A Multiplier Theorem

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

Siu Lun Ma
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

Abstract

We show that the assumption $n_1 > \lambda$ in the Second Multiplier Theorem can be replaced by a divisibility condition weaker than the condition in McFarland's multiplier theorem, thus obtaining significant progress towards the multiplier conjecture.

1 Introduction

A (v, k, λ, n) **difference set** in a finite group G of order v is a k-subset D of G such that every element $g \neq 1$ of G has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. As usual, we assume $1 < k < v/2$. The positive integer $n = k - \lambda$ is called the **order** of the difference set.

Hall [5] introduced the concept of multipliers of difference sets. An integer t is a **multiplier** of D if $\{d^t : d \in D\} = \{dg : d \in G\}$ for some $g \in G$.

In 1947, Hall [5] proved that every prime divisor of the order of a planar difference set is a multiplier of the difference set. In 1951, Hall and Ryser [7] generalized this result and obtained what is now called the First Multiplier Theorem. The following conjecture, which is a classical unsolved problem, originated from their paper [7].

Conjecture 1.1 (Multiplier Conjecture) *Let D be a (v, k, λ, n) difference set in an abelian group. If p is a prime dividing n, but not v, then p is a multiplier of D.*

Another substantial result on the multiplier conjecture was obtained by Hall [6]. Later it was generalized by Menon [11] to what is now known as the Second Multiplier Theorem.

Result 1.2 (Second Multiplier Theorem) *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 $t \equiv u^{f_u} \pmod{v^*}$. If $n_1 > \lambda$, then t is a multiplier of D.*

A beautiful approach to the multiplier conjecture was developed by McFarland [9] in 1970. The Second Multiplier Theorem is a simple special case in his work, thus giving an elegant, short proof of this theorem. More importantly, he obtained the following result, which goes much further and is the strongest known multiplier theorem. For the definition of the function M' used in this theorem, please see Section 5.

Result 1.3 (McFarland [9, Thm. 6, p. 68]) *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 $t \equiv u^{f_u} \pmod{v^*}$. If v and $M'(n/n_1)$ are coprime, then t is a multiplier of D.*

Qiu [13, 14, 15], Muzychuk [12], and Feng [3] improved Result 1.3 for certain values of n/n_1, e.g., $n/n_1 \in \{2, 3, 4, 5\}$. Beyond that there has not been significant progress towards the multiplier conjecture since McFarland's work. A generalization of the Second Multiplier Theorem to divisible difference sets can be found in [1].

We will show that, in general, $M'(n/n_1)$ in McFarland's result can be replaced by a significantly smaller number, thus obtaining a substantial improvement upon existing multiplier theorems. For the formulation of our result, we define a function $M(m, b)$ for all positive integers m, b recursively as follows. We set $M(1, b) = 1$ for all b. For $m > 1$, let p be a prime divisor of m, and let p^e be the highest power of p dividing m. Then $M(m, b)$ is the product of the distinct prime factors of

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

The following is the main result of this paper.

Theorem 1.4 *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 $t \equiv u^{f_u} \pmod{v^*}$. If v and $M(n/n_1, \lfloor k/n_1 \rfloor)$ are coprime, then t is a multiplier of D.*

Note that $M(m, b)$ in general is not uniquely defined, as it depends on the order in which the prime divisors of m are chosen for the recursion. But Theorem 1.4 holds no matter which of the possible values for $M(m, b)$ is chosen. The flexibility in choosing the order of the prime divisors of m for the computation of $M(m, b)$ is significant. For a given parameter set (v, k, λ, n), one choice for the order of prime divisors might give a value for

$M(m,b)$, which is coprime to v, while another choice may result in a value for $M(m,b)$, which has a common divisor with v.

A remark concerning the formulation of Theorem 1.4 is in order. To avoid the ambiguity concerning $M(m,b)$, we could replace $M(m,b)$ by the set $\mathcal{M}(m,b)$ of all values for $M(m,b)$, which can be obtained from some choice of the order of prime divisors of m. Then the statement of Theorem 1.4 would be "If v is coprime to at least one number in $\mathcal{M}(m,b)$, then t is a multiplier of D". We follow McFarland, however, and avoid this clumsier formulation, which might be considered more precise, but only from a superficial point of view.

Theorem 1.4 is a significant improvement of Result 1.3. The improvement is obtained by a new way to study putative nontrivial solutions of group ring equations $XX^{(-1)} = m$ over abelian groups G. McFarland [9] discovered a lower bound on the number of nonzero coefficients of X, which leads to a contradiction if m is too small compared to the orders of prime divisors of m modulo prime divisors of $|G|$. Our approach is to look at the behavior of the coefficient of the identity in X in a sequence of homomorphic images of X. Quite surprisingly, this coefficient can be controlled over this sequence under reasonable conditions. Eventually, when we reach the homomorphic image of X in the trivial group, bounds on the coefficient of the identity produce a contradiction, which means that X itself must be trivial.

2 Preliminaries

Let G be a finite abelian group of order v. The least common multiple of the orders of the elements of G is called the **exponent** of G. We denote the group of complex character of G by $\hat{G}$. The character sending all elements of G to 1 is called **trivial**.

We will make use of the integral group ring $\mathbb{Z}[G]$. Let $X = \sum a_g g \in \mathbb{Z}[G]$, and let t be an integer. The a_g's are called the **coefficients** of X. We write $|X| = \sum a_g$ and $X^{(t)} = \sum a_g g^t$. The set $\mathrm{supp}(X) = \{g \in G : a_g \neq 0\}$ is called the **support** of X. Let 1 denote the identity element of G. For $a \in \mathbb{Z}$ we simply write a for the group ring element $a \cdot 1$. The coefficient of 1 in a

group ring element is called the **coefficient of the identity** (and will play an important role in this paper). For $S \subset G$, we write S instead of $\sum_{g \in S} g$. We say that $X \in \mathbb{Z}[G]$ is **trivial** if $X = ag$ for some integer a and $g \in G$.

Using the group ring notation, a k-subset of G is a (v, k, λ, n) difference set in G if and only if

$$DD^{(-1)} = n + \lambda G \tag{1}$$

in $\mathbb{Z}[G]$. Furthermore, this group ring equation holds if and only if $\chi_0(D) = k$ for the trivial character χ_0 of G and $|\chi(D)|^2 = n$ for all nontrivial characters χ of G.

We need the following fact.

Lemma 2.1 *Let G be a finite group of order q^a where q is a prime, and let t be a positive integer with $(q, t) = 1$. Let Y be an orbit of $x \mapsto x^t$ on $G \setminus \{1\}$. Then $|Y| \equiv 0 \pmod{\mathrm{ord}_q(t)}$.*

Proof Choose $g \in G \setminus \{1\}$ such that $Y = \{g^{t^i} : i \in \mathbb{Z}\}$. Let y be the smallest positive integer with $g^{t^y} = g$. Note that $Y = \{g, g^t, \ldots, g^{t^{y-1}}\}$ and thus $|Y| = y$. Moreover, $g^{t^y - 1} = 1$, which implies $t^y - 1 \equiv 0 \pmod{o(g)}$, where $o(g)$ denotes the order of g in G. As $g \neq 1$, we have $o(g) \equiv 0 \pmod{q}$. Hence $t^y - 1 \equiv 0 \pmod{q}$ and thus $|Y| = y \equiv 0 \pmod{\mathrm{ord}_q(t)}$. □

We write $\zeta_v = \exp(2\pi i/v)$. For a simple proof of the following result, see [2, Chapter VI, Theorem. 15.2].

Result 2.2 *Let p be a prime, and let m be a positive integer with $(m, p) = 1$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ such that $\zeta_m^\sigma = \zeta_m^{p^i}$ for some positive integer i. Then σ fixes all prime ideals above p in $\mathbb{Z}[\zeta_m]$.*

For a proof of the following result, see [2, Section VI.3].

Result 2.3 *Let G be a finite abelian group, and let $D = \sum_{g \in G} d_g g \in \mathbb{Z}[G]$. Then*

$$d_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(Dg^{-1})$$

for all $g \in G$ (Fourier Inversion Formula).

We will use the following consequence of Results 2.2 and 2.3 repeatedly. In the proof we will use some basic facts from algebraic number theory. We refer to [8] for the necessary background.

Corollary 2.4 *Let G be a finite abelian group of exponent v^*. Suppose that $X \in \mathbb{Z}[G]$ satisfies*

$$XX^{(-1)} + \alpha G \equiv 0 \pmod{w} \tag{2}$$

for some integers α and w with $(|G|, w) = 1$. Moreover, suppose that z is a positive integer with $(|G|, z) = 1$ such that, for every prime divisor p of w, there is an integer f_p with

$$z \equiv p^{f_p} \pmod{v^*}. \tag{3}$$

Then

$$X^{(z)}X^{(-1)} + \alpha G \equiv 0 \pmod{w}. \tag{4}$$

Proof Let p be any prime divisor of w and let p^e be the largest power of p dividing w. We will show that $X^{(z)}X^{(-1)} + \alpha G \equiv 0 \pmod{p^e}$, which implies (4).

Let

$$p\mathbb{Z}[\zeta_{v^*}] = \prod \mathfrak{p}_i$$

be the prime ideal factorization of the ideal $p\mathbb{Z}[\zeta_{v^*}]$ in $\mathbb{Z}[\zeta_{v^*}]$. Note that the $\mathfrak{p}_i$'s are pairwise distinct, as p is coprime to v^* by the assumption $(|G|, w) = 1$. Let ν_i be the valuation corresponding to $\mathfrak{p}_i$, i.e., for every $y \in \mathbb{Z}[\zeta_{v^*}]$, the highest power of $\mathfrak{p}_i$ dividing $y\mathbb{Z}[\zeta_{v^*}]$ is $\mathfrak{p}_i^{\nu_i(y)}$.

Let χ be any nontrivial character of G. By (2), we have

$$\chi(X)\overline{\chi(X)} = \chi(XX^{(-1)}) \equiv 0 \pmod{p^e}$$

and thus

$$\nu_i\left(\chi(X)\right) + \nu_i\left(\overline{\chi(X)}\right) \geq e \tag{5}$$

for all i.

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{v^*})/\mathbb{Q})$ be defined by $\zeta_{v^*}^{\sigma} = \zeta_{v^*}^{z}$. It follows from Result 2.2 and (3) that σ fixes all prime ideals $\mathfrak{p}_i$. Note that $\chi(X^{(z)}) = \chi(X)^{\sigma}$. As σ fixes each $\mathfrak{p}_i$, we have $\nu_i\left(\chi(X)^{\sigma}\right) = \nu_i\left(\chi(X)\right)$. Hence

$$\nu_i\left(\chi(X^{(z)})\right) = \nu_i\left(\chi(X)^{\sigma}\right) = \nu_i\left(\chi(X)\right)$$

for all i. Combining this with (5), we conclude

$$\nu_i\left(\chi(X^{(z)})\right) + \nu_i\left(\overline{\chi(X)}\right) \geq e$$

for all i. Hence

$$\chi(X^{(z)}X^{(-1)} = \chi(X^{(z)})\overline{\chi(X)} \equiv 0 \pmod{p^e} \tag{6}$$

for all nontrivial characters χ of G.

Write $F = X^{(z)}X^{(-1)} + \alpha G$. By (6), we have $\chi(F) \equiv 0 \pmod{p^e}$ for all nontrivial characters χ of G. Let χ_0 denote the trivial character of G. Note that $\chi_0(X^{(z)}) = \chi_0(X^{(-1)}) = \chi_0(X)$. By (2), we have $\chi_0(X)^2 + \alpha|G| \equiv 0 \pmod{p^e}$. Thus

$$\chi_0(F) = \chi_0(X^{(z)})\chi_0(X^{(-1)}) + \alpha|G| = \chi_0(X)^2 + \alpha|G| \equiv 0 \pmod{p^e}.$$

In summary, we have shown $\chi(F) \equiv 0 \pmod{p^e}$ for all characters χ of G. Recall that p is coprime to $|G|$ by assumption. Thus Result 2.3 implies $F \equiv 0 \pmod{p^e}$. □

The next result is due to McFarland [9]. We include a proof for the convenience of the reader.

Result 2.5 *Let G be an abelian group, and let t be an integer with $(v,t) = 1$.*

(a) Suppose $F \in \mathbb{Z}[G]$ satisfies $FF^{(-1)} = n$ for some integer n. If $F^{(-1)}F^{(t)}$ is divisible by n, then $F^{(t)} = Fg$ for some $g \in G$.

(b) Let D be a (v,k,λ,n) difference set in G. If $D^{(-1)}D^{(t)} - \lambda G$ is divisible by n, then t is a multiplier of D.

Proof

(a) Write $F = \sum_{h\in G} a_h h$ and $F^{(t)} = \sum_{h\in G} b_h h$. Note $\sum a_h^2 = \sum b_h^2$. Since

$FF^{(-1)} = n$, we have $\sum a_h^2 = n$. Write $X = F^{(-1)}F^{(t)}$. Since $FF^{(-1)} = n$, we have $XX^{(-1)} = n^2$. Hence the sum of the squares of the coefficients of X is n^2. As X is divisible by n by assumption, this implies $X = gn$ for some $g \in G$. Comparing the coefficient of g on both sides of $F^{(-1)}F^{(t)} = gn$, we get $\sum_{h\in H} a_h b_{gh} = n$. Hence

$$\sum_{h\in H}(a_h - b_{gh})^2 = \sum_{h\in H} a_h^2 + \sum_{h\in H} b_h^2 - 2\sum_{h\in H} a_h b_{gh} = n + n - 2n = 0.$$

Thus $b_{gh} = a_h$ for all $h \in G$, i.e., $F^{(t)} = Fg$. This proves part (a).

(b) Write $E = D^{(-1)}D^{(t)} - \lambda G$ and suppose that E is divisible by n. A straightforward computation shows that $EE^{(-1)} = n^2$ and $DE = nD^{(t)}$. Note that $|E| = k^2 - \lambda v = n > 0$. As E is divisible by n and $EE^{(-1)} = n^2$, we conclude that E has at most one nonzero coefficient. Hence $E = ng$ for some $g \in G$. This implies $nD^{(t)} = DE = nDg$ and thus $D^{(t)} = Dg$. □

Remark 2.6 The proof of Result 2.5 (b) shows that t is multiplier of D if $E = D^{(-1)}D^{(t)} - \lambda G$ is trivial. Furthermore, $EE^{(-1)} = n^2$.

McFarland and Mann [10] showed that every multiplier of a difference set fixes at least one translate of the difference set. This implies the following.

Result 2.7 *Suppose D is a (v, k, λ, n) difference set in an abelian group G, where $v = q^b$ for a prime q and a positive integer b. Let t be an integer with $(q, t) = 1$ and write $f = \mathrm{ord}_q(t)$. If t is a multiplier of D, then $k \equiv 0 \pmod f$ or $k \equiv 1 \pmod f$.*

Proof By [10], we can assume $D^{(t)} = D$. Thus D is a union of orbits of $x \mapsto x^t$ on G. By Lemma 2.1, the sizes of all orbits of $x \mapsto x^t$ on $G \setminus \{1\}$ are divisible by f. Hence $k = |D| \equiv 0 \pmod f$ if $1 \notin D$ and $k \equiv 1 \pmod f$ if $1 \in D$. □

3 Triviality of Solutions to $XX^{(-1)} = m^2$

Let G be an abelian group and let m be a positive integer. In view of Remark 2.6, the triviality of solutions to $XX^{(-1)} = m^2$ can be used to prove

the existence of multipliers. This fundamental idea is due to McFarland. In this section, we improve upon McFarland's results by providing new sufficient conditions for the triviality of solutions to $XX^{(-1)} = m^2$.

First we define a function $M(m)$, which is similar to McFarland's M-function, but has significantly smaller values for $m \geq 5$.

Definition 3.1 Let $M(m,t)$ be the function defined in Section 1. Define

$$M(m) = \begin{cases} (4m-1)M(m,2m-2) & \text{if } 4m-1 \text{ is a prime,} \\ M(m,2m-2) & \text{otherwise.} \end{cases}$$

Again, note that the function $M(m)$ is not uniquely defined in general, but all our results hold, no matter which version of $M(m)$ is used. One may wonder why there is an extra term when $4m-1$ is a prime. As it can be seen in the proof of Theorem 3.4, the case where $4m-1$ is a prime plays a special role. In fact, it can be shown that there are nontrivial solutions to $XX^{(-1)} = m^2$ when $4m-1$ is a prime.

Now we are ready to state the main result of this section.

Theorem 3.2 *Let G be a finite abelian group and suppose that $X \in \mathbb{Z}[G]$ is a solution of $XX^{(-1)} = m^2$, where m is a positive integer. If the order of G is is coprime to $M(m)$, then X is trivial.*

The proof of Theorem 3.2 turns out to be complicated. We first need to consider the problem with the additional condition $X^{(z)} = X$, where z is an integer with $(|G|, z) = 1$.

Theorem 3.3 *Let G be a finite abelian group and let m, z be positive integers with $(|G|, z) = 1$. Let $X \in \mathbb{Z}[G]$ be a solution of $XX^{(-1)} = m^2$ and suppose that $X^{(z)} = X$. Let b_0 be the coefficient of the identity in X.*

If there exists a positive real number a such that $-a \leq b_0$ and $\mathrm{ord}_q(z) > m + a$ for all prime divisors q of $|G|$, then X is trivial.

Proof Suppose that X is nontrivial. Note that $|X| = \pm m$, since $XX^{(-1)} = m^2$. Replacing X by $-X$ if necessary, we may assume $|X| = m$. Let $q_1, \ldots, q_s$ be the distinct prime divisors of $|G|$ and write

$$G = G_1 \times \cdots \times G_s,$$

where G_i is the Sylow q_i-subgroup of G, $i = 1, \ldots, s$. For convenience, we may assume

$$\mathrm{ord}_{q_1}(z) \geq \mathrm{ord}_{q_2}(z) \cdots \geq \mathrm{ord}_{q_s}(z). \tag{7}$$

We consider the sequence of homomorphisms

$$\rho_i : G \to G_{i+1} \times \cdots \times G_s, \ i = 0, \ldots, s-1,$$

defined by $\rho_i(g) = 1$ for $g \in G_1 \times \cdots \times G_i$ and $\rho_i(g) = g$ for $g \in G_{i+1} \times \cdots \times G_s$. Moreover, define ρ_s by $\rho_s(g) = 1$ for all $g \in G$. The subsequent application of $\rho_1, \ldots, \rho_s$ sends all elements of G to the identity, and we may visualize this process by

$$G \xrightarrow{\rho_1} G_2 \times \cdots \times G_s \xrightarrow{\rho_2} \cdots \xrightarrow{\rho_{s-2}} G_{s-1} \times G_s \xrightarrow{\rho_{s-1}} G_s \xrightarrow{\rho_s} \{1\}.$$

Note that $\rho_s(X)$ is trivial. Hence there exists a smallest integer $r \leq s$ such that $\rho_r(X)$ is trivial. Our aim is to show $r = 0$ by deriving a contradiction if $r > 0$. Thus suppose $r > 0$.

Recall that $XX^{(-1)} = m^2$ and $X^{(z)} = X$ by assumption. Hence

$$\rho_i(X)\rho_i(X)^{(-1)} = m^2 \ \text{ and } \ \rho_i(X)^{(z)} = \rho_i(X)$$

for all i. Furthermore, $|\rho_i(X)| = |X| = m$ for all i.

For $i = 0, \ldots, s$, let b_i be the coefficient of the identity in $\rho_i(X)$. The key to our proof is to investigate how the b_i's are related.

We have $|b_i| \leq m$ for all i. To see this, write $\rho_i(X) = b_i + \sum_{g \in G \setminus \{1\}} a_g g$ with $a_g \in \mathbb{Z}$. Comparing the coefficient of the identity on both sides of $\rho_i(X)\rho_i(X)^{(-1)} = m^2$ gives $b_i^2 + \sum_{g \in G \setminus \{1\}} a_g^2 = m^2$. This implies $|b_i| \leq m$.

We now show that $\rho_i(X)$ is trivial if and only if $b_i = m$ (this holds for all i including $i = 0$). To this end, first suppose that $\rho_i(X)$ is trivial. Recall

that we assume $|X| = m$. Hence $|\rho_i(X)| = m$ and thus $\rho_i(X) = mk$ for some $k \in \rho_i(G)$. Recall that $\mathrm{ord}_q(z) > m + a > 1$ for all prime divisors q of $|G|$ by assumption. This implies $(|G|, z-1) = 1$. As $\rho_i(X)^{(z)} = \rho_i(X)$, we have $k^z = k$ and thus $k^{z-1} = 1$. As $(|G|, z-1) = 1$, we conclude $k = 1$. Thus $\rho_i(X) = m$, i.e., $b_i = m$.

Now suppose $b_i = m$. Recall that $b_i^2 + \sum_{g \in G \setminus \{1\}} a_g^2 = m^2$. As $b_i = m$, this implies $a_g = 0$ for all $g \in G \setminus \{1\}$ and thus $\rho_i(X) = b_i = m$. Hence $\rho_i(X)$ is trivial. This completes the proof for the claim that $\rho_i(X)$ is trivial if and only if $b_i = m$.

Recall that r is the smallest positive integer such that $\rho_r(X)$ is trivial. Hence, by what we have shown, r is the smallest positive integer such that $b_r = m$. Furthermore, $b_i < m$ for all $i < r$.

Next we claim that

$$b_{i+1} = b_i + y_{i+1}\mathrm{ord}_{q_{i+1}}(z) \tag{8}$$

with $y_{i+1} = \{-1, 0, 1\}$, for $i = 0, \ldots, s-1$. Recall that

$$\rho_i(X) \in \mathbb{Z}[G_{i+1} \times \cdots \times G_s]$$

by the definition of ρ_i. Hence we can write

$$\rho_i(X) = Y_i + Z_i \tag{9}$$

with $\mathrm{supp}(Y_i) \subset G_{i+1}$ and $\mathrm{supp}(Z_i) \subset (G_{i+1} \times \cdots \times G_s) \setminus G_{i+1}$.

Now we consider the action of $x \mapsto x^z$ on $G_{i+1} \times \cdots \times G_s$. Recall that $\rho_i(X)^{(z)} = \rho_i(X)$. As $G_{i+1}^{(z)} = G_{i+1}$, we conclude $Y_i^{(z)} = Y_i$ and $Z_i^{(z)} = Z_i$. As $Y_i^{(z)} = Y_i$, we can write

$$Y_i = b_i + \sum a_j T_j, \tag{10}$$

where $a_j \in \mathbb{Z}$ and the T_j's are orbits of $x \mapsto x^z$ on $G_{i+1} \setminus \{1\}$. Recall that the order of G_{i+1} is a power of q_{i+1}. Hence

$$|T_j| \equiv 0 \pmod{\mathrm{ord}_{q_{i+1}}(z)} \tag{11}$$

for all j by Lemma 2.1. Recall that b_{i+1} is the coefficient of the identity in $\rho_{i+1}(X)$. Applying ρ_{i+1} to (9), we get $b_{i+1} = |Y_i|$. Thus (10) and (11) imply

$$b_{i+1} = |Y_i| \equiv b_i \pmod{\mathrm{ord}_{q_{i+1}}(z)}.$$

Hence $b_{i+1} = b_i + y_{i+1}\mathrm{ord}_{q_{i+1}}(z)$ for some integer y_{i+1}. Moreover, as $|b_i| \leq m$, $|b_{i+1}| \leq m$, and $\mathrm{ord}_{q_{i+1}}(z) > m + a > m$, it follows that $|y_{i+1}| \leq 1$. This proves (8).

Recall that r is the smallest integer such that $b_r = m$ and that $b_i < m$ for $i < r$. Suppose $r > 0$. Then $b_{r-1} < m$. By (8), we have $b_r = b_{r-1} + y_r \mathrm{ord}_{q_r}(z)$. Since $b_r = m > b_{r-1}$, this implies $y_r = 1$. As $\mathrm{ord}_{q_r}(z) > m + a$, we conclude $b_{r-1} = b_r - \mathrm{ord}_{q_r}(z) = m - \mathrm{ord}_{q_r}(z) < -a$.

Next, we claim that $b_0 = b_1 = \cdots = b_{r-1}$. We proof this by induction. First recall that $|b_i| \leq m$ for all $i = 0, \ldots, s$ and $\mathrm{ord}_{q_i}(z) > m + a$ for $i = 1, \ldots, s$. Suppose $b_j = b_{j+1} = \cdots = b_{r-1}$ for some j with $1 \leq j \leq r-1$. Then $b_j < -a$, as $b_{r-1} < -a$. We have $b_j = b_{j-1} + y_j \mathrm{ord}_{q_j}(z)$ by (8). If $y_j = 1$, then $b_j \geq -m + \mathrm{ord}_{q_j}(z) > -m + (m + a) > a$, contradicting $b_j < -a$. Now suppose $y_j = -1$. Recall that $b_{r-1} = b_r - \mathrm{ord}_{q_r}(z) = m - \mathrm{ord}_{q_r}(z)$. Hence

$$b_{j-1} = b_j - y_j \mathrm{ord}_{q_j}(z) = b_{r-1} + \mathrm{ord}_{q_j}(z) = m - \mathrm{ord}_{q_r}(z) + \mathrm{ord}_{q_j}(z).$$

As $j < r$, we have $\mathrm{ord}_{q_j}(z) \geq \mathrm{ord}_{q_r}(z)$ by (7). Hence $b_{j-1} \geq m$ and thus $b_{j-1} = m$. Thus $\rho_{j-1}(X)$ is trivial. As $j - 1 < r$, this contradicts the definition of r. Therefore, $y_j = 0$ and $b_{j-1} = b_j$. This completes the proof for the claim that $b_0 = b_1 = \cdots = b_{r-1}$.

Finally, we conclude that $b_0 = b_{r-1} < -a$, which contradicts the assumption on b_0. Thus we have shown that $r > 0$ is impossible. Hence $r = 0$, which implies that X is trivial, a contradiction.

□

Theorem 3.4 *Let G be a finite abelian group and let m, z be positive integers with $(|G|, z) = 1$. Let $X \in \mathbb{Z}[G]$ be a solution of $XX^{(-1)} = m^2$ with $|X| = m$, and suppose that $X^{(z)} = X$. Furthermore, suppose that $\mathrm{ord}_q(z) \geq 2m - 1$ for all prime divisors q of $|G|$. Then at least one of the following holds.*

(*i*) *X is trivial.*

(*ii*) *$4m - 1$ is a prime dividing $|G|$ and $\mathrm{ord}_{4m-1}(z) = 2m - 1$.*

Proof As before, we assume that X is nontrivial and denote the coefficient of the identity in X by b_0. As argued before, we have $|b_0| \leq m - 1$.

Suppose $b_0 \geq -(m-2)$. Then we can apply Theorem 3.3 with $a = m-2$, which shows that X is trivial. Hence we can assume $b_0 = -m+1$.

Using the assumption $X^{(z)} = X$, we can write

$$X = -m + 1 + \sum a_i T_i$$

with $a_i \in \mathbb{Z}$, where the T_i's are orbits of $x \mapsto x^z$ on $G \setminus \{1\}$. Note that $|T_i| \geq 2m-1$ for all i by Lemma 2.1, since $\mathrm{ord}_q(z) \geq 2m-1$ for all prime divisors q of $|G|$ by assumption.

Recall that the sum of the squares of the coefficients of X is m^2, since $XX^{(-1)} = m^2$. Hence $m^2 = (m-1)^2 + \sum |T_i| a_i^2 \geq (m-1)^2 + (2m-1)\sum a_i^2$, which implies $a_i = \pm 1$ for one i, $a_j = 0$ for all $j \neq i$, and $|T_i| = 2m-1$. Hence $X = -m + 1 + a_i T_i$ with $a_i = \pm 1$. Since $|X| = m$ and $|T_i| = 2m-1$, we have $m = |X| = -m + 1 + a_i(2m-1)$, i.e., $a_i = 1$. In summary, we have shown

$$X = -m + 1 + T,$$

where $T = T_i$ is an orbit of size $2m-1$ of $x \mapsto x^z$ on G. Let $H = \{1\} \cup T \cup T^{(-1)}$. We will show that H is a subgroup of G and that $|H| = 4m-1$ is a prime.

Note that $H = H^{(-1)}$. Moreover, $H = H^{(z)}$ since $T^{(z)} = T$. It is straightforward to check that $XX^{(-1)} = m^2$ implies $\mathrm{supp}(TT^{(-1)}) \subset H$. As T is an orbit of $x \mapsto x^z$ on G, we can write $T = \sum_{i=0}^{f-1} k^{z^i}$ for some $k \in G$ and some integer f. Let $i, j \in \{0, ..., f-1\}$, $i \neq j$, be arbitrary. Note that $k^{z^i} \neq k^{z^j}$. Since $\mathrm{supp}(TT^{(-1)}) \subset H$, we have $k^{z^i - z^j} = k^{\pm z^c}$ for some positive integer c. Hence

$$(k^{z^i + z^j})^{\pm z^c} = (k^{z^i + z^j})^{z^i - z^j} = k^{z^{2i} - z^{2j}} \in H.$$

Since $H = H^{(z)}$, this implies $k^{z^i + z^j} \in H$.

So far we have shown $H = H^{(-1)}$ and that $x, y \in H$, $x \neq y$, implies $xy \in H$. Now let $x \in H$, $x \neq 1$, be arbitrary, say $x = k^{\pm z^i}$. Choose j such that $k^{z^j} \neq x$. Then, by what we have shown, $y := k^{\pm z^i + z^j} \in H$ and $y_1 := k^{\pm z^i - z^j} \in H$. Hence $x^2 = y y_1 \in H$. We have thus shown that H is a group. The order of H is $1 + 2|T| = 1 + 2(2m-1) = 4m-1$. Let q be a prime divisor of $4m-1$. If $q \neq 4m-1$, then $q < 2m-1$. Hence

$\mathrm{ord}_q(z) < q < 2m-1$. But q divides $|G|$ since H is a subgroup of G. This contradicts the assumption $\mathrm{ord}_q(z) \geq 2m-1$. Hence $4m-1$ is a prime and $\mathrm{ord}_{4m-1}(z) = |T| = 2m-1$. □

Proof of Theorem 3.2

First we deal with the case $m = 1$. In this case, $XX^{(-1)} = 1$ and thus the sum of the squares of the coefficients of X is 1. Hence $X = \pm g$ for some $g \in G$, i.e., X is trivial.

Now let $m \geq 2$ and suppose that X is nontrivial. As in the proof of [9, Thm. 3, p. 36], we proceed by induction on the number of distinct prime divisors of m.

Let p be a prime factor of m, and let p^e be the highest power of p dividing m. Note that p does not divide $|G|$ as p is a prime factor of $M(m)$. First, we claim that we may assume $X^{(p)} = X$.

Write $F = X^{(-1)}X^{(p)}$. Note that $XX^{(-1)} = m^2 \equiv 0 \pmod{p^{2e}}$. Hence $F \equiv 0 \pmod{p^{2e}}$ by Corollary 2.4 (with $\alpha = 0$, $w = p^{2e}$, $z = p$). Thus $E := F/p^{2e} \in \mathbb{Z}[G]$ satisfies $EE^{(-1)} = m^4/p^{4e}$.

To apply the inductive argument, we need to show that $M(m^2/p^{2e})$ divides $M(m)$. First of all, $M(m)$ is divisible by $M(m, 2m-2)$ by the definition of $M(m)$. Furthermore, again by definition, $M(m, 2m-2)$ is divisible by $M(m^2/p^{2e}, 2m^2/p^{2e} - 2)$. Since $4m^2/p^{2e} - 1 = (2m/p^e - 1)(2m/p^e + 1)$ is not a prime, we have $M(m^2/p^{2e}, 2m^2/p^{2e} - 2) = M(m^2/p^{2e})$ by Definition 3.1. Therefore, $M(m^2/p^{2e})$ divides $M(m)$.

Note that the number of distinct prime factors of m^2/p^{2e} is less than that of m. Recall that, by assumption, $|G|$ is coprime to $M(m)$. Since $M(m^2/p^{2e})$ divides $M(m)$, we have $(|G|, M(m^2/p^{2e})) = 1$. Hence E is trivial by induction.

As E as trivial, it is divisible by m^2/p^{2e}. Thus $X^{(-1)}X^{(p)} = F = p^{2e}E$ is divisible by m^2. This implies $X^{(p)} = Xg$ for some $g \in G$ by Result 2.5 (a). Note that, by definition, $M(m)$ is divisible by all prime divisors of $p-1$. Hence $(p-1, |G|) = 1$, since $(|G|, M(m)) = 1$ by assumption. Thus there is

$g_1 \in G$ with $g_1^{p-1} = g^{-1}$. We have

$$(Xg_1)^{(p)} = Xgg_1^p = (Xg_1)(gg_1^{p-1}) = Xg_1.$$

Hence, replacing X by Xg_1, if necessary, we can assume $X^{(p)} = X$.

We are going to complete the proof by applying Theorem 3.4 to X. Let q be any prime divisor of $|G|$. Then $q \neq p$, since m divides $M(m)$ by definition. Moreover, q does not divide any of the numbers $p-1, p^2-1, ..., p^{2m-2}-1$ by the assumption $(|G|, M(m)) = 1$ and the definition of $M(m)$. Hence $\mathrm{ord}_q(p) \geq 2m-1$ for every prime divisor q of $|G|$, which means that the assumptions of Theorem 3.4 are satisfied.

Recall that we assume that X is nontrivial. Hence $4m-1$ is a prime dividing $|G|$ by Theorem 3.4. But then $4m-1$ divides $M(m)$ by definition, contradicting the assumption $(|G|, M(m)) = 1$. □

4 Proof of Theorem 1.4

Our argument is similar to the proof of [9, Thm. 6, p. 68]. Let

$$F = D^{(t)}D^{(-1)} - \lambda G. \tag{12}$$

A straightforward computation using (1) shows that $FF^{(-1)} = n^2$. By Result 2.5 (b), to prove that t is a multiplier of D, it is sufficient to show that F is trivial.

We proceed as before. Recall that, by the assumptions of Theorem 1.4, for every prime divisor u of n_1, there is an integer f_u with

$$t \equiv u^{f_u} \pmod{v^*}. \tag{13}$$

Furthermore,

$$DD^{(-1)} - \lambda G = n \equiv 0 \pmod{n_1} \tag{14}$$

by (1). Hence, from (12), (13), (14), and using Corollary 2.4 (with $w = n_1$ and $\alpha = -\lambda$), we conclude $F \equiv 0 \pmod{n_1}$. Hence $E := F/n_1$ is in $\mathbb{Z}[G]$. Note that $EE^{(-1)} = n^2/n_1^2$.

Let p be a prime divisor of n/n_1 and p^e be the largest power of p dividing n/n_1. Write $E_1 = E^{(-1)}E^{(p)}$. Then

$$E_1E_1^{(-1)} = EE^{(-1)}\left(EE^{(-1)}\right)^{(p)} = \frac{n^4}{n_1^4}. \tag{15}$$

We will apply Theorem 3.2 to show that E_1 is trivial. Note that

$$EE^{(-1)} = \frac{n^2}{n_1^2} \equiv 0 \pmod{p^{2e}}. \tag{16}$$

Hence $E_1 = E^{(-1)}E^{(p)} \equiv 0 \pmod{p^{2e}}$ by Corollary 2.4 (with $\alpha = 0$ and $z = p$). Thus $E_2 := E_1/p^{2e}$ is in $\mathbb{Z}[G]$. By (15), we have

$$E_2E_2^{(-1)} = \frac{n^4}{n_1^4p^{4e}}. \tag{17}$$

To apply Theorem 3.2, we need to show that $M(n^2/(n_1^2p^{2e}))$ divides $M(n/n_1, \lfloor k/n_1 \rfloor)$. Note that, by definition, $M(n^2/(n_1^2p^{2e}), 2n^2/(n_1^2p^{2e}) - 2)$ divides $M(n/n_1, \lfloor k/n_1 \rfloor)$. Furthermore,

$$M(n^2/(n_1^2p^{2e})) = M(n^2/(n_1^2p^{2e}), 2n^2/(n_1^2p^{2e}) - 2),$$

since $4n^2/(n_1^2p^{2e}) - 1$ is not a prime. Hence $M(n/n_1, \lfloor k/n_1 \rfloor)$ is divisible by $M(n^2/(n_1^2p^{2e}))$.

We have $(v, M(n/n_1, \lfloor k/n_1 \rfloor)) = 1$ by assumption and therefore v and $M(n^2/(n_1^2p^{2e}))$ are coprime. Thus E_2 is trivial by (17) and Theorem 3.2. Hence $E_1 = E^{(-1)}E^{(p)}$ is trivial, too. By applying a similar argument as in the proof of Theorem 3.2, we may assume $E = E^{(p)}$.

Suppose that E is nontrivial. Let a_0 and b_0 be the coefficients of the identity in F, respectively E. Note that $b_0 = a_0/n_1$. Recall that $F = D^{(-1)}D^{(t)} - \lambda G$. Hence $a_0 = |D \cap D^{(t)}| - \lambda \geq -\lambda$. Furthermore, as we assume that E is nontrivial, we have $|b_0| < n/n_1$. Hence

$$-\frac{\lambda}{n_1} \leq b_0 < \frac{n}{n_1}. \tag{18}$$

Let q be a prime divisor of v. Then $\mathrm{ord}_q(p) > k/n_1$, since q does not divide any of the numbers $p - 1$, $p^2 - 1$,$\ldots$,$p^{\lfloor k/n_1 \rfloor} - 1$ by the assumption

$(|G|, M(n/n_1, \lfloor k/n_1 \rfloor)) = 1$ and the definition of $M(n/n_1, \lfloor k/n_1 \rfloor)$. Set $a = \lambda/n_1$. Then $b_0 \geq -a$ by (18) and $\mathrm{ord}_q(p) > k/n_1 = n/n_1 + \lambda/n_1 = n/n_1 + a$ for all prime divisors q of $|G|$. Thus we can apply Theorem 3.3 with $m = n/n_1$ and $a = \lambda/n_1$ and conclude that E is trivial, a contradiction. Hence E and thus F is trivial and this completes the proof of Theorem 1.4. □

Corollary 4.1 *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 $t \equiv u^{f_u} \pmod{v^*}$. If v and $M(n/n_1)$ are coprime, then t is a multiplier of D.*

Proof Define E as in the proof of Theorem 1.4. Then E is trivial by Theorem 3.4, since $EE^{(-1)} = n^2/n_1^2$ and $(v, M(n/n_1)) = 1$ by assumption. Hence the same argument as in the proof of Theorem 1.4 shows that t is a multiplier of D. □

5 Examples

McFarland [9] defined his M-function as follows. Let m be a positive integer. For $m \leq 4$, define $M'(m)$ by

$$M'(1) = 1, \quad M'(2) = 2 \cdot 7, \quad M'(3) = 2 \cdot 3 \cdot 11 \cdot 13, \quad M'(4) = 2 \cdot 3 \cdot 7 \cdot 31.$$

For $m \geq 5$, let p be a prime factor of m, and define $M'(m)$ as the product of the distinct prime factors of

$$m, M'(m^2/p^{2e}), p-1, p^2-1, ..., p^u-1,$$

where p^e is the highest power of p dividing m, and $u = (m^2 - m)/2$. Note that $M'(m)$ is not uniquely defined in general, as it depends on the order in which prime divisors of m are chosen for the recursion.

Example 5.1 Corollary 4.1, and all the more Theorem 1.4, strengthen McFarland's Result 1.3 substantially, since (for $m \geq 5$) $M(m)$ is much smaller than $M'(m)$. For instance, we have

$M'(5) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 71 \cdot 313 \cdot 521 \cdot 829 \cdot 19531,$
$M'(6) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 31 \cdot 41 \cdot 61 \cdot 73 \cdot 547 \cdot 757 \cdot 1093 \cdot 3851 \cdot 4561 \cdot 797161,$
$M'(7) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 113 \cdot 181 \cdot 191 \cdot 281 \cdot 419 \cdot$
$911 \cdot 1063 \cdot 1123 \cdot 1201 \cdot 2801 \cdot 4021 \cdot 4733 \cdot 14009 \cdot 117307 \cdot 159871 \cdot 169553 \cdot$
$293459 \cdot 2767631689 \cdot 11898664849 \cdot 16148168401 \cdot 4534166740403,$
and
$M(5) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 71 \cdot 313 \cdot 19531,$
$M(6) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 31 \cdot 41 \cdot 61 \cdot 757 \cdot 1093,$
$M(7) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 29 \cdot 37 \cdot 43 \cdot 181 \cdot 191 \cdot 1063 \cdot 1123 \cdot 1201 \cdot 2801 \cdot 4733 \cdot 293459.$

Of course, for larger values of m, the difference in order of magnitude between $M(m)$ and $M'(m)$ becomes much more significant.

Example 5.2 To demonstrate that $M(m)$ can take different values depending on the order in which the prime divisors of m are chosen in the recursion, we compute $M(6)$ in the two possible ways. Note that $4 \cdot 6 - 1 = 23$ is a prime. Hence 23 divides $M(6)$.

First we choose $p = 3$ as the first prime divisor of 6. Then, by definition, $M(4, 6) = M(6)$ is the product of the distinct prime divisors of $6, 23, M(4), 3 - 1, 3^2 - 2, \ldots, 3^{10} - 1$. Moreover, $M(4)$ is the product of the distinct prime divisors of $2, 2^2 - 1, 2^3 - 1, \ldots, 2^6 - 1$. This gives $M_1 := 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 31 \cdot 41 \cdot 61 \cdot 757 \cdot 1093$ for $M(6)$, which is the number given in Example 5.1.

Now let us choose $p = 2$ as the first prime divisor of 6. Then $M(6)$ is the product of the distinct prime divisors of $6, 23, M(9), 2 - 1, 2^2 - 2, \ldots, 2^{10} - 1$. Moreover, $M(9, 16) = M(9)$ is the product of the distinct prime divisors of $3, 3 - 1, 3^2 - 1, \ldots, 3^{16} - 1$. This gives $M_2 := 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 127 \cdot 193 \cdot 547 \cdot 757 \cdot 1093 \cdot 1871 \cdot 3851 \cdot 4561 \cdot 34511 \cdot 797161$ for $M(6)$.

In this case, the first way of choosing the order of the prime divisors of m is "optimal" since M_1 divides M_2. However, in general, there is no optimal way to choose the order of the prime divisors of m. Hence we need to allow the ambiguity of $M(m)$ and $M(m, b)$ in order to keep the full strength of our

multiplier theorem. The same phenomenon was observed by McFarland [9] concerning his version of the M-function.

Example 5.3 A good test case for multiplier results is the parameters of known cyclic Paley-Hadamard difference sets. Such difference sets have parameters $(v, k, \lambda, n) = (p, (p-1)/2, (p-3)/4, (p+1)/4)$ where $p \equiv 3 \pmod 4$ is a prime, and they are known to exist for every prime $p \equiv 3 \pmod 4$, see [2].

There are 39322 primes $p \equiv 3 \pmod 4$ with $7 \leq p < 10^6$.

- The Second Multiplier Theorem implies the validity of the multiplier conjecture for Paley-Hadamard parameters for 23125 of these primes.
- The Second Multiplier Theorem together with Hall's result on 6th power difference sets [6] implies the validity of the multiplier conjecture for 6587 of the remaining 16197 cases.
- McFarland's result 1.3 implies the validity of the multiplier conjecture for 5068 of the remaining 9610 cases.
- Thus, prior to the results of this paper, there were 4542 open cases for of the multiplier conjecture for Paley-Hadamard parameters in this range. Theorem 1.4 implies the validity of the multiplier conjecture for 3034 of these cases. There are 1508 cases in this range which remain unresolved.

The computational details of the search described in this example are available in electronic form upon request.

Example 5.4 A list of open cases for the existence of cyclic difference sets can be found under [4]. Our multiplier theorem can be used to rule out some of these cases: Difference sets D with the following parameters do not exist.

v	k	λ	n
419	133	42	91
1123	154	21	133
1381	276	55	221

Proof For $v = 419$, we take $t = n_1 = 13$ in Corollary 4.1. Note that v and $M(n/n_1) = M(7)$ are coprime. Hence 13 is a multiplier of D. A quick computer search based on this fact rules out this difference set. Note that Result 1.3 does not imply that 13 is a multiplier as $M'(7)$ is divisible by 419.

For $v = 1123$, we take $t = n_1 = 19$ in Theorem 1.4. As $\mathrm{ord}_v(7) = 11 > k/n_1 = 154/19$, we conclude that $M(n/n_1, \lfloor k/n_1 \rfloor)$ is not divisible by v. Hence 19 is a multiplier of D. As $\mathrm{ord}_v(19) = 561$, Result 2.7 rules out this difference set.

For $v = 1381$, take $t = n_1 = 17$, in Theorem 1.4. As $\mathrm{ord}_v(13) = 23 > k/n_1 = 276/17$, we conclude that 17 is a multiplier of D. As $\mathrm{ord}_v(17) = 84$, Result 2.7 rules out this difference set. □

Example 5.5 Theorem 1.4 often can be used to show that known difference with certain parameters are unique. Here is an example of twin prime difference sets: Up to equivalence, there is a unique difference set D with parameters $(v, k, \lambda, n) = (213443, 106721, 53360, 53361)$.

Proof A difference set with these parameters exists as $v = 461 \cdot 463$, and 461 and 463 are primes, see [2]. Note that $n = 3^2 \cdot 7^2 \cdot 11^2$ and $11 \equiv 3^{31459} \pmod{v}$. Hence we can take $t = 3$ and $n_1 = 3^2 \cdot 11^2$ in Corollary 4.1. Since $\mathrm{ord}_{461}(7) = 460$, $\mathrm{ord}_{463}(7) = 154$ and $154 > 2 \cdot 49 - 2$ we infer that $M(n/n_1) = M(49)$ is coprime to v. Hence 3 is a multiplier of D by Corollary 4.1, and we can assume $D = D^{(3)}$. Note that $x \mapsto x^3$ has exactly 5 orbits on the cyclic group of order v of size 106260, 106260, 460, 462, 1, respectively. As $k - 106260 = 461$, we conclude that D consists of one orbit of size 106260, and the orbits of size 460 and 1. As there is an automorphism of the cyclic group of order v, which maps the two orbits of size 106260 to each other and fixes the orbits of size 460 and 1, respectively, we conclude that D is unique up to equivalence.

We note that Result 1.3 does not imply that 3 is a multiplier of D, since both 461 and 463 divide $M'(49)$.

Acknowledgements We thank the anonymous referees for useful suggestions concerning the exposition of the paper. The third author is grateful to

Dieter Jungnickel for his hospitality during a visit at the Universität Augsburg, during which part of this research was done.

Ka Hin Leung's and Siu Lun Ma's research is supported by grant No. R-146-000-158-112, Ministry of Education, Singapore.

References

[1] K. T. Arasu, Q. Xiang: Qing Multiplier theorems. *J. Combin. Des.* **3** (1995), 257–268.

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

[3] T. Feng: Difference sets with $n = 5p^r$. *Des. Codes Cryptogr.* **51** (2009), 175–194.

[4] D. Gordon: *La Jolla Difference Set Repository.* `http://www.ccrwest.org/diffsets/diff_sets/index.html`.

[5] M. Hall: Cyclic projective planes. *Duke Math. J.* **14** (1947), 1079–1090.

[6] M. Hall: A survey of difference sets. *Proc. Amer. Math. Soc.* **7** (1956) 975–986.

[7] M. Hall, H. J. Ryser: Cyclic incidence matrices. *Canad. J. Math.* **3** (1951), 495–502.

[8] K. Ireland, M. I. Rosen: *A Classical Introduction to Modern Number Theory* (2nd edition). Springer 1990.

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

[10] R. L. McFarland, H. B. Mann: On multipliers of difference sets. *Canad. J. Math.* **17** (1965), 541–542.

[11] K. P. Menon: Difference sets in Abelian groups. *Proc. Amer. Math. Soc.* **11** (1960), 368–376.

[12] M. Muzychuk: Difference Sets with $n = 2p^m$. *J. Alg. Combin.* **7** (1999), 77–89.

[13] W. S. Qiu: The multiplier conjecture for elementary abelian groups. *J. Combin. Des.* **2** (1994), 117–129.

[14] W. S. Qiu: A method of studying the multiplier conjecture and some partial solutions for it. *Ars Combin.* **39** (1995), 5–23.

[15] W. S. Qiu: The multiplier conjecture for the case $n = 4n_1$. *J. Combin. Des.* **3** (1995), 393–397.