \alpha_\ell$. Clearly, $\alpha(t,\ell) < 0$. We also define

$$B(t,\ell) = \{(i,j) : i \ge t \text{ and } \alpha_i - \alpha_j \le \alpha(t,\ell)\}.$$

Note that $i < j$ for all $(i,j) \in B(t,\ell)$, since $\alpha(t,\ell) < 0$. Observe that $\alpha_j - \alpha_\ell \ge \alpha_i - \alpha_t \ge 0$ for $(i,j) \in B(t,\ell)$. Thus $j \ge \ell$ whenever $(i,j) \in B(t,\ell)$. Moreover, $j > \ell$ whenever $(i,j) \in B(t,\ell)$ and $i > t$. Therefore, we can write

$$B(t,\ell) = \{(t,\ell)\} \cup B'(t,\ell)$$

where $B'(t,\ell) = \{(i,j) \in B(t,\ell) : j > \ell\}$.

By (13), we have

$$Y_{\alpha(1,\ell)} = \sum_{(i,j)\in B(1,\ell)} X_i X_j^{(-1)} g_i g_j^{-1} = 0 \text{ for } \ell > 1. \tag{14}$$

First, setting $\ell = K$ in (14), we get $X_1 X_K^{(-1)} = 0$, as $B(1,K) = \{(1,K)\}$. Now we prove by induction that

$$X_1 X_K^{(-1)} = X_1 X_{K-1}^{(-1)} = \cdots = X_1 X_2^{(-1)} = 0. \tag{15}$$

Suppose we have

$$X_1 X_K^{(-1)} = X_1 X_{K-1}^{(-1)} = \cdots = X_1 X_\ell^{(-1)} = 0 \tag{16}$$

with $\ell \ge 3$. Recall that $B(1,\ell-1) = \{(1,\ell-1)\} \cup B'(1,\ell-1)$. Therefore,

$$Y_{\alpha(1,\ell-1)} = X_1 X_{\ell-1}^{(-1)} + \sum_{(i,j)\in B'(1,\ell-1)} X_i X_j^{(-1)} g_i g_j^{-1} = 0. \tag{17}$$

By the induction assumption (16), we have $X_1 X_j^{(-1)} = 0$ for $j \geq \ell$. As $j \geq \ell$ for $(i,j) \in B'(1, \ell-1)$, after multiplying (17) by X_1, we get

$$(X_1)^2 X_{\ell-1}^{(-1)} = 0. \tag{18}$$

Let χ be any complex character of G. Note that (18) 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 10. This completes the proof of (15).

Now we show by induction on t that $X_i X_j^{(-1)} = 0$ whenever $i \leq t$ and $i < j$. For $t = 1$ this holds by (15). Suppose that $X_i X_j^{(-1)} = 0$ whenever $i \leq t-1$ and $i < j$. We have

$$0 = Y_{\alpha(t,\ell)} = \sum_{\substack{i,j=1 \\ \alpha_i - \alpha_j \leq \alpha(t,\ell)}}^{K} X_i X_j^{(-1)} g_i g_j^{-1}$$

for all $\ell > t$ by (13), as $\alpha(t,\ell) < 0$. In the sum above, all terms with $i < t$ vanish by the induction assumption. Therefore,

$$0 = \sum_{\substack{i,j=1 \\ i \geq t \\ \alpha_i - \alpha_j \leq \alpha(t,\ell)}}^{K} X_i X_j^{(-1)} g_i g_j^{-1} = \sum_{(i,j) \in B(t,\ell)} X_i X_j^{(-1)} g_i g_j^{-1}$$

for $\ell > t$ by the definition of $B(t,\ell)$. Now apply the same argument as before, we obtain $X_t X_j^{(-1)} = 0$ for all $j > t$.

In summary, we have shown $X_i X_j^{(-1)} = 0$ whenever $i \neq j$. Hence $\chi(X_i)\overline{\chi(X_j)} = 0$ for all complex characters χ of G and all $i \neq j$. This implies $\chi(X_i)\chi(X_j) = 0$ for all complex characters χ of G and thus $X_i X_j = 0$ for all $i \neq j$ by Result 10. This completes the proof of part (iii) of Theorem 18.

□

5 Group Invariant Weighing Matrices

In this section, we prove the results on group invariant matrices stated in the introduction.

Proof of Theorem 4 Let n be a positive integer and let X be a weighing matrix of weight n invariant under an abelian group G. By Lemma 1, we can view X as an element of $\mathbb{Z}[G]$ satisfying $XX^{(-1)} = n$. We need to show that X is generated from subgroup H of G with $|H| \leq 2^{n-1}$.

Write $A = \mathrm{supp}(X)$. Replacing X by Xg for some $g \in G$, if necessary, we can assume $1 \in A$. If $|\langle A \rangle| \leq 2^{n-1}$, there is nothing to show, since then X trivially is generated from $\langle A \rangle$ (in this case $K = 1$ and $X_1 = X$). Thus we may assume $|\langle A \rangle| > 2^{n-1}$. But then X is generated from a subgroup H of $\langle A \rangle$ with $|H| \leq 2^{n-1}$ by Theorem 18. □

Proof of Corollary 6 Let G be a cyclic group of order v. Suppose there exists a proper circulant weighing matrix $X \in \mathbb{Z}[G]$ of weight n, where is an odd prime power. We need to show $v \leq 2^{n-1}$.

Suppose $v > 2^{n-1}$. We may assume $1 \in \mathrm{supp}(X)$. Since X is proper, we have $\langle \mathrm{supp}(X) \rangle = G$ and thus $|\langle \mathrm{supp}(X) \rangle| = v > 2^{n-1}$. By Theorem 18, there is a proper subgroup H of G such that X is generated from H. Hence $X = \sum_{i=1}^{K} X_i g_i$ with $X_i \in \mathbb{Z}[H]$ and $g_i \in G$ for some positive integer K, such that the conditions (i)-(iii) of Theorem 18 are satisfied. Note that $K \geq d(G) - m + 2 \geq 2$. But this is impossible by [12, Thm. 2.6]. Thus $v \leq 2^{n-1}$. □

Proof of Theorem 8 Suppose a proper G-invariant weighing matrix X of weight n exists, and that $\prod_{i=1}^{m} v_i > 2^{n-1}$, where the v_i's are invariant factors of G. We have to show

$$n \geq (d(G) - m + 2)^2 . \tag{19}$$

By Theorem 18, we have $X = \sum_{i=1}^{K} X_i g_i$ where $K \geq d(G) - m + 2$ and the conditions stated in Theorem 18 hold. Let $i \in \{1, \ldots, K\}$ be arbitrary. Since $X_i \neq 0$, there is a character χ of G such that $\chi(X_i) \neq 0$. As $X_i X_j = 0$ for all $j \neq i$, we conclude $\chi(X_j) = 0$ for $j \neq 0$. Thus $\chi(X) = \chi(X_i g_i)$. Since $XX^{(-1)} = n$, we have $|\chi(X)|^2 = n$. Hence $|\chi(X_i)| = \sqrt{n}$. This implies $|X_i| \geq \sqrt{n}$. Comparing the coefficient of the identity in $n = XX^{(-1)} = \sum_{i=1}^{K} X_i X_i^{(-1)}$, we get $n = \sum_{i=1}^{K} |X_i| \geq K\sqrt{n}$, i.e., $n \geq K^2$. Since $K \geq d(G) - m + 2$, this proves (19). □

6 Application to Multipliers of Difference Sets

We now sketch how Theorem 18 can be used to improve the multiplier theorem for difference sets obtained in [13]. We first recall a simplified slightly weakened version of this result. We refer the reader to [8] for the necessary background on difference sets.

Define a function $M(m)$ for all positive integers m recursively as follows. Set $M(1) = 1$. For $m > 1$, let p be a prime divisor of m, and let p^e be the highest power of p dividing m. Then $M(m)$ is the product of the distinct prime factors of

$$m, M(\frac{m^2}{p^{2e}}), p-1, p^2-1, ..., p^{2m}-1.$$

We remark that the number $M(m)$ depends on the order in which the prime divisors of m are chosen for the recursion. Result 19 below, however, holds for all possible values of $M(m)$. By [13, Thm. 1.4], we have the following.

Result 19. *Let D be a (v, k, λ, n) difference set in an abelian group G of exponent v^*. Let n_1 be a divisor of n with $(v, n_1) = 1$. Suppose that t is an integer such that, for every prime divisor u of n_1, there is an integer f_u with $t \equiv u^{f_u} \pmod{v^*}$. Let $m = n/n_1$. If v and $M(m)$ are coprime, then t is a multiplier of D.*

The connection to the results of the current paper is that Theorem 18 can be used to remove all prime divisors of $M(m)$ which are larger than 2^{m^2-1}, without affecting the validity of Result 19. The proof of this fact will be presented in [14]. In cases where m has a large number of distinct prime divisors, this yields a substantial improvement upon Result 19, since $M(m)$ often will have many prime divisors larger than 2^{m^2-1} for such m.

For instance, suppose $m = \pi(2t)$ where $\pi(s)$ denotes the product of the first s primes. It is well known that $\pi(s) = s^{(1+o(1))s}$. It can be seen [14] that, no matter which order of the prime divisors of m is chosen to compute $M(m)$, there are a prime divisor p of $\pi(2t)$ and an integer $u > \pi(t)^{2^t}$ such that all prime divisors of $p^u - 1$ divide $M(m)$. On the other hand, as a consequence of Theorem 18, all prime divisors exceeding $2^{\pi(2t)^2-1}$ can be removed from $M(m)$ without affecting the validity of Result 19. Note that $u = t^{2^t(1+o(1))t}$ and $\pi(2t)^2 = t^{(4+o(1))t}$ and thus $p^u \gg 2^{\pi(2t)^2}$ for large t. This indicates that Theorem 18

indeed can be used to replace $M(m)$ by a substantially smaller number and thus yields a significant improvement of the multiplier theorem in [13] in cases where m has many distinct prime divisors.

References

[1] M. H. Ang, S. L. Ma: Symmetric weighing matrices constructed using group matrices. *Des. Codes Cryptogr.* **37** (2005), 195–210.

[2] 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.

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

[4] K. T. Arasu, J. R. Hollon: Group developed weighing matrices. *Australasian J. Comb.* **55** (2013), 205–233.

[5] K.T. Arasu, K.H. Leung, S.L. Ma, A. Nabavi, D.K. Ray-Chaudhuri: Determination of all possible orders of weight 16 circulant weighing matrices. *Finite Fields Appl.* **12** (2006) 498–538.

[6] K.T. Arasu, K.H. Leung, S.L. Ma, A. Nabavi, D.K. Ray-Chaudhuri: Circulant weighing matrices of weight 2^{2t}. *Des. Codes Crypt.* **41** (2006), 111–123.

[7] K.T. Arasu, S.L. Ma: Some new results on circulant weighing matrices. *J. Alg. Comb.* **14** (2001), 91-101.

[8] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (2*nd edition*). Cambridge University Press 1999.

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

[10] P. Eades, R. M. Hain: On Circulant Weighing Matrices. *Ars Comb.* **2** (1976), 265–284.

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

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

[13] K. H. Leung, S. L. Ma, B. Schmidt: A multiplier theorem. *J. Combin. Theory* Ser. A **124** (2014), 228–243.

[14] K. H. Leung and B. Schmidt: Improvements on multiplier theorems. In preparation.

[15] R. L. McFarland: On multipliers of abelian difference sets. Ph.D. Dissertation, Ohio State University (1970).

[16] C. Norman: *Finitely Generated Abelian Groups and Similarity of Matrices over a Field.* Springer 2012.

[17] A. Schinzel: An inequality for determinants with real entries. *Colloq. Math.* **38** (1977/78), 319–321.

[18] B. Schmidt: *Characters and cyclotomic fields in finite geometry.* Lecture Notes in Mathematics **1797**. Springer 2002.

[19] J. Seberry, A. L. Whiteman: Some results on weighing matrices. *Bull. Aust. Math. Soc.* **12** (1975) 433–447.

[20] Y. Strassler: *The classification of circulant weighing matrices of weight 9.* Ph.D. Thesis, Bar-Ilan University 1997.

[21] E. Steinitz: Ernst Rechteckige Systeme und Moduln in algebraischen Zahlkörpern. I. *Math. Ann.* **71** (1911), 328–354.