A Survey of the Multiplier Conjecture

Daniel M. Gordon
IDA Center for Communications Research
4320 Westerra Court
San Diego, CA 92121
USA

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

September 30, 2015

Abstract

We review the current status of the multiplier conjecture for difference sets, present some new results on it, and determine the open cases of the conjecture for abelian groups of order $< 10^6$. It turns out that for Paley parameters $(4n-1, 2n-1, n-1, n)$, where $4n-1$ is a prime power, the validity of the multiplier conjecture can be verified in the vast majority of cases, while for other parameter sets numerous cases remain open.

Keywords: Difference sets, multiplier theorems, group ring equations, cyclotomic fields

Mathematics Subject Classification: 05B10

1 Introduction

A (v, k, λ, n) **difference set** in an abelian 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 $d_1, d_2 \in D$. By replacing D by $G \setminus D$ if necessary, we may assume $1 < k < v/2$. The positive integer $n = k - \lambda$ is called the **order** of the difference set.

One of the most fruitful approaches to the study of difference sets is the concept of multipliers due to Hall [5]. An integer t is a **multiplier** of D if $\{d^t : d \in D\} = \{dg : d \in G\}$ for some $g \in G$. Note that we only consider abelian groups here.

Hall [5] proved that every prime divisor of the order of a difference set with $\lambda = 1$ is a multiplier of the difference set. Later Hall and Ryser [7] generalized this result and obtained what is now called the First Multiplier Theorem.

Result 1.1 (First Multiplier Theorem). *Let D be a (v, k, λ, n) difference set in an abelian group. Let p be a prime which divides n, but not v. If $p > \lambda$, then p is a multiplier of D.*

The following conjecture, by now a classical unsolved problem, originated from [7].

Conjecture 1.2 (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.*

In [6], Hall substantially strengthened the results of [5, 7]. Hall's work in [6] was slightly generalized by Menon [15] to what is now known as the Second Multiplier Theorem.

Result 1.3 (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 much more powerful approach to the multiplier conjecture was developed by McFarland [12] in 1970. To formulate his striking result, we need the following definition. 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 $M'(m)$ to be 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. But the following result holds in any case, no matter what order of the prime divisors of m is chosen.

Result 1.4 (McFarland [12, 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 [17, 18, 19], Muzychuk [16], and Feng [21] improved Result 1.4 for certain values of n/n_1, e.g., $n/n_1 \in \{2, 3, 4, 5\}$. Beyond that there had not been significant progress towards the multiplier conjecture since McFarland's work until the work of Leung, Ma, and Schmidt [11] in 2014.

In Theorem 3.1 in Section 3, we present a generalization of the result in [11]. In fact, Theorem 3.1 contains all previous multiplier theorems for difference sets as special cases. In Section 4, we present a new result which settles some of the cases of the multiplier conjecture which are left open by Theorem 3.1. The main idea behind this result is to use the putative nonexistence of multipliers to construct certain "difference systems". If, in turn, these difference systems can be shown to nonexistent, then new multipliers are obtained.

Finally, in Section 5 we give results of computations for difference set parameters with $v < 10^6$, detailing how often known results are sufficient to imply the multiplier conjecture.

2 Preliminaries

2.1 Number Theoretic Background

Let $\zeta_m = \exp(2\pi i/m)$ be a primitive mth root of unity. The minimum polynomial of ζ_m over $\mathbb{Q}$ is the cyclotomic polynomial

$$\Phi_m = \prod_{\substack{i=1 \\ (i,m)=1}}^{m} (x - \zeta_m^i).$$

The degree of the field extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is $\varphi(m)$, where φ denotes the Euler totient function. Thus every element of $\mathbb{Q}(\zeta_m)$ has a unique representation as

$$\sum_{i=0}^{\varphi(m)-1} a_i \zeta_m^i$$

with $a_i \in \mathbb{Q}$.

For an integer d with $(d, m) = 1$, an automorphism σ_d of $\mathbb{Q}(\zeta_m)$ is defined by

$$\left(\sum_{i=0}^{\varphi(m)-1} a_i \zeta_m^i \right)^{\sigma_d} = \sum_{i=0}^{\varphi(m)-1} a_i \zeta_m^{di}.$$

The extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is a Galois extension with Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \{\sigma_d : 1 \le d \le m,\ (d, m) = 1\}.$$

The norm of $x \in \mathbb{Q}(\zeta_m)$ is

$$\mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(x) = \prod_{\substack{d=1 \\ (d,m)=1}}^{m} x^{\sigma_d}.$$

The elements of the ring

$$\mathbb{Z}[\zeta_m] = \left\{ \sum_{i=0}^{m-1} b_i \zeta_m^i : b_i \in \mathbb{Z} \right\}$$

are called **cyclotomic integers**. It is easy to see that $\mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(x)$ is a nonzero integer for every $x \in \mathbb{Z}[\zeta_m]$, $x \neq 0$.

A **prime ideal** of $\mathbb{Z}[\zeta_m]$ is an ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_m]$ with the following property. If $ab \in \mathfrak{p}$ for any $a, b \in \mathbb{Z}[\zeta_m]$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. A **proper** ideal of $\mathbb{Z}[\zeta_m]$ is an ideal which is different from $\mathbb{Z}[\zeta_m]$. A **maximal ideal** of $\mathbb{Z}[\zeta_m]$ is a proper ideal which is not properly contained in any proper ideal of $\mathbb{Z}[\zeta_m]$. It is a standard result that a nonzero ideal of $\mathbb{Z}[\zeta_m]$ is maximal if and only if it is prime.

Every proper nonzero ideal I of $\mathbb{Z}[\zeta_m]$ can be uniquely factorized into a product of finitely many prime ideals, i.e., we have $I = \prod_{i=1}^{t} \mathfrak{p}_i$ for some positive integer t, where the $\mathfrak{p}_i$'s are (not necessarily distinct) prime ideals of $\mathbb{Z}[\zeta_m]$ and the multiset $\{\mathfrak{p}_i : i = 1, \ldots, t\}$ (and thus t) is uniquely determined by I. The principal ideal of $\mathbb{Z}[\zeta_m]$ generated by $a \in \mathbb{Z}[\zeta_m]$ is denoted by $a\mathbb{Z}[\zeta_m]$. Note that a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_m]$ occurs in the prime ideal factorization of $a\mathbb{Z}[\zeta_m]$ if and only if $a \in \mathfrak{p}$. For a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_m]$, let $\nu_{\mathfrak{p}}(a)$ denote the number of factors equal to $\mathfrak{p}$ in the prime ideal factorization of $a\mathbb{Z}[\zeta_m]$. We write $a \equiv 0 \pmod{b}$ for $a, b \in \mathbb{Z}[\zeta_m]$ if $a = bc$ for some $c \in \mathbb{Z}[\zeta_m]$. Due to the unique prime ideal factorization, we have the following fact.

Result 2.1. *Let $a, b \in \mathbb{Z}[\zeta_m]$, $a, b \neq 0$. We have $a \equiv 0 \pmod{b}$ if and only if $\nu_{\mathfrak{p}}(a) \geq \nu_{\mathfrak{p}}(b)$ for all prime ideals $\mathfrak{p}$ with $b \in \mathfrak{p}$.*

The following well known result is the fundamental number theoretic fact behind all multiplier theorems. Because of its importance for this paper, we give a complete proof.

Result 2.2. *Let p be a prime number and let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta_m]$ with $p \in \mathfrak{p}$. Write $m = p^a m'$ with $(m', p) = 1$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. If*

$$(\zeta_{m'})^\sigma = \zeta_{m'}^{p^j}. \tag{1}$$

for some positive integer j, then $\mathfrak{p}^\sigma = \mathfrak{p}$.

Proof. First, we claim that

$$(\zeta_{p^a}^i)^\tau \equiv 1 \pmod{\mathfrak{p}} \tag{2}$$

for all nonnegative integers i and all $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. If $a = 0$, then $\zeta_{p^a} = 1$ and (2) holds. Thus let $a > 0$. Using the fact that $1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$, it is straightforward to check that

$$\prod_{\substack{i=1 \\ (i,p)=1}}^{p^a-1} (x - \zeta_{p^a}^i) = \sum_{j=0}^{p-1} x^{jp^{a-1}}.$$

Setting $x = 1$, we get

$$\prod_{\substack{i=1 \\ (i,p)=1}}^{p^a-1} (1 - \zeta_{p^a}^i) = p. \tag{3}$$

Note that $(1-\zeta_{p^a}^i)/(1-\zeta_{p^a}) = 1+\zeta_{p^a}+\cdots+\zeta_{p^a}^{i-1}$. Moreover, if $(i, p) = 1$, then there is j with $\zeta_{p^a} = \zeta_{p^a}^{ij}$, and we have $(1-\zeta_{p^a})/(1-\zeta_{p^a}^i) = 1+\zeta_{p^a}^i+\cdots+\zeta_{p^a}^{i(j-1)}$. This shows that $(1 - \zeta_{p^a}^i)/(1 - \zeta_{p^a})$ is a unit in $\mathbb{Z}[\zeta_m]$ whenever $(i, p) = 1$. Hence (3) implies

$$(1 - \zeta_{p^a})^{p^{a-1}(p-1)}\mathbb{Z}[\zeta_m] = p\mathbb{Z}[\zeta_m]. \tag{4}$$

Due to unique prime ideal factorization, (4) implies $1 - \zeta_{p^a} \in \mathfrak{p}$. As $1 - \zeta_{p^a}^i = (1 + \zeta_{p^a} + \cdots + \zeta_{p^a}^{i-1})(1 - \zeta_{p^a})$, we conclude $1 - \zeta_{p^a}^i \in \mathfrak{p}$ for all $i > 0$. This implies (2).

Let A be any element of $\mathbb{Z}[\zeta_m]$ and write $A = \sum_{i=0}^{p^a-1} \zeta_{p^a}^i f_i(\zeta_{m'})$ with $f_i \in \mathbb{Z}[x]$. By the multinomial theorem, we have

$$\sum_{i=0}^{p^a-1} f_i(\zeta_{m'}^{p^j}) \equiv \left(\sum_{i=0}^{p^a-1} f_i(\zeta_{m'})\right)^{p^j} \pmod{p}.$$

As $p \in \mathfrak{p}$, this congruence also holds modulo $\mathfrak{p}$. Suppose $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ satisfies (1). Using (2) and the congruence we just derived, we conclude

$$\begin{aligned} A^\sigma &= \sum_{i=0}^{p^a-1} (\zeta_{p^a}^i)^\sigma f_i(\zeta_{m'}^{p^j}) \\ &\equiv \sum_{i=0}^{p^a-1} f_i(\zeta_{m'}^{p^j}) \\ &\equiv \left(\sum_{i=0}^{p^a-1} f_i(\zeta_{m'})\right)^{p^j} \\ &\equiv \left(\sum_{i=0}^{p^a-1} \zeta_{p^a}^i f_i(\zeta_{m'})\right)^{p^j} \\ &\equiv A^{p^j} \pmod{\mathfrak{p}}. \end{aligned}$$

Note that $A \in \mathfrak{p}$ implies $A^{p^j} \in \mathfrak{p}$, as $\mathfrak{p}$ is an ideal. We just have shown $A^\sigma \equiv A^{p^j} \pmod{\mathfrak{p}}$. Hence $A \in \mathfrak{p}$ implies $A^\sigma \in \mathfrak{p}$. This shows $\mathfrak{p}^\sigma \subset \mathfrak{p}$. But $\mathfrak{p}^\sigma$ is a prime ideal and thus maximal. So we have $\mathfrak{p}^\sigma = \mathfrak{p}$. □

Let p be a prime, let m be a positive integer, and write $m = p^a m'$ with $(p, m') = 1$, $a \geq 0$. If there is an integer j with $p^j \equiv -1 \pmod{m'}$, then p is called **self-conjugate modulo m**. A composite integer n is called self-conjugate modulo m if every prime divisor of n is self-conjugate modulo m. The following is a result of Turyn [22].

Result 2.3. *Suppose that $A \in \mathbb{Z}[\zeta_m]$ satisfies*

$$|A|^2 \equiv 0 \bmod n^2$$

for some positive integer n which is self-conjugate modulo m. Then $A \equiv 0 \bmod n$.

2.2 Group Rings and Characters

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 characters 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 $X^{(t)} = \sum a_g g^t$. Let 1 denote the identity element of G. For $a \in \mathbb{Z}$ we simply write a for the group ring element $a \cdot 1$. For $S \subset G$, we write S instead of $\sum_{g \in S} g$.

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

$$DD^{(-1)} = n + \lambda G \tag{5}$$

in $\mathbb{Z}[G]$. Furthermore, (5) 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.

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

Result 2.4 (Fourier inversion formula)**.** *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 $g \in G$.

The next result is due to McFarland [12]. 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.*

(*c*) *Suppose $E \in \mathbb{Z}[G]$ satisfies $EE^{(-1)} = m^2$ for some positive integer m. If all coefficients of E are nonnegative, then $E = mg$ for some $g \in G$.*

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 $D^{(t)} = Dg$.

(c) Write $E = \sum_{g \in G} e_g g$ with $e_g \in \mathbb{Z}$, $e_g \geq 0$. As $EE^{(-1)} = m^2$, we have $|E|^2 = m^2$ and thus $\sum_{g \in G} e_g = |E| = m$ (note that $|E| = -m$ is impossible, since E has only nonnegative coefficients). Comparing the coefficient of the identity in $EE^{(-1)} = m^2$, we get $\sum_{g \in G} e_g^2 = m^2$. But $\sum_{g \in G} e_g = m$ and $\sum_{g \in G} e_g^2 = m^2$ imply that there is $g \in G$ with $e_g = m$ and $e_h = 0$ for all $h \in g$. Thus $E = mg$. $\square$

2.3 Group Ring Equations

The most powerful multiplier theorems are based on results on group ring equations of the form $XX^{(-1)} = m^2$, where $X \in \mathbb{Z}[G]$, G is an abelian group, and m is a positive integer. We call a solution X of $XX^{(-1)} = m^2$ **trivial** if it has the form $X = \pm gm$ for some $g \in G$.

For a proof of the following result, [11, Thm. 3.3].

Result 2.6. *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.

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

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

Furthermore, set

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

The following is [11, Thm. 3.2].

Result 2.7. *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.*

3 The Multiplier Theorem of Leung, Ma, and Schmidt

The strongest known multiplier theorem for difference sets is [11, Thm. 1.4]. It is an improvement of [12, Thm. 6, p. 68], which had been proved by McFarland no less than 44 years earlier. Theorem 3.1 below is a slight generalization of [11, Thm. 1.4] and, to our knowledge, contains all previous multiplier theorems for difference sets in abelian groups as special cases.

Theorem 3.1. *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 and suppose that t is an integer with $(v,t) = 1$ such that, for every prime divisor u of n_1,*

(i) there is a positive integer f_u with $t \equiv u^{f_u} \pmod{v^*}$ or

(ii) u is self-conjugate modulo v^*.

If $n_1/(v,n_1) > \lambda$ or

$$\left(v, M\left(\frac{n(v,n_1)}{n_1}, \left\lfloor \frac{k(v,n_1)}{n_1} \right\rfloor\right)\right) = 1, \tag{6}$$

then t is a multiplier of D.

Proof. The proof is based on that of [11, Thm. 1.4], but requires some additional arguments. For the convenience of the reader, we present the details here. Let

$$F = D^{(t)}D^{(-1)} - \lambda G. \tag{7}$$

A straightforward computation using (5) shows that

$$FF^{(-1)} = n^2. \tag{8}$$

By Result 2.5 (b), to prove that t is a multiplier of D, it is sufficient to show that F is trivial. First, we claim

$$\chi(F) \equiv 0 \pmod{n_1} \tag{9}$$

for all characters χ of G. Note that $k^2 = n + \lambda v$, as $DD^{(-1)} = n + \lambda G$. Hence, if χ is the trivial character, then $\chi(F) = k^2 - \lambda v = n$ and thus $\chi(F) \equiv 0 \pmod{n_1}$. Now suppose that χ is a nontrivial character of G. Then

$$\chi(D)\overline{\chi(D)} = n \tag{10}$$

by (5) and $\chi(F) = \chi(D^{(t)})\overline{\chi(D)}$ by the definition of F. Note that $\chi(D^{(t)}) = \chi(D)^{\sigma_t}$, where σ_t is the automorphism of $\mathbb{Q}(\zeta_{v^*})$ with $\zeta_m^{\sigma} = \zeta_m^t$. Hence

$$\chi(F) = \chi(D)^{\sigma_t}\ \overline{\chi(D)}. \tag{11}$$

Let u be any prime divisor of n_1 and let u^a be the largest power of u dividing n. We will show $\chi(F) \equiv 0 \pmod{u^a}$, which implies (9). First suppose that u is self-conjugate modulo v^*. Note that $|\chi(F)|^2 = n^2$ by (9). Thus $\chi(F) \equiv 0 \pmod{u^a}$ by Result 2.3.

Now suppose that u is not self-conjugate modulo v^*. Then, by assumption, there is a positive integer f_u with $t \equiv u^{f_u} \pmod{v^*}$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta_{v^*}]$ with $u \in \mathfrak{p}$. By (10), we have

$$\nu_{\mathfrak{p}}(\chi(D)) + \nu_{\mathfrak{p}}(\overline{\chi(D)}) = \nu_{\mathfrak{p}}(n) = \nu_{\mathfrak{p}}(u^a). \tag{12}$$

As $t \equiv u^{f_u} \pmod{v^*}$, we have $\mathfrak{p}^{\sigma_t} = \mathfrak{p}$ by Result 2.2. Thus

$$\nu_{\mathfrak{p}}\left(\chi(D)^{\sigma_t}\right) = \nu_{\mathfrak{p}^{\sigma_t}}\left(\chi(D)^{\sigma_t}\right) = \nu_{\mathfrak{p}}\left(\chi(D)\right).$$

Hence (11) and (12) imply

$$\nu_{\mathfrak{p}}(\chi(F)) = \nu_{\mathfrak{p}}(\chi(D)) + \nu_{\mathfrak{p}}(\overline{\chi(D)}) = \nu_{\mathfrak{p}}(u^a). \tag{13}$$

Since (13) holds for every prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_{v^*}]$ with $u \in \mathfrak{p}$, we have $\chi(F) \equiv 0 \pmod{u^a}$ by Result 2.1. This completes the proof of (9).

By (9) and Result 2.4, we have $vF \equiv 0 \pmod{n_1}$. This implies

$$F \equiv 0 \ \left(\bmod\ \frac{n_1}{(v, n_1)}\right). \tag{14}$$

Suppose that $n_1/(v, n_1) > \lambda$. Recall that $F = D^{(t)}D^{(-1)} - \lambda G$ and note that all coefficients $D^{(t)}D^{(-1)}$ are nonnegative. Moreover, F cannot have any coefficients lying in the interval $[-\lambda, -1]$ by (14). Hence all coefficients of F are nonnegative. Thus F is trivial by Result 2.6 (c). This shows that Theorem 3.1 holds if $n_1/(v, n_1) > \lambda$.

Now suppose that (6) holds. Set $N = n_1/(v, n_1)$. Then $E := F/N$ is an element of $\mathbb{Z}[G]$ by (14) and

$$EE^{(-1)} = \frac{n^2}{N^2}.$$

by (8).

Our aim is to show that E is trivial. If $n = N$, then $EE^{(-1)} = 1$ and thus $E = \pm g$ for some $g \in G$, i.e., E is trivial. Hence we may assume $n > N$. Let p be a prime divisor of n/N and let p^e be the largest power of p dividing n/N. Write $E_1 = E^{(-1)}E^{(p)}$. Then

$$E_1 E_1^{(-1)} = EE^{(-1)} \left(EE^{(-1)}\right)^{(p)} = \frac{n^4}{N^4}. \tag{15}$$

We will apply Theorem 2.7 to show that E_1 is trivial. Note that

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

Since p divides n/N and thus $M(n/N, \lfloor k/N \rfloor)$ by the definition of the M-function, we have $(p, v) = 1$ by (6). Furthermore, the automorphism of

$\mathbb{Q}(\zeta_{v^*})$ determined by $\zeta_{v^*} \to \zeta_{v^*}^p$ fixes every prime ideal of $\mathbb{Z}[\zeta_{v^*}]$ containing p by Result 2.2. Hence the same argument as for the proof of (14) shows that

$$E_1 = E^{(-1)}E^{(p)} \equiv 0 \pmod{p^{2e}}.$$

Thus $E_2 := E_1/p^{2e}$ is in $\mathbb{Z}[G]$. By (15), we have

$$E_2 E_2^{(-1)} = \frac{n^4}{N^4 p^{4e}}. \tag{17}$$

To apply Theorem 2.7, we need to show that $M(n^2/(N^2p^{2e}))$ divides $M(n/N, \lfloor k/N \rfloor)$. Note that, by definition, $M(n^2/(N^2p^{2e}), 2n^2/(N^2p^{2e}) - 2)$ divides $M(n/N, \lfloor k/N \rfloor)$. Furthermore,

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

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

We have $(v, M(n/N, \lfloor k/N \rfloor)) = 1$ by assumption and therefore v and $M(n^2/(N^2p^{2e}))$ are coprime. Thus E_2 is trivial by (17) and Theorem 2.7. Hence $E_1 = E^{(-1)}E^{(p)}$ is trivial, too, i.e., $E_1 = \pm(n^2/N^2)h$ for some $h \in G$. By Result 2.6 (a), this implies $E^{(p)} = Eg$ for some $g \in G$. Note that, by definition, $M(n/N, \lfloor k/N \rfloor)$ is divisible by all prime divisors of $p-1$, since p divides n/N. Hence $(p-1, v) = 1$ by (6). Thus there is $g_1 \in G$ with $g_1^{p-1} = g^{-1}$. We conclude

$$(Eg_1)^{(p)} = Egg_1^p = (Eg_1)(gg_1^{p-1}) = Eg_1.$$

Hence, replacing E by Eg_1, if necessary, we can assume $E^{(p)} = E$.

Suppose that E is nontrivial. Let a_0 and b_0 be the coefficients of the identity in F, respectively E. Note that $b_0 = a_0/N$. 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 $|b_0| < n/N$. Hence

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

Let q be a prime divisor of v. Then $\mathrm{ord}_q(p) > k/N$, since q does not divide any of the numbers $p-1$, p^2-1,...,$p^{\lfloor k/N \rfloor} - 1$ by (6) and the definition of

$M(n/N, \lfloor k/N \rfloor)$. Set $a = \lambda/N$. Then $b_0 \geq -a$ by (18) and $\mathrm{ord}_q(p) > k/N = n/N + \lambda/N = n/N + a$ for all prime divisors q of $|G|$. Thus we can apply Theorem 2.6 with $m = n/N$ and $a = \lambda/N$ and conclude that E is trivial, a contradiction. Hence E and thus F is trivial and this completes the proof of Theorem 3.1. $\square$

4 Finding Multipliers of Higher Order

For numerous open cases of the multiplier conjecture, we have the situation that Theorem 3.1 guarantees the existence of nontrivial multipliers, but multipliers of higher order are required to verify the conjecture in these cases. In this section, we prove a new result which is useful for this purpose.

Let C_x denote a cyclic group of order x and let g be a generator of C_x. Let $A_1, \ldots, A_w$ be subsets of C_x (the A_i's are allowed to be empty). Write $\ell = \sum_{i=1}^{w} |A_i|$. Let M be a set of nonnegative integers. If

$$\sum_{i=1}^{w} A_i A_i^{(-1)} = \ell + \sum_{a=1}^{x-1} m_a g^a \tag{19}$$

with $m_a \in M$ for all a, we say that $(A_1, \ldots, A_w)$ is a **(w, ℓ, M) difference system over C_x**.

Lemma 4.1. *If a (w, ℓ, M) difference system over C_x exists, then*

$$\max M \geq \frac{\ell^2 - \ell w}{w(x-1)}.$$

Proof. Note that $\sum_{i=1}^{w} |A_i|^2 \geq (1/w)(\sum_{i=1}^{w} |A_i|)^2 = \ell^2/w$. On the other hand, $\sum_{i=1}^{w} |A_i|^2 \leq \ell + (x-1) \max M$. This implies the assertion. $\square$

Theorem 4.2. *Let D be a (v, k, λ, n) difference set in an abelian group G with exponent v^*, where $v = p^a$ for a prime p with $(p, n) = 1$. Let n_1 be a divisor of n, and let p_1,...,p_s be the distinct prime divisors of n_1. Assume that D has a multiplier of order f and that* $\gcd(\mathrm{ord}_p(p_1), ..., \mathrm{ord}_p(p_s)) = xf$

for some prime x. Write $k_1 = k$ if $k \equiv 0 \pmod f$ and $k_1 = k-1$ otherwise. If there is no

$$\left(\frac{v-1}{xf}, \frac{k_1}{f}, \left\{\frac{k_1}{f} - sn_1 : 1 \le s \le \frac{k_1}{fn_1}\right\}\right)$$

difference system over C_x, then D has a multiplier of order xf.

Proof. Let t be integer with $\mathrm{ord}_v(t) = xf$ and

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

Then $FF^{(-1)} = n^2$, $F \equiv 0 \pmod{n_1}$, and $E := F/n_1$ satisfies $EE^{(-1)} = n^2/n_1^2$.

Assume that t is not a multiplier of D. Then E is nontrivial. Let a_0 be the coefficient of 1 in E. As E is nontrivial, we have $|a_0| < n/n_1$. Note that E has a multiplier of order f, since D has a multiplier of order f by assumption. Hence $a_0 \equiv |E| \equiv n/n_1 \pmod f$. Thus $a_0 = n/n_1 - sf$ for some positive integer s.

Note that $|D \cap D^{(t)}|$ is the coefficient of 1 in $D^{(-1)}D^{(t)}$. Hence

$$|D \cap D^{(t)}| = a_0 n_1 + \lambda = n - sfn_1 + \lambda = k - sfn_1. \tag{20}$$

Note that $1 \in D$ if $k \not\equiv 0 \pmod f$. Write $D_1 = D$ if $k \equiv 0 \pmod f$ and $D_1 = D - 1$ if $k \not\equiv 0 \pmod f$. Then (20) implies

$$|D_1 \cap D_1^{(t)}| = k_1 - sfn_1. \tag{21}$$

Note that $t^2, ..., t^{x-1}$ are not multipliers of D, since t is not a multiplier of D. Hence, by the same argument as above, we have

$$|D_1 \cap D_1^{(t^a)}| = k_1 - s_a f n_1. \tag{22}$$

for $a = 1, ..., x-1$ and some integers s_a with $1 \le s_a \le k_1/fn_1$.

Write $w = (v-1)/(xf)$ and let Ω_0,...,Ω_{w-1} be the orbits of $y \mapsto y^t$ on G. Note that each Ω_i contains exactly x orbits of $y \mapsto y^{t^x}$ on G. Write

$$\Omega_i = \sum_{j=0}^{x-1} \Omega_{i,j}$$

such that $\Omega_{i,j+1} = \Omega_{i,j}^{(t)}$ for all i, j where the second indices in $\Omega_{i,j}$ are taken mod x. Since t^x is a multiplier of D, we can assume $D^{t^x} = D$ by [14, Thm. 2]. Hence

$$D_1 = \sum_{i=0}^{w-1}\sum_{j=0}^{x-1} d_{i,j}\Omega_{i,j} \tag{23}$$

with $d_{i,j} \in \{0,1\}$ and $\sum_{i,j} d_{i,j} = k_1/f$. Note that

$$D_1^{(t^a)} = \sum_{i=0}^{w-1}\sum_{j=0}^{x-1} d_{i,j}\Omega_{i,j+a} = \sum_{i=0}^{w-1}\sum_{j=0}^{x-1} d_{i,j-a}\Omega_{i,j} \tag{24}$$

for $a = 1, ..., x-1$, where the second indices in $d_{i,j}$ are taken mod x. We conclude

$$|D_1 \cap D_1^{(t^a)}| = f \sum_{i=0}^{w-1}\sum_{j=0}^{x-1} d_{i,j}d_{i,j-a}. \tag{25}$$

Let C_x denote a cyclic group of order x and let g be a generator of C_x. Write $A_i = \sum_{j=0}^{x-1} d_{i,j}g^j$, $i = 0, \ldots, w-1$. Then the coefficient of g^a in

$$T := \sum_{i=0}^{w-1} A_i A_i^{(-1)}$$

is

$$\sum_{i=0}^{w-1}\sum_{j=0}^{x-1} d_{i,j}d_{i,j-a}.$$

Also note that the coefficient of 1 in T is $\sum d_{i,j} = k_1/f$. Hence

$$T = \frac{k_1}{f} + \sum_{a=1}^{x-1}\left(\sum_{i=0}^{w-1}\sum_{j=0}^{x-1} d_{i,j}d_{i,j-a}\right) g^a.$$

From (22) and (25), we have

$$\sum_{i=0}^{w-1}\sum_{j=0}^{x-1} d_{i,j}d_{i,j-a} = (1/f)|D_1 \cap D_1^{(t^a)}| = k_1/f - s_a n_1.$$

Thus

$$\sum_{i=0}^{w-1} A_i A_i^{(-1)} = \frac{k}{f'} + \sum_{a=1}^{x-1}\left(\frac{k}{f'} - s_a n_1\right) g^a. \tag{26}$$

Hence $(A_0, ..., A_{w-1})$ is a

$$\left(\frac{v-1}{xf}, \frac{k_1}{f}, \left\{\frac{k_1}{f} - sn_1 : 1 \le s \le \frac{k_1}{fn_1}\right\}\right)$$

difference system over C_x, contradicting the assumptions. □

Corollary 4.3. *Let D be a (v, k, λ, n) difference set in an abelian group G with exponent v^*, where $v = p^a$ for a prime p with $(p, n) = 1$. Let n_1 be a divisor of n, and let p_1,...,p_s be the distinct prime divisors of n_1. Assume that D has a multiplier of order f and that $\gcd(\mathrm{ord}_p(p_1), ..., \mathrm{ord}_p(p_s)) = xf$ for some integer $x > 1$. Write $k_1 = k$ if $k \equiv 0 \pmod f$ and $k_1 = k - 1$ otherwise. If*

$$n_1 > \frac{k_1 q(v - k_1 - 1)}{f(v-1)(q-1)}, \tag{27}$$

where q is the smallest prime divisor of x, then D has a multiplier of order xf.

Proof. Let r be any prime divisor of x and suppose that D does not have a multiplier of order rf. Then, by Theorem 4.2, there is a

$$\left(\frac{v-1}{rf}, \frac{k_1}{f}, \left\{\frac{k_1}{f} - sn_1 : 1 \le s \le \frac{k_1}{fn_1}\right\}\right)$$

difference system over C_r. Note that

$$\max\left\{\frac{k_1}{f} - sn_1 : 1 \le s \le \frac{k_1}{fn_1}\right\} = \frac{k_1}{f} - n_1.$$

Thus

$$\frac{k_1}{f} - n_1 \ge \frac{\frac{k_1^2}{f^2} - \frac{k_1}{f}\frac{v-1}{rf}}{\frac{v-1}{rf}(r-1)}$$

by Lemma 4.1. This implies

$$n_1 \le \frac{k_1 r(v - k_1 - 1)}{f(v-1)(r-1)},$$

which contradicts (27), since $r \ge q$ and thus $r/(r-1) \le q/(q-1)$. Hence D has a multiplier of order rf.

If $r < x$, then we choose a prime divisor r_1 of x/r and repeat the same argument as above with f replaced by fr and r replaced by r_1. This shows that D has a multiplier of order frr_1. Continuing in this way, we see that D has a multiplier of order fx □

Example 4.4. Let D be a $(4n-1, 2n-1, n-1, n)$ difference set with $n = 266$. Note that $v = 4n - 1 = 1063$ is a prime. We have $n = 2 \cdot 7 \cdot 19$, $\mathrm{ord}_p(2) = 531$, $\mathrm{ord}_p(7) = 9$, and $\mathrm{ord}_p(19) = 531$. Theorem 3.1 with $n_1 = n$ shows that 7 is a multiplier of D. Hence D has a multiplier of order $f = 9$. Theorem 3.1, however, does not imply that 2 and 19 are multipliers of D. Set $x = 59 = 531/9$, $n_1 = 38$. Note that

$$38 = n_1 > \frac{k_1 x(v - k_1 - 1)}{f(v-1)(x-1)} = \frac{531 \cdot 59 \cdot (1063 - 531 - 1)}{9 \cdot 1062 \cdot 58}.$$

Hence D has a multiplier of order 531 by Corollary 4.3. This implies that 2 and 19 are multipliers of D, as predicted by the multiplier conjecture.

5 Computational Results

It is natural to ask how close Theorem 3.1 brings us to the multiplier conjecture. No counterexample has ever been found, but this is not strong evidence. Known difference sets fit into a few families, for most of which the multiplier conjecture follows immediately.

For parameters of Hadamard, McFarland, Spence, Davis-Jedwab and Chen difference sets, the multiplier conjecture is vacuously true, since all primes dividing n also divide v. Singer difference sets (and other inequivalent difference sets with the same parameters) satisfy the multiplier conjecture by the Second Multiplier Theorem. Lehmer [10] showed that for difference sets composed of nth power residues, the multipliers are the elements of the difference set.

To gather more evidence, we looked at (v, k, λ, n) difference sets D in abelian groups G of order $v < 10^6$, to see which primes $p|n$, $\gcd(p, v) = 1$ are known to be multipliers for all such D. Eliminating parameters which do not pass known necessary conditions (counting arguments, Bruck-Ryser-Chowla, and many others; see [2]) leaves 222531 sets of parameters, with 413586 primes p covered by the multiplier conjecture.

The primary ways of establishing whether a given parameter set and prime p satisfies the multiplier conjecture are Theorem 3.1 and Corollary 4.3. Another tool is the following result which essentially is due to Hall and Yamamoto. Let φ denote the Euler totient function.

Result 5.1. *Let q be an odd prime power and let D be a (q, k, λ, n) difference set in the additive group of the finite field $\mathbb{F}_q$. If D has a multiplier of order at least $\varphi(q)/14$, then the multiplier conjecture holds for D.*

Proof. Write $q = p^a$ where p is an odd prime. Let t be a multiplier of D of order $f \geq \varphi(q)/14$. Note that $f = \mathrm{ord}_p(t)$ and thus f divides $p - 1$. By [14, Thm. 2], we can assume that D is fixed by t, i.e., $tD = D$.

Let C_0 be the orbit of t on $\mathbb{F}_q$ which contains 1. Then $C_0 = \{t^i : i = 0, \ldots, f-1\}$ is the (multiplicative) subgroup of $\mathbb{F}_q^*$ of order f. Similarly, the other orbits of t on $\mathbb{F}_q^*$ are cosets of C_0 in $\mathbb{F}_q^*$. Hence $D \setminus \{0\}$ is a union of eth power cyclotomic cosets where $e = (q-1)/f$ (see [3, Section 6.8] for background on cyclotomic cosets).

First suppose that q is a prime. Note that, in this case, $e \leq 14$, as $f \leq (v-1)/14$. For q prime, Hall [6] and Yamamoto [24, 25] classified all difference sets D in $\mathbb{F}_q$ such that $D \setminus \{0\}$ is a union of eth power cyclotomic cosets with $e \leq 14$. Furthermore, the multiplier conjecture holds for all these difference sets. This proves Theorem 5.1 for q prime.

Now suppose that q is not a prime, i.e., $a \geq 2$. We have $f \geq \varphi(q)/14 = p^{a-1}(p-1)/14$. As f divides $p - 1$, this implies $p^{a-1} \leq 14$. Hence $p \leq 13$ and $q \leq 169$. But the multiplier conjecture has been verified for all abelian groups of order less than 343 (see the tables in the appendix). This completes the proof. $\square$

When the above mentioned tools do not suffice, for small parameters it may be possible to do an exhaustive search of unions of orbits of known multipliers, finding all inequivalent difference sets and directly testing whether

p is a multiplier. This was done with C code used in [2], improved to handle larger cases, and reimplemented in Sage [20] to verify the results.

Of the 413586 primes for possible difference sets with $v < 10^6$ covered by the multiplier conjecture, 268592, or 65%, are known to be multipliers by the results given in this paper. If we restrict ourselves to Paley parameters $(4n-1, 2n-1, n-1, n)$, where G is the additive group of a finite field, there are 116386 primes, of which 115457, or 99%, are known to satisfy the multiplier conjecture.

There are a number of cases where we show that p cannot be a multiplier, either because it violates Mann's condition on multipliers (see Theorem 2 of [9]), or, in the cyclic case, that the group generated by p and known multipliers is larger than k, which contradicts the bound of [23]. Finally, an exhaustive search of the orbits of a multiplier group including p may show that no combination of orbits forms a difference set.

For parameters where difference sets are known to exist, the only cases where the multiplier conjecture is open are parameters of some Paley or twin prime power (TPP) difference sets. Table 1 gives such parameters with $v < 10^4$ for which the multiplier conjecture is open.

For other parameters where the existence of any difference sets is open, there are many more cases where the multiplier conjecture is open (presumably it is often true because there are no such difference sets). Table 2 gives the smallest open cases. Tables for all parameters with $v < 10^6$ may be found online at [4].

The column "MC primes" in the tables gives prime factors of n which are multipliers under the multiplier conjecture. A circle around a number means that it is not known whether the prime must be a multiplier, and a box around a prime or set of primes mean that the primes cannot be multipliers (and so the existence of such a difference set would contradict the multiplier conjecture).

v	k	λ	G	n	MC primes	comment
343	171	85	[7, 7, 7]	$2 \cdot 43$	2 43	Paley
631	315	157	[631]	$2 \cdot 79$	2 79	Paley
783	391	195	[3, 3, 87]	$2^2 \cdot 7^2$	2 7	TPP(27)
911	455	227	[911]	$2^2 \cdot 3 \cdot 19$	2 3 19	Paley
1331	665	332	[11,11,11]	$3^2 \cdot 37$	3 37	Paley
1483	741	370	[1483]	$7 \cdot 53$	7 53	Paley
1763	881	440	[1763]	$3^2 \cdot 7^2$	3 7	TPP(41)
2303	1151	575	[7, 329]	$2^6 \cdot 3^2$	2 3	TPP(47)
2663	1331	665	[2663]	$2 \cdot 3^2 \cdot 37$	2 3 37	Paley
3571	1785	892	[3571]	$19 \cdot 47$	19 47	Paley
3851	1925	962	[3851]	$3^2 \cdot 107$	3 107	Paley
3911	1955	977	[3911]	$2 \cdot 3 \cdot 163$	2 3 163	Paley
3923	1961	980	[3923]	$3^2 \cdot 109$	3 109	Paley
4999	2499	1249	[4999]	$2 \cdot 5^4$	2 5	Paley
5183	2591	1295	[5183]	$2^4 \cdot 3^4$	2 3	TPP(71)
6163	3081	1540	[6163]	$23 \cdot 67$	23 67	Paley
6871	3435	1717	[6871]	$2 \cdot 859$	2 859	Paley
7351	3675	1837	[7351]	$2 \cdot 919$	2 919	Paley
8171	4085	2042	[8171]	$3^2 \cdot 227$	3 227	Paley
8179	4089	2044	[8179]	$5 \cdot 409$	5 409	Paley
8951	4475	2237	[8951]	$2 \cdot 3 \cdot 373$	2 3 373	Paley

Table 1: Parameters with $v < 10^4$ for which difference sets are known to exist

v	k	λ	G	n	MC primes
343	171	85	[7, 49]	$2 \cdot 43$	2 43
416	166	66	[2, 208]	$2^2 \cdot 5^2$	5
416	166	66	[4, 104]	$2^2 \cdot 5^2$	5
425	160	60	[5, 85]	$2^2 \cdot 5^2$	2
448	150	50	[2, 224]	$2^2 \cdot 5^2$	5
448	150	50	[4, 112]	$2^2 \cdot 5^2$	5
448	150	50	[8, 56]	$2^2 \cdot 5^2$	5
469	208	92	[469]	$2^2 \cdot 29$	$\boxed{2}$ 29
477	204	87	[3, 159]	$3^2 \cdot 13$	13
495	247	123	[3, 165]	$2^2 \cdot 31$	2 31
621	156	39	[3, 207]	$3^2 \cdot 13$	13
621	156	39	[3, 3, 69]	$3^2 \cdot 13$	13
639	232	84	[639]	$2^2 \cdot 37$	$\boxed{2}$ 37
639	232	84	[3, 213]	$2^2 \cdot 37$	$\boxed{2}$ 37
703	325	150	[703]	$5^2 \cdot 7$	$\boxed{5}$ 7
729	273	102	$\exp(G) \leq 27$	$3^2 \cdot 19$	19
736	196	52	$\exp(G) \leq 368$	$2^4 \cdot 3^2$	3
765	192	48	[3, 255]	$2^4 \cdot 3^2$	2
781	300	115	[781]	$5 \cdot 37$	$\boxed{5\ \ 37}$
783	391	195	[3, 261]	$2^2 \cdot 7^2$	$\boxed{2}$ 7
816	326	130	[2, 408]	$2^2 \cdot 7^2$	$\boxed{7}$
847	423	211	[11, 77]	$2^2 \cdot 53$	$\boxed{2}$ 53
855	183	39	[3, 285]	$2^4 \cdot 3^2$	$\boxed{2}$
909	228	57	[3, 303]	$3^2 \cdot 19$	$\boxed{19}$
910	405	180	[910]	$3^2 \cdot 5^2$	$\boxed{3}$

Table 2: Open difference set parameters

References

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

[2] L. D. Baumert, D. M. Gordon: On the existence of cyclic difference sets with small parameters. *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams.* Fields Inst. Commun. **41**, 61-68.

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

[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] E. S. Lander: Restrictions upon multipliers of a abelian difference set. *Arch. Math.* **50** (1988), 241–242.

[10] E. Lehmer: On residue difference sets. *Canad. J. Math.* **5** (1953), 425–432.

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

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

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

[14] R. L. McFarland, B. F. Rice: Translates and multipliers of abelian difference sets. *Proc. Amer. Math. Soc.* **68** (1978), 375–379.

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

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

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

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

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

[20] *Sage Mathematics Software (Version 6.1.1)*, The Sage Developers, 2015, `http://www.sagemath.org`.

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

[22] R. J. Turyn: Character sums and difference sets. *Pacific J. Math.* **15** (1965), 319–346.

[23] Q. Xiang, Y. Q. Chen: On the size of the multiplier groups of cyclic difference sets. *J. Combin. Theory* Ser. A **69** (1995), 168–169.

[24] K. Yamamoto: On Jacobi sums and difference sets. J. Comb. Th. **3** (1967), 146–181.

[25] K. Yamamoto: On the application of half-norms to cyclic difference sets. In: *Combinatorial mathematics and its applications (eds. R. C. Bose and T. A. Dowling).* University of North Carolina Press, Chapel Hill (1969), 247–255.