INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.
Difference Sets: Their Multipliers and Existence

Dissertation

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of The Ohio State University

By

Qing Xiang, B. S., M. S.

* * * * *

The Ohio State University

1995

Dissertation Committee:

Professor D. K. Ray-Chaudhuri
Professor Thomas A. Dowling
Professor Ronald Solomon

Approved by

[Signature]
Adviser

Department of Mathematics
I would like to express my sincere gratitude to Professor D. K. Ray-Chaudhuri, for all he has taught me, mathematically and otherwise, in the past four years. I want to thank him also for the advice, encouragement and help he gave me in the preparation of this work. Thanks also go to other members of my committee, Professors Thomas A. Dowling and Ronald Solomon, for their careful reading of the draft of this work, and many helpful comments.

I would like to thank K. T. Arasu, J. A. Davis, C. Y. Ho, J. Hsia, D. Jungnickel, W. M. Kantor, S. L. Ma, M. K. Siu, R. M. Wilson and M. Y. Xia. I greatly benefited from conversations, electronic communications, or joint work with them.

I want to thank my classmates Y. Q. Chen, W. K. Chan and Radha Kessar, for their helpful discussions and friendship. Especially, I thank Y. Q. Chen for many stimulating conversations and long time collaboration.

Finally, I thank my wife, Zeyun Cui, for her support and faith in me through the years.
VITA

July 13, 1965............ Born in Hubei, People's Republic of China

1990.........................M. S., Sichuan University, P. R. China

1990-1991...............Graduate Teaching Assistant, Department of
Math. and Stat., Wright State University
Dayton, OH 45435

1991-1995...............Graduate Teaching Associate, Department of
Mathematics, The Ohio State University
Columbus, OH 43210

Publications

1. (with W. Wei, and S. Gao) Extraneous Multipliers of Abelian Difference Sets, In


8. *Reversible* $(m,n,k,\lambda_1,\lambda_2)$-*abelian divisible difference sets with $k - \lambda_1$ nonsquare*, Disc. Math. 142, 1995, pp193-201.

**Fields of Study**

Major Field: Mathematics

Studies in Combinatorics with Professor D. K. Ray-Chaudhuri

Studies in Group Representation Theory with Professor Ron Solomon

Studies in Number Theory with Professor John S. Hsia
TABLE OF CONTENTS

ACKNOWLEDGMENTS.................................................................ii

VITA.....................................................................................iii

INTRODUCTION..........................................................................1

CHAPTER PAGE

I Definitions and Background...................................................8
   1.1 Symmetric designs and difference sets.................................8
   1.2 Group rings and characters................................................14
   1.3 Background in algebraic number theory...............................18
   1.4 Finite fields, cyclotomy......................................................21
   1.5 Codes and point sets in projective geometry.......................24

II Multipliers of difference sets...............................................28
   2.1 Multiplier theorems..........................................................28
   2.2 Numerical multiplier groups of difference sets...................42

III Skew Hadamard difference sets.........................................54
   3.1 Introduction and a summary of old results..........................54
   3.2 A new exponent bound.....................................................57

IV Reversible difference sets..................................................62
4.1 Definitions and introduction ................................................................. 62
4.2 A result on Ma's conjecture ................................................................. 65
4.3 Hadamard difference sets ................................................................. 67
4.4 New necessary conditions for HDSs ................................................... 70
4.5 On Xia's construction ................................................................. 86

V Further research problems .................................................................... 94

REFERENCES ....................................................................................... 98
INTRODUCTION

Let $G$ be a finite group of order $v$. A subset $D$ of size $k$ in group $G$ is called a $(v,k,\lambda)$-difference set if the list of differences $d_1d_2^{-1}$, $d_1 \neq d_2$, $d_1, d_2 \in D$ contains each non-identity element of $G$ exactly $\lambda$ times. Difference sets are important objects in combinatorial design theory because they are equivalent to symmetric designs with a regular automorphism group. The study of difference sets is also deeply connected with coding theory, and has found many applications in signal analysis and design.

The history of difference sets goes back to Singer's famous paper [S] in 1938, however, the systematic study of difference sets only started with the fundamental papers of Marshall Hall Jr [HA1] in 1947 (who considered cyclic projective planes and introduced the concept of multiplier) and Bruck [B] in 1955 (who started the investigation of difference sets in general groups). The central research problem in difference sets is: for each positive integer $v$, which group $G$ of order $v$ admits a nontrivial difference set? This problem is far from being resolved (not even for cyclic groups), despite a large literature spanning more than half a century. The research in this work basically centers around multiplier and existence problems of difference sets.
Let us begin with the definition of multiplier. Let $G$ be a finite group of order $v$, $D$ a subset of $G$, and $t$ an integer co-prime with $v$. If $D^{(t)} = \{dt | d \in D\} = Dg$ for some $g \in G$, then $t$ is called a numerical multiplier of $D$. The following theorem is often called the first multiplier theorem which is a generalization of Hall’s original multiplier theorem for cyclic projective planes.

**First Multiplier Theorem.** Let $D$ be a $(v, k, \lambda)$-difference set in an abelian group $G$, and let $p$ be a prime dividing $n := k - \lambda$ but not $v$. If $p > \lambda$, then $p$ is a multiplier of $D$.

From this theorem, we can see that very often the parameters of an abelian difference set $D$ force the existence of numerical multipliers which then can be used to help with either the construction or a nonexistence proof of the difference set. This shows the importance of the first multiplier theorem.

All known examples of abelian difference sets admit every prime divisor of $n$ as a multiplier, whether or not $p > \lambda$. This leads to the following long-standing conjecture.

**The Multiplier Conjecture.** The first multiplier theorem holds without the assumption $p > \lambda$.

This conjecture plays a prominent role in the theory of abelian difference sets. Although it is widely believed, the attempts to prove its general form have not yet been successful. A considerable amount of work has been done in this area. The reader can find a summary of known results on multipliers of difference sets in Chapter II of this work.
In Section 1 of Chapter II, we first prove a general multiplier theorem for central elements in a group ring. This multiplier theorem unifies and improves most previous multiplier theorems, it also gives new multipliers which can not be obtained by previous multiplier theorems. As an application, we prove the nonexistence of certain relative difference sets that correspond to the so-called elliptic semiplanes. The material in this section basically comes from the paper by Arasu and Xiang [AX].

In Section 2 of Chapter II, we developed a number theoretic approach to study multipliers of abelian difference sets. Let $G$ be an abelian group of order $v$, with exponent $e_G$, $D$ a $(v, k, \lambda)$-difference set in $G$, and $M$ the numerical multiplier group of $D$. By a result of McFarland and Rice [MR], we may assume that $D$ is fixed by every element of $M$. Let $K_G = Q(\xi_{e_G})$, $K_D = Q(\chi_0(D), \chi_1(D), \cdots, \chi_{v-1}(D))$, where $\xi_{e_G}$ is a primitive $e_G$-th root of unity, and $\{\chi_0, \chi_1, \cdots, \chi_{v-1}\} = G^*$, the character group of $G$. Then it is not difficult to see that $M = Gal_{K_G}/K_D$ (Lemma 2.2.1 in Chapter II). Using this point of view and a deep theorem of Cohen [CO], we get an upper bound for the size of the multiplier groups of cyclic difference sets. We also give examples to show that the upper bound is best possible. Next by using this number theoretic approach, we prove that a prime $p$ is a multiplier of $D$ if and only if $p$ splits completely in $Q(\chi(D))$, for every nonprincipal character $\chi$ of $G$. Based on this characterization of multipliers, we prove that if $\chi(D) + \overline{\chi(D)}$ is a rational integer for every nonprincipal character $\chi$ of the group, then the multiplier conjecture is true for $D$. But in general, we still can not verify the multiplier conjecture. The difficulty lies in the lack of information about the field $K_D$. We study the
cases $K_D=\text{a quadratic extension of } Q$, and $K_D = Q$ in more detail in Chapter III and IV.

In Chapter III, we study skew Hadamard difference sets. The field $K_D$ of a skew Hadamard difference set $D$ is an imaginary quadratic extension of $Q$, which is one of the easiest extensions among all abelian extensions of $Q$. Also as an application of our characterizations of multipliers, we considered the case when 2 is a multiplier of abelian difference sets (since 2 is the smallest prime). We proved in Chapter II by number theoretic arguments that if $D$ is an abelian difference set which is fixed by the multiplier 2, then $D$ is skew Hadamard. These are the motivations for us to study skew Hadamard difference sets. Skew Hadamard difference sets were previously studied in connection with Hadamard matrices and $\lambda$-ovals (see [JU],[JU1]). Paley [PA] constructed skew Hadamard difference sets in the additive group of $GF(q)$, where $q$ is a prime power congruent to 3 (mod 4). It is conjectured that these are the only examples. In this chapter we obtained an exponent bound for non-elementary $p$-groups which admit skew Hadamard difference sets. The previously best known bound was due to Johnsen, Camion and Mann [JO], [CM] in the 1970's. Our exponent bound in particular shows that if $|G| = p^3$ or $p^5$, $G$ is abelian and contains a skew Hadamard difference set, then $G$ is elementary abelian. Also the method of obtaining this exponent bound has application in other situations, for example, it can be applied to reversible Hadamard difference sets (see Theorem 4.3.5) and Paley type partial difference sets [XQ1].

In chapter IV, we study abelian difference sets with multiplier -1. By a result of McFarland and Rice [MR], we may assume that a difference set $D$ with
-1 multiplier is fixed by -1, then $D$ is called a reversible or symmetric difference set. It is well known that if $D$ is a reversible difference set, then every integer $t$ relatively prime to $v$ is a multiplier for the difference set, hence $K_D = Q$.

It turns out that reversible abelian difference sets split naturally into two classes, those satisfying $v \neq 4(k - \lambda)$ and those with $v = 4(k - \lambda)$. So far, there is only one known example for the first case.

**Example 1.** There exists a reversible $(4000, 775, 150)$-difference set in $\mathbb{Z}_2^5 \times \mathbb{Z}_5^3$. This example is due to McFarland [MC1].

McFarland has proposed the following conjecture.

**McFarland's Conjecture.** If $D$ is a reversible abelian $(v, k, \lambda)$-difference set, then either $v = 4000, k = 775, \lambda = 150$ (as in Example 1) or $v = 4(k - \lambda)$.

After studying sub-difference sets of reversible abelian difference sets, Ma [MA] proposed the following conjecture which implies McFarland's Conjecture.

**Ma's Conjecture.** Let $p$ be an odd prime, $a \geq 0$, and $b, m, r \geq 1$. Then

1. $Y = 2^{2a+2}p^{2m} - 2^{a+2}p^{m+r} + 1$ is a square if and only if $m = r$ (i.e. $Y = 1$).
2. $Z = 2^{b+2}p^{2m} - 2^{b+2}p^{m+r} + 1$ is a square if and only if $p = 5, b = 3, m = 1, r = 2$ (i.e. $Z = 2401$).

In Section 2 of Chapter IV, we give a proof for part (1) of Ma's conjecture by using Pell's equation. In view of this result, in order to prove McFarland's conjecture on abelian difference sets with multiplier -1, all we need to
do is to prove part (2) of Ma's conjecture. This remains open at present. The material in this section comes from the paper by Le and Xiang [LX].

Once McFarland's conjecture is proved, the study of reversible abelian difference sets is reduced to the case when \( v = 4(k - \lambda) \). A \((v, k, \lambda)\)-difference set satisfying \( v = 4(k - \lambda) \) is called a Hadamard difference set, and it must have parameters \((4u^2, 2u^2 \pm u, u^2 \pm u)\). Hadamard difference sets are of special interest because of their close connection to Hadamard matrices and perfect binary arrays, hence they have received a lot of attention during the past thirty years. Several years ago, McFarland conjectured that if a \((4u^2, 2u^2 \pm u, u^2 \pm u)\)-abelian Hadamard difference set exists, then \( u = 2^a 3^b \). A body of evidence has accumulated, involving both constructive and nonexistence results, supporting McFarland's conjecture. But recently Xia [X] disproved McFarland's conjecture spectacularly by explicitly constructing Hadamard difference sets in groups \( H \times \mathbb{Z}_{p_1}^4 \times \cdots \times \mathbb{Z}_{p_r}^4 \), where \( H \) is either the Klein 4-group or the cyclic group of order 4 and each \( p_j \) is a prime congruent to 3 modulo 4. This is a major advance in the field of difference sets. But Xia's construction depends on very complicated calculations involving cyclotomic classes of high orders, therefore it is not clear why the construction works. It was generally considered that Xia's construction is not well understood.

We study Hadamard difference sets with multiplier -1 in depth. In particular we show that certain reversible Hadamard difference sets can give rise to projective three-weight codes and vice versa. We state the theorem as follows.
Theorem. There is a reversible Hadamard difference set $D$ in abelian group $G = Z_2 \times Z_2 \times (Z_p)^{2\alpha}$, $p$ an odd prime, $\alpha$ even, if and only if there are four projective $(n, 2\alpha, \frac{n}{p} - p^{\alpha-1}, \frac{n}{p}, \frac{n}{p} + p^{\alpha-1})$ sets $O_i$, $i = 0, 1, 2, 3$, in $PG(2\alpha - 1, p)$ with $n = \frac{p(p^{\alpha-1})}{2(p-1)}$ such that for any hyperplane $H$ in $PG(2\alpha - 1, p)$, there is a unique $i$, $0 \leq i \leq 3$, such that $|H \cap O_i| \neq \frac{n}{p}$, and $|H \cap O_j| = \frac{n}{p}$, if $j \neq i$.

The above theorem allows us to view Xia’s construction in a more coding theoretic (or geometric) way. Based on this perspective, we give a very simple proof for Xia’s construction and show that the projective three-weight codes in Xia’s construction come from the combination of two 2-weight codes. The two 2-weight codes come from subspace examples and cyclotomy examples respectively.

The method used to prove the above theorem can be applied to Hadamard difference sets in general (not necessarily the ones with multiplier -1). For example, in Section 4 of Chapter IV, we prove that if $p$ is a prime congruent to 1 (mod 4), and $\alpha$ is odd, then there exists no Hadamard difference set in $Z_2 \times Z_2 \times P$, where $|P| = p^{2\alpha}$, $P$ is abelian. Combining this result with some techniques of Chan [CH] and McFarland [MC2], we can prove more general nonexistence results for abelian Hadamard difference sets.

We conclude this work by presenting a few research problems in Chapter V. Research Problem 5.1 is clearly related to the multiplier conjecture, so it is of fundamental importance in the study of difference sets. Other problems are related to the cases when the field $K_D$ of a difference set $D$ is a quadratic extension of $Q$ or $Q$ itself. We hope that someday we can have a complete understanding of these two cases.
Chapter I
Definitions and Background

1. Symmetric Designs and Difference Sets

A balanced incomplete block design (BIBD) with parameters \((v, b, r, k, \lambda)\) is a pair \((\mathcal{P}, \mathcal{B})\) that satisfies the following properties:

1. \(\mathcal{P}\) is a set of \(v\) elements (called points).
2. \(\mathcal{B}\) is a set of \(b\) subsets of \(\mathcal{P}\), each of cardinality \(k\) (called blocks).
3. Every point occurs in exactly \(r\) blocks.
4. Every pair of distinct points occurs in exactly \(\lambda\) blocks.

We shall assume that \(k < v\). It is easy to see that the five parameters of a BIBD are not independent, simple counting yields the following two relations:

\[
bk = vr \quad \text{(1.1.1)}
\]
\[
\lambda(v - 1) = r(k - 1) \quad \text{(1.1.2)}
\]

Determining necessary and sufficient conditions for the existence of BIBDs is one of the central problems in design theory. We first prove the following basic result about BIBDs. The proof is very typical in design theory.
**Theorem 1.1.1.** Let $B$ be a block of a $(v, b, r, k, \lambda)$-BIBD. Then the number of blocks not disjoint from $B$ is at least $k(r-1)^2/((k-1)(\lambda-1)+(r-1))$. Equality holds if and only if blocks which are not disjoint from $B$ meet it in a constant number of points. If this occurs, then the constant number is $1 + \frac{(k-1)(\lambda-1)}{r-1}$.

**Proof:** Let $d$ be the number of blocks which are distinct from but not disjoint from $B$, suppose that $a_i$ of these blocks meet $B$ in $i$ points, $0 < i \leq k$. Count blocks, pairs $(p, B')$ with $p \in B \cap B'$, and triples $(p, q, B')$ with $p \neq q$ and $\{p, q\} \subset B \cap B'$, we find

\[
\sum_{i=1}^{k} a_i = d
\]
\[
\sum_{i=1}^{k} i a_i = k(r - 1)
\]
\[
\sum_{i=1}^{k} \binom{i}{2} a_i = \binom{k}{2} (\lambda - 1).
\]

From these we have

\[
\sum_{i=1}^{k} (i - x)^2 a_i = dx^2 - 2k(r - 1)x + k((k - 1)(\lambda - 1) + (r - 1)).
\]

This quadratic form in $x$ must be positive semi-definite, hence $d \geq \frac{k(r-1)^2}{(k-1)(\lambda-1)+(r-1)}$. It vanishes only if $d = \frac{k(r-1)^2}{(k-1)(\lambda-1)+(r-1)}$, in which case $a_i = 0$ for all $i \neq 1 + \frac{(k-1)(\lambda-1)}{r-1}$. This completes the proof. □

One of the most basic necessary conditions for the existence of a BIBD is known as Fisher's inequality, we can now deduce it quickly from Theorem 1.1.1.
**Theorem 1.1.2.** For a \((v, b, r, k, \lambda)-\text{BIBD}\) with \(v > k\), we have \(b \geq v\).

**Proof:** By Theorem 1.1.1, we have

\[
b - 1 \geq \frac{k(r - 1)^2}{(k - 1)(\lambda - 1) + (r - 1)} \tag{1.1.5}
\]

Using (1.1.1) and (1.2.1), and noting that \(v > k\), we have \(b \geq v\). This completes the proof. □

A BIBD with \(b = v\) is called a symmetric BIBD, or a symmetric design.

From Theorem 1.1.1, we have the following theorem.

**Theorem 1.1.3.** For a \((v, b, r, k, \lambda)-\text{BIBD}\) with \(v > k\), the following are equivalent:

1. \(b = v\).
2. \(r = k\).
3. Any two blocks meet in \(\lambda\) points.

**Proof:** (1) \(\Leftrightarrow\) (2) follows from (1.1.1).

(2) \(\Rightarrow\) (3): Consider any block \(B\) of the design. For \(0 \leq i \leq k\) let \(a_i\) be the number of blocks (\(\neq B\)) that have \(i\) points in common with \(B\). Then as in the proof of Theorem 1.1.1, we have

\[
\sum_{i=0}^{k} a_i = v - 1
\]

\[
\sum_{i=0}^{k} ia_i = k(k - 1)
\]

\[
\sum_{i=0}^{k} \binom{i}{2} a_i = \binom{k}{2} (\lambda - 1). \tag{1.1.6}
\]

From which we find \(\sum_{i=0}^{k} (i - \lambda)^2 a_i = 0\). Hence any block \(B' \neq B\) has \(\lambda\) points in common with \(B\).
(3)⇒(2): If any two blocks meet in $\lambda$ points, by Theorem 1.1.1, $\lambda = 1 + \frac{(k-1)(k-1)}{r-1}$. If $\lambda > 1$ then $r = k$. If $\lambda = 1$, again by Theorem 1.1.1, we have $b - 1 = k(r - 1)$. Using (1.1.1) and (1.1.2), we have $v(r - k) = k(r - k)$, since $v > k$, we have $r = k$. This completes the proof of the theorem. □

From now on, we are basically interested in $(v, k, \lambda)$-symmetric designs, in fact, this work mainly deals with a special kind of symmetric designs, namely difference sets (see the definition later).

Besides the apparent parameter relation $\lambda(v - 1) = k(k - 1)$, there is a further necessary condition for the existence of a symmetric design which is known as the Bruck-Ryser-Chowla theorem. We state the theorem without giving proof.

**Theorem 1.1.4.** Suppose that a $(v, k, \lambda)$-symmetric design exists.

1. If $v$ is even, then $k - \lambda$ is a square.
2. If $v$ is odd, the Diophantine equation $(k - \lambda)x^2 + (-1)^{\frac{v}{2}}(k - \lambda)y^2 = z^2$ has a solution in integers $x, y, z$ not all zero.

We remark that the condition $k(k - 1) = \lambda(v - 1)$ and the Bruck-Ryser-Chowla theorem are not sufficient for the existence of a symmetric design. One single parameter triple, i.e. $(111, 11, 1)$ is known which satisfies these conditions where no design exists.

Two symmetric designs are said to be isomorphic if there is a bijection of the respective point sets that preserves blocks. An automorphism of a symmetric design is an isomorphism with itself. The set of all automorphisms of a symmetric design forms a group under functional composition. Moreover this automorphism group acts in a natural way as a permutation group on the
points of the design, or on its blocks.

A \((v, k, \lambda)\)-symmetric design \(\mathcal{D}\) is called regular if it admits an automorphism group \(G\) acting sharply transitively on points. It is a well-known result that in this case \(G\) also acts sharply transitively on blocks (see [BJL]).

One may then select a "base point" \(p_0\) and identify the point set of \(\mathcal{D}\) with the group \(G\) as follows: If \(g\) is the unique element of \(G\) mapping \(p_0\) to \(p\), then we identify \(p\) with \(g\); in particular, \(p_0\) is identified with \(0 \in G\) (here we write \(G\) additively, even if \(G\) is nonabelian). Now choose a "base block" \(B_0\), and let \(D\) be the corresponding \(k\)-set of elements of \(G\) (so all blocks of the symmetric designs now take the form \(D + h\) for \(h \in G\)). Then \(D\) is a \((v, k, \lambda)\)-difference set in \(G\); that is, the list of all differences \(d - d'\) (where \(d, d' \in D, d \neq d'\)) contains each nonzero group element exactly \(\lambda\) times. To see this, one just note that for any \(g \neq 0\), by Theorem 1.1.3, 

\[
|\{(D + g) \cap D\}| = \lambda,
\]

so \(g\) has exactly \(\lambda\) different representations as \(g = d - d', d, d' \in D\).

We give the complete definition of difference sets here.

**Definition 1.1.1.** Let \(G\) be a finite group of order \(v\). A \(k\)-subset \(D\) of \(G\) is called a \((v, k, \lambda)\)-difference set if the list of "differences" \(d_1 d_2^{-1}, d_1 \neq d_2, d_1, d_2 \in D\) represent each nonidentity element of \(G\) exactly \(\lambda\) times.

A similar argument as above shows that any \((v, k, \lambda)\)-difference set \(D\) gives rise to a \((v, k, \lambda)\)-symmetric design:

\[
\mathcal{D} = devD = (G, \{D + g : g \in G\})
\]

that admits \(G\) as a regular automorphism group (acting by right translation).

Thus we have
Theorem 1.1.5. A \((v, k, \lambda)\)-symmetric design with a regular automorphism group \(G\) is equivalent to a \((v, k, \lambda)\)-difference set in \(G\).

The design \(\text{dev}D\) is usually called the development of \(D\), the blocks \(D + g\) are often referred to as the translates of \(D\). We will call a difference set \(D\) in \(G\) cyclic (resp. abelian, nonabelian) if \(G\) has the respective property. If \(\alpha\) is an automorphism of \(G\), then a subset \(D\) of \(G\) is a difference set if and only if \(\alpha(D)\) is. Two \((v, k, \lambda)\)-difference sets \(D_1\) and \(D_2\) in \(G\) are said to be equivalent if there are \(\alpha \in \text{Aut}G\) and \(g \in G\) such that \(D_2 = \alpha(D_1) + g\).

Before we continue, we give two examples of difference sets.

Example 1.1.1. For every prime power \(q\) and every integer \(d \geq 2\), there exists a cyclic \((v, k, \lambda)\)-difference set \(D\) with parameters \(v = \frac{q^d-1}{q-1}\), \(k = \frac{q^d-1}{q-1}\), and \(\lambda = \frac{q^d-1}{q-1}\), equivalent to the classical symmetric design \(PG_{d-1}(d, q)\) of points and hyperplanes in the projective \(d\)-space \(PG(d, q)\) over \(GF(q)\).

Example 1.1.2. Let \(q = 4n - 1\) be a prime power. Then the set \(D\) of nonzero quadratic residues in \(GF(q)\) is an elementary abelian \((4n - 1, 2n - 1, n - 1)\)-difference set. The corresponding symmetric design is the classical Paley-Hadamard design.

In this work, we are mainly concerned with abelian difference sets. The central research problems in the study of difference sets are:

(1) Given parameter triple \((v, k, \lambda)\) satisfying \(\lambda(v - 1) = k(k - 1)\) and the Bruck-Ryser-Chowla theorem, which groups \(G\) of order \(v\) contain a nontrivial \((v, k, \lambda)\)-difference set?

(2) If \(G\) contains a nontrivial \((v, k, \lambda)\)-difference set, how many inequivalent \((v, k, \lambda)\)-difference sets are there?
These two problems are far from being resolved despite a large body of literature. The methods to attack problem (1) usually involve nonexistence proofs and explicit constructions which we will use very often in the later chapters. Problem (2) is more difficult than Problem (1), there are only a few results related to Problem (2) at present.

2. Group Rings and Characters

As we will soon see, the group ring provides a natural and convenient setting for studying abelian difference sets, and character theory is a powerful tool to attack problem (1) in the last section. Here we collect some basic facts about group rings and characters.

Let $R$ be a commutative ring with identity and $G$ a finite group written multiplicatively. Then elements of the group ring $R[G]$ are all formal sums $A = \sum_{g \in G} a_g g$, where $a_g \in R$ for each $g \in G$. We define addition and scalar multiplication in the obvious way:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g)g$$

$$c \sum_{g \in G} a_g g = \sum_{g \in G} ca_g g$$

Multiplication in $R[G]$ is defined by

$$(\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{g \in G} (\sum_{g=hh'} a_h b_{h'}) g$$

With these definitions, $R[G]$ is a commutative, associative $R$-algebra. We will use $Z[G]$ most of the time, where $Z$ is the set of all integers. For a subset $S \subset G$, we will identify it with the corresponding group ring element $S = \sum_{s \in S} s$. For
\[ A = \sum_{g \in G} a_g g \in \mathbb{Z}[G], \] we define \( A^{(-1)} = \sum_{g \in G} a_g g^{-1} \). So for a \( k \)-subset \( D \) of a group \( G \) of order \( v \), \( D \) is a \((v, k, \lambda)\)-difference set in \( G \) if and only if

\[ DD^{(-1)} = n1_G + \lambda G \]  

holds in the group ring \( \mathbb{Z}[G] \), where \( n = k - \lambda \) is called the order of the difference set.

Let \( G \) be an abelian group. A character \( \chi \) of \( G \) is a homomorphism from \( G \) to the multiplicative group of complex roots of unity. If \( e_G \) is the exponent of \( G \) (i.e., the order of the largest cyclic subgroup of \( G \)), then \( \chi(g), g \in G \), are \( e_G \)-th root of unity. It is well-known that under termwise multiplication the set of characters of \( G \) form a group which is isomorphic to \( G \). This group is called the character group of \( G \) and will be denoted by \( G^* \). The identity of \( G^* \) is the principal character \( \chi_0 \) that maps every element of \( G \) to 1. The orthogonality relations are

\[ \sum_{\chi \in G^*} \chi(g) = \begin{cases} v, & \text{if } g = 1_G; \\ 0, & \text{otherwise}. \end{cases} \]  

\[ \sum_{g \in G} \chi(g) = \begin{cases} v, & \text{if } \chi = \chi_0; \\ 0, & \text{otherwise}. \end{cases} \]  

The characters of \( G \) can be extended linearly to the group ring \( \mathbb{Z}[G] \):

\[ \chi\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \chi(g), \chi \in G^*. \]  

If \( u \) is the order of \( \chi \), then \( \chi \) defines a ring homomorphism from \( \mathbb{Z}[G] \) onto \( \mathbb{Z}[e^{2\pi i/u}] \), the ring of integers of \( Q(e^{2\pi i/u}) \).

The following result is known as inversion formula which will be used many times in the future.
Theorem 1.2.1. Let $G$ be a finite abelian group of order $v$ and let $A = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$. Then for each $g \in G$, $a_g = \frac{1}{v} \sum_{\chi \in G^*} \chi(A) \chi(g^{-1})$.

The proof of the inversion formula follows readily from the orthogonality relations. It shows that $A$ is uniquely determined by $\chi(A)$, $\chi \in G^*$.

We remark that when $G$ is non-abelian, there is also an inversion formula which includes Theorem 1.2.1 as a corollary, we refer the reader to Serre [SE] for that formula.

Using the inversion formula, we have the following basic result in difference sets.

Theorem 1.2.2. Let $D$ be a $k$-subset of an abelian group $G$ of order $v$. Then $D$ is a $(v, k, \lambda)$-difference set if and only if

$$\chi(D)\overline{\chi(D)} = k - \lambda \quad (1.2.4)$$

for all nonprincipal characters $\chi$ of $G$.

Proof: $\Rightarrow$: If $D$ is a $(v, k, \lambda)$-abelian difference set, then (1.2.1) holds. Applying any nonprincipal character $\chi$ to (1.2.1), by the orthogonality relation, we have $\chi(D)\overline{\chi(D)} = k - \lambda$.

$\Leftarrow$: Let $DD^{(-1)} = \sum_{g \in G} a_g g$. By inversion formula,

$$a_g = \frac{1}{v} \sum_{\chi \in G^*} \chi(DD^{(-1)}) \chi(g^{-1}) = \frac{1}{v} (k^2 + (k - \lambda) \sum_{\chi \neq \chi_0} \chi(g^{-1})).$$

If $g = 1_G$, then $a_g = k$. If $g \neq 1_G$, then $a_g = \frac{1}{v} (k^2 - (k - \lambda)) = \lambda$. Hence $DD^{(-1)} = k - \lambda + \lambda G$. Therefore $D$ is a $(v, k, \lambda)$-difference set in $G$. This completes the proof. $\square$

Although this work is mainly about abelian difference sets, sometimes it is possible to extend the theory to nonabelian case with some extra condition.
For this purpose, we introduce the following definitions and recall several results in this respect.

Let $G$ be a finite group (not necessarily abelian) of order $v = mn$, $N$ a normal subgroup of $G$ of order $n$, $Irr_G = \{ \chi : \chi \text{ is an irreducible complex character of } G \}$, $IRR(CG) = \{ V : V \text{ is an irreducible } CG\text{-module} \}$, where $C$ is the field of complex numbers. $Irr_N$, $IRR(CN)$ are similarly defined. Given $\theta \in Irr_N$, $W \in IRR(CN)$, we set $Irr(G|\theta) = \{ \chi \in Irr_G : (\chi_N, \theta)_N \neq 0 \}$, $IRR(CG|W) = \{ V \in IRR(CG) : W|V_N \}$, where $(\chi_N, \theta)_N = \frac{1}{|N|} \sum_{h \in N} \chi_N(h)\theta(h^{-1})$ and $W|V_N$ means that $W$ is a direct summand of $V_N$. Assume that $\theta_0$ is the trivial character of $N$, and $W_0$ is the 1-dim trivial representation of $N$. We have

**Lemma 1.2.4.** (1) $IRR(CG/N) = IRR(CG|W_0)$.

(2) $Irr(G/N) = Irr(G|\theta_0)$.

**Proof:** We will prove (1), (2) is an immediate consequence of (1). Let $V \in IRR(CG|W_0)$. By Clifford theory (see [NT], page 202), we have

$$V_N \cong e \cdot W_0, \quad (1.2.5)$$

where $e = \text{dim}_C V$. Hence $N$ acts trivially on $V$, therefore $V$ is a $CG/N$-module.

If $W$ is a proper $CG/N$-submodule of $V$, then let $N$ act trivially on $W$, so $W$ is a proper $CG$-submodule of $V$, this contradicts that $V$ is an irreducible $CG$-module. Hence $V$ is an irreducible $CG/N$-module. Conversely, if $V \in IRR(CG/N)$, and the corresponding representation is $\rho : G/N \to GL(V)$. We can extend the definition of $\rho$ to $G$ and get a representation $\rho'$ of $G$ as follows: Given $g \in G$, define $\rho'(g) = \rho(gN)$. Then $\rho'(gh) = \rho(gN) = \rho(gN \cdot hN) = \rho(gN)\rho(hN) = \rho'(g)\rho'(h)$. This makes $V$ into a $CG$-module, and $N$ acts trivially on it. Also it
is easy to see that $V$ is irreducible. Hence $V \in \text{IRR}(CG[W_0])$. This completes the proof. □

We also need the following result in the future.

**Lemma 1.2.5.** For any $\chi \in \text{Irr} G$, the map $\omega : CG \to \mathcal{C}$ via $g \mapsto \frac{\chi(g)}{\chi(1)}$ is a $\mathcal{C}$-algebra homomorphism from the center of $CG$ to $\mathcal{C}$. If $A \in \text{Cent}(CG)$ and $g \in G$, then $\omega(Ag) = \omega(A)\omega(g)$.

**Proof:** The first part of this lemma is standard, for example see Serre [SE]. We prove the second part of the lemma as follows. First we show that if $g = aha^{-1}, h, a \in G$, then $\omega(gA) = \omega(hA)$. To see this, one notes that $\omega(gA) = \frac{\chi(gA)}{\chi(1)} = \frac{\chi(aha^{-1}A)}{\chi(1)} = \frac{\chi(hA)}{\chi(1)} = \omega(hA)$. Let $C$ be the conjugacy class containing $g$. Then $\omega(CA) = |C|\omega(gA)$. On the other hand, $\omega(CA) = \omega(C)\omega(A) = |C|\omega(g)\omega(A)$. Hence $\omega(gA) = \omega(g)\omega(A)$. This completes the proof. □

### 3. Background in Algebraic Number Theory

From (1.2.4), we see that abelian difference sets are intimately connected with the factorization of $n = k - \lambda$ in some cyclotomic field. Hence algebraic number theory has found many applications in difference sets. In this section, we review some basic results in algebraic number theory. The proofs of the theorems stated below can be found in standard text books of number theory, for example, [WE], [MAR].

Let $L/K$ be a finite extension of number fields, and $O_L, O_K$ be the integer rings of $L$ and $K$ respectively. Given a prime $\wp$ in $O_K$, we write $\wp O_L = \pi_1^{e_1}\pi_2^{e_2} \cdots \pi_g^{e_g}$, $e_i \geq 1$, $g \geq 1$, where $\pi_i$'s are distinct prime ideals in $O_L$. $e_i$
is called the ramification index of $\pi_i$, and will be denoted by $e_i = e(\pi_i|\wp)$, $f_i = f(\pi_i|\wp) = [O_L/\pi_i : O_K/\wp]$ is called the residue degree. It is well-known that
\[\sum_{i=1}^g e_i f_i = [L : K].\]
We say that $\wp$ splits completely if $e_1 = e_2 = \cdots = e_g = 1$, and $f_1 = f_2 = \cdots = f_g = 1$.

**Theorem 1.3.1.** Let $K \subset M \subset L$ denote a tower of finite number field extensions, and let $\wp$, $\pi$, $P$ be prime ideals in $O_K$, $O_M$, $O_L$ respectively with the property that $P|\pi|\wp$. Then $e(P|\wp) = e(P|\pi)e(\pi|\wp)$, $f(P|\wp) = f(P|\pi)f(\pi|\wp)$.

Assuming that $L/K$ is Galois, and letting $GalL/K = G$, we have

**Theorem 1.3.2.**
1. $G$ acts transitively on $\{\pi_1, \pi_2, \cdots, \pi_g\}$.
2. $e_i = e_j$ and $f_i = f_j$ for all $i, j$. Therefore we set $e = e(\wp) := e_1$, $f = f(\wp) := f_1$.

Let $\pi$ be one of those $\pi_i$'s. Then
1. $D(\pi|\wp) = \{ \alpha \in GalL/K : \alpha(\wp) = \wp \}$ is called the decomposition group of $\pi$ over $\wp$.
2. $I(\pi|\wp) = \{ \alpha \in GalL/K : \alpha(x) \equiv x (mod \pi) \}$ is called the inertia group of $\pi$ over $\wp$.
3. The fixed field $Z = Z(\pi|\wp)$ of $D(\pi|\wp)$ is called the decomposition field, the fixed field $T = T(\pi|\wp)$ of $I(\pi|\wp)$ is called the inertia field of $\pi|\wp$.

With the notations as above, we have

**Theorem 1.3.3.**
1. The decomposition group $D(\pi|\wp)$ has order $e(\pi|\wp)f(\pi|\wp)$.
2. The inertia group $I(\pi|\wp)$ is a normal subgroup of $D(\pi|\wp)$ of order $e(\pi|\wp)$. 
(3) The residue class extension $O_L/\pi$ over $O_K/\wp$ is a Galois extension. Any automorphism $\alpha \in D(\pi|\wp)$ induces an automorphism $\bar{\alpha}$ of $O_L/\pi$ over $O_K/\wp$ by setting $\bar{\alpha}(x + \pi) = \alpha(x) + \pi$ for $x \in O_L$. The mapping from $D(\pi|\wp)$ to the Galois group of $O_L/\pi$ over $O_K/\wp$ via $\alpha \mapsto \bar{\alpha}$ is a surjective homomorphism whose kernel is the inertia group $I(\pi|\wp)$.

We are particularly interested in the decomposition of a rational prime $p$ in the cyclotomic field $Q(\xi_d)$, where $\xi_d$ is a primitive $d$-th root of unity, and its decomposition group. Let $(a, b)$ denote the greatest common divisor of two integers $a, b$. We quote the following theorem.

**Theorem 1.3.4.** Let $p$ be a rational prime integer.

1. If $d = p^e$, the ideal $(p)$ in $Q(\xi_d)$ decomposes as $(p) = \pi^{\phi(d)}$, where $\pi$ is the principal ideal $(1 - \xi_d)$ and $\phi(d)$ is the Euler phi-function. Also $D(\pi|p) = \text{Gal}Q(\xi_d)/Q$.

2. If $(d, p) = 1$, the ideal $(p)$ in $Q(\xi_d)$ decomposes as $(p) = \pi_1 \pi_2 \cdots \pi_g$, where $\pi_i$ are distinct prime ideals, $g = \phi(d)/f$, $f = \text{ord}_d(p)$. Furthermore $D(\pi_1|p) = D(\pi_2|p) = \cdots = D(\pi_g|p)$. Let $D_p = D(\pi_i|p)$. We have $D_p = \langle \xi_d \mapsto \xi_d^{p^f} \rangle$, which is a cyclic group of order $f$.

3. Suppose that $d = p^e d'$ with $(p, d') = 1$. Then the ideal $(p)$ in $Q(\xi_d)$ decomposes as $(p) = (\pi_1 \pi_2 \cdots \pi_g)^{\phi(p^f)}$ where $\pi_i$ are distinct prime ideals, $g = \phi(d')/f$, $f = \text{ord}_{d'}(p)$. Furthermore $D(\pi_1|p) = D(\pi_2|p) = \cdots = D(\pi_g|p)$. Let $D_p = D(\pi_i|p)$. We have $D_p = \{ \xi_d \mapsto \xi_{d'}^t | t = p^f + yd', 0 \leq x \leq f - 1, 1 \leq y \leq p^f - 1, (y, p) = 1 \}$.

The following theorem is usually called Kummer's theorem.

**Theorem 1.3.5** Let $L/K$ be a number field extension, $O_L, O_K$ be their
integer rings respectively, and let $[L : K] = m$, $L = K(\alpha)$, $\alpha \in O_L$. Assume $f(X)$ is the minimal polynomial of $\alpha$, fix a prime ideal $\wp$ of $O_K$, and use $\overline{f(X)}$ to denote the corresponding polynomial in $O_K/\wp[X]$ obtained by reducing the coefficients of $f(X)$ mod $\wp$. If $\overline{f(X)}$ has the following canonical factorization in $O_K/\wp[X]$

$$\overline{f(X)} = \overline{g_1(X)}^{e_1} \overline{g_2(X)}^{e_2} \cdots \overline{g_h(X)}^{e_h} \quad (1.3.1)$$

and $p \nmid |O_L/O_K[\alpha]|$, where $p$ is the prime of $\mathbb{Z}$ lying under $\wp$. Then we have the following prime ideal decomposition of $\wp O_L$.

$$\wp O_L = \pi_1^{e_1} \pi_2^{e_2} \cdots \pi_h^{e_h} \quad (1.3.2)$$

where $\pi_i = (\wp, g_i(\alpha))$, $f(\pi_i/\wp) = \deg(g_i)$, $1 \leq i \leq h$.

4. Finite Fields, Cyclotony

Finite fields, especially the cyclotomy of finite fields, are very useful in the construction of difference sets. There are several detailed accounts of this topic available (see Storer [ST], also Baumert [BA] and Hall [HA]). Here we give a brief introduction to this subject.

Let $p$ be a prime and let $q$ be a power of $p$. Then there exists a field $GF(q)$ of $q$ elements, and this is essentially unique. Let $g$ be a fixed primitive element of $GF(q)$, so that any nonzero element of $GF(q)$ can be written uniquely in the form $g^i$, where $0 \leq i \leq q - 2$. Let $e$ be any divisor of $q - 1$, $e \geq 2$, and let $f = \frac{q-1}{e}$. The $e$-th cyclotomic classes $C_0, C_1, \cdots, C_{e-1}$ are defined by

$$C_i = \{g^{et+i} : t = 0, 1, 2, \cdots, f - 1\} \quad (1.4.1)$$
for $i = 0, 1, 2, \ldots, e - 1$.

Let $\xi_p = exp(2\pi i/p)$ be a primitive $p$-th root of unity, $Tr$ be the trace map, $Tr : GF(q) \rightarrow GF(p)$. The cyclotomic periods $\eta_i$ are given by

$$\eta_i = \sum_{x \in C_i} \xi_p^{Tr(x)}$$

(1.4.2)

for $i = 0, 1, 2, \ldots, e - 1$. When $k \geq e$, the subscripts in $C_k$ and $\eta_k$ are to be interpreted modulo $e$.

Explicit determinations of cyclotomic periods are usually very difficult for large $e$. But in one case, i.e. when $-1$ is a power of the characteristic $p$ modulo $e$, the cyclotomic periods can be easily calculated (This case is referred to as uniform cyclotomy in [BMW] which contains a detailed discussion on this subject). We find it more convenient to use the following theorem from [MY].

**Theorem 1.4.1.** Assume there exists a positive integer $j$ such that $p^j \equiv -1 (mod e)$, and assume $j$ is the smallest such integer. Let $q = p^\alpha$ with $\alpha = 2j\gamma$. Then the cyclotomic periods are given by

1. If $\gamma, p, \frac{p^\gamma + 1}{e}$ are all odd, then

$$\eta_i = \frac{(e - 1)p^{i\gamma} - 1}{e}, \eta_i = \frac{-1 - p^{j\gamma}}{e}, i \neq e/2$$

(1.4.3)

2. In all other cases

$$\eta_0 = \frac{-1 - (-1)^{\gamma}(e - 1)p^{j\gamma}}{e}, \eta_i = \frac{(-1)^{\gamma}p^{j\gamma} - 1}{e}, i \neq 0$$

(1.4.4)

Now let us review some basic facts about additive characters of $GF(q)$. We will use $G$ to denote the additive group of $GF(q)$. The function defined by
$\chi_1(c) = \xi_p^{Tr(c)}$ for all $c \in GF(q)$ is a character of $G$, since for $c_1, c_2 \in GF(q)$, we have $Tr(c_1 + c_2) = Tr(c_1) + Tr(c_2)$, and so $\chi_1(c_1 + c_2) = \chi_1(c_1)\chi_1(c_2)$. Instead of "character of the additive group of $GF(q)$", we shall use the term additive character of $GF(q)$. The character $\chi_1$ is called the canonical additive character of $GF(q)$. All additive characters of $GF(q)$ can be expressed in terms of $\chi_1$.

**Theorem 1.4.2.** For $b \in GF(q)$ the function $\chi_b$ with $\chi_b(c) = \chi_1(bc)$ for all $c \in GF(q)$ is an additive character of $GF(q)$, and every additive character is obtained in this way.

**Proof:** For $c_1, c_2 \in GF(q)$, we have

$$\chi_b(c_1 + c_2) = \chi_1(bc_1 + bc_2) = \chi_1(bc_1)\chi_1(bc_2) = \chi_b(c_1)\chi_b(c_2),$$

(1.4.5)

and the first part is established. Since $Tr$ map is surjective, $\chi_1$ is a nonprincipal character. Therefore, if $a, b \in GF(q)$ with $a \neq b$, then

$$\frac{\chi_a(c)}{\chi_b(c)} = \frac{\chi_1(ac)}{\chi_1(bc)} = \chi_1((a - b)c) \neq 1$$

(1.4.6)

for suitable $c \in GF(q)$, so $\chi_a$ and $\chi_b$ are distinct characters. Hence if $b$ runs over $GF(q)$, we get $q$ distinct characters $\chi_b$. On the other hand we know that $GF(q)$ has exactly $q$ additive characters, so the list of additive characters of $GF(q)$ is already complete. □

In fact the map $b \mapsto \chi_b$ is an isomorphism $G \to G^*$, where $G^*$ is the character group of $G = (GF(q), +)$. The trivial character is $\chi_0$. Using the inversion formula, it is easy to prove the following two lemmas.

**Lemma 1.4.3.** If $H$ is a subgroup of $G$, $|H| \geq 2$, then $\sum_{h \in H} \chi_\beta(h) = 0$ if $H \not\subseteq \{x \in G | Tr(\beta x) = 0\}$. 
Lemma 1.4.4. Let $A = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$. $\chi_{\beta}(A) = 0$ for all $\beta \neq 0$ if and only if $A = aG$ for some integer $a$.

We also need the following result about quadratic forms over $GF(p)$, where $p$ is an odd prime. Let $s$ be a positive integer. Given $\beta \in GF(p^{2s})$, $\beta \neq 0$, the map $Q(x) = Tr(\beta x^{1+p^s})$, for all $x \in GF(p^{2s})$ defines a quadratic form over $GF(p)$. The corresponding bilinear form is given by $B(x, y) = Tr(\beta x^{p^s} y + \beta xy^{p^s})$ for all $x, y \in GF(p^{2s})$. Let $V = GF(p^{2s})$, which is viewed as a vector space of dimension $2s$ over $GF(p)$. $Rad V = \{ y \in V : B(x, y) = 0 \text{ for all } x \in V \}$, we have the following lemma.

Lemma 1.4.5. If $\beta^{p^s-1} \neq -1$, then $Rad V = \{0\}$, if $\beta^{p^s-1} = -1$, then $Rad V = V$.

Proof. If $y \in GF(p^{2s}), y \neq 0$, then

$$Tr(\beta xy^{p^s} + \beta x^{p^s} y) = 0 \text{ for all } x \in V$$

$\Rightarrow$$Tr(\beta^{p^s} x^{p^s} y + \beta x^{p^s} y) = 0 \text{ for all } x \in V$

$\Rightarrow$$Tr((\beta^{p^s} y + \beta y)x^{p^s}) = 0 \text{ for all } x \in V$

$\Rightarrow$$\beta^{p^s} y + \beta y = 0 \Rightarrow \beta^{p^s-1} = -1$

Therefore if $\beta^{p^s-1} = -1$, then $Rad V = V$, and if $\beta^{p^s-1} \neq -1$, then $Rad V = \{0\}$. This completes the proof of the lemma. □

5. Codes and Point Sets in Projective Geometry

Let $q = p^a$, where $p$ is a prime, and $GF(q)$ be the finite field with $q$ elements. If $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ are vectors in $GF(q)^n$, then the dot product is defined to be $u \cdot v = \sum_{i=1}^n u_i v_i$. An $[n, k]$-code $C$ over $GF(q)$ is a $k$-dim subspace of $GF(q)^n$. Vectors in $C$ are called codewords. The
dual code is $C^\perp = \{ v \in GF(q)^n : v \cdot x = 0 \text{ for all } x \in C \}$, $C^\perp$ is an $[n, n-k]$-code.

The weight $wt(x)$ of a vector $x$ in $GF(q)^n$ is the number of nonzero entries. The weight enumerator $W_C(x, y)$ of $C$ is the polynomial

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

(1.5.1)

where $A_i$ is the number of codewords of weight $i$.

The MacWilliam identities relate the weight enumerator of $C$ to that of $C^\perp$ as follows

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q - 1)y, x - y).$$

(1.5.2)

A two (resp. three)-weight code is a code for which $|\{ i : i \neq 0, A_i \neq 0 \}| = 2$ (resp. 3). Two-weight codes are related to strongly regular graphs and partial difference sets, they have been studied extensively, we refer the reader to a paper by Calderbank and Kantor [CK] for a survey.

The distance $d(x, y)$ between two vectors $x, y$ in $GF(q)^n$ is the number of entries where they differ. Thus $d(x, y) = wt(x - y)$ and the minimum distance between two codewords is the minimum weight among all non-zero codewords. A code $C$ is said to be an $[n, k, d]$-code if $d$ is the minimum non-zero weight in $C$. If $d = 2e + 1$, then $C$ is called an $e$-error-correcting code.

Given an $[n, k]$-code $C$ over $GF(q)$, let $G$ be a $k \times n$ generating matrix of $C$, i.e. the rows of $G$ are a basis of the vector space $C$, let $g_1, g_2, \ldots, g_n$ be the columns of $G$. Identifying $g_i$ with the linear form $h \mapsto h \cdot g_i$, where $h \in GF(q)^k$, we shall call $\Omega = \{g_1, g_2, \ldots, g_n\}$ the set of coordinate forms of $C$ associated with the generator matrix $G$. Thus any codeword $c \in C$ is given by

$$c = c(h) = (h \cdot g_1, h \cdot g_2, \ldots, h \cdot g_n), \quad h \in GF(q)^k$$

(1.5.3)
Since $\text{dim}(C) = k$ the vectors $g_1, g_2, \cdots, g_n$ span $GF(q)^k$. If no two of the vectors $g_1, g_2, \cdots, g_n$ are dependent, then $C$ is said to be projective. Thus $C$ is projective if and only if the minimum weight in the dual code $C^\perp$ is at least 3.

An $n \times n$ monomial matrix $M$ is a matrix of the form $M = DP$, where $D$ is an $n \times n$ diagonal matrix and $P$ is an $n \times n$ permutation matrix. Two $[n, k]$-codes $C$ and $C'$ over $GF(q)$ are said to be equivalent if there exists an $n \times n$ monomial matrix $M$ such that $MC = C'$. Note that monomial transforms are precisely those linear transformations that preserve the metric $d(x, y)$ on $GF(q)^n$.

A projective $(n, k, h_1, h_2, h_3)$ set $\Omega$ is a proper, non-empty set of $n$ points of the projective space $PG(k - 1, q)$ with the property that every hyperplane meets $\Omega$ in $h_1$ points, or $h_2$ points, or $h_3$ points.

Given a point set $\Omega = \{< g_1 >, < g_2 >, \cdots, < g_n >\}$ in $PG(k - 1, q)$, the subspace $C(\Omega)$ generated by the rows of a matrix whose column set is $\Omega$ is called the projective code associated to $\Omega$. The code $C(\Omega)$ is only defined up to equivalence.

The following proposition tells us that projective $(n, k, h_1, h_2, h_3)$ sets and projective 3-weight codes are equivalent.

**Proposition 1.5.1.** If the code $C$ defined by (1.5.3) is a projective 3-weight $[n, k]$ code with weights $w_1, w_2, w_3$, then $\{< g_i > \mid i = 1, 2, \cdots, n\}$ is a projective $(n, k, n - w_1, n - w_2, n - w_3)$ set that spans $PG(k - 1, q)$. Conversely, if $\Omega = \{< g_i > \mid i = 1, 2, \cdots, n\}$ is a projective $(n, k, n - w_1, n - w_2, n - w_3)$ set that spans $PG(k - 1, q)$ then the code $C(\Omega)$ defined by (1.5.3) is a projective
3-weight \([n,k]\) code with weights \(w_1, w_2, w_3\).

**Proof:** Let \(h\) be any non-zero vector in \(GF(q)^k\). If \(h^\perp = \{y \in GF(q)^k | h \cdot y = 0\}\). Then

\[
wt(c(h)) = n - |h^\perp \cap \{g_1, g_2, \cdots, g_n\}|
\]

(1.5.4)

The results now follow immediately. □

**Remark:** For \(h \in GF(q)^k\), we can define an additive character of \(GF(q)^k\) as follows. \(\chi_h : x \mapsto \xi_p^{Tr(h \cdot x)}\), for all \(x \in GF(q)^k\), where \(\xi_p\) is a primitive \(p\)-th root of unity, and \(Tr\) is the trace map from \(GF(q)\) to \(GF(p)\). If we let \(\overline{\Omega} = \bigcup_{i=1}^n GF(q)^* g_i\), then for any nonprincipal additive character \(\chi_h\) of \(GF(q)^k\), we have

\[
\chi_h(\overline{\Omega}) = (q - 1)(n - wt(c(h))) + (-1)^{wt(c(h))} = (q - 1)n - wt(c(h))q.
\]

(1.5.5)

From this formula and the proof of Proposition 1.5.1, we see that the character values of \(\overline{\Omega}\), the weights of codewords \(c(h), h \in GF(q)^k\), and the size of \(h^\perp \cap \{g_1, g_2, \cdots, g_n\}\) are closely related. We will use these connections in Chapter IV.
Chapter II
Multipliers of Difference Sets

1. Multiplier Theorems

Let $G$ be an abelian group of order $v$, and $D$ a subset of $G$. An automorphism $\alpha$ of $G$ is called a multiplier of $D$ if $\alpha(D) = \sum_{d \in D} \alpha(d) = Dg$ for some $g \in G$. For any integer $t$, $(t, e_G) = 1$, where $e_G$ is the exponent of $G$, the mapping $x \mapsto x^t$, $x \in G$ is an automorphism of $G$, if it happens to be a multiplier of $D$, then it is called a numerical multiplier of $D$. Usually we just say that $t$ is a multiplier of $D$. It is easy to see that the set $M$ of all numerical multipliers of $D$ forms a group, which can be viewed as a subgroup of $(\mathbb{Z}/(e_G))^*$, the group of units of the ring $\mathbb{Z}/(e_G)$.

The concept of multiplier was first introduced by Hall [HA1] for cyclic projective planes. This ingenious discovery is very useful for both construction and nonexistence proof of difference sets. Since the appearance of Hall’s fundamental multiplier theorem for cyclic projective planes, there have been quite a few generalizations. For example, Chowla and Ryser [CR], also Hall and Ryser [HR] proved the so called first multiplier theorem which can be stated as follows.
Theorem 2.1.1. (First Multiplier Theorem) Let $D$ be a $(v, k, \lambda)$ difference set in an abelian group $G$, and let $p$ be a prime dividing $n := k - \lambda$ but not $v$. If $p > \lambda$, then $p$ is a multiplier of $D$.

From this theorem, we can see that very often the parameters of an abelian difference set $D$ force the existence of numerical multipliers which then can be used to help with either the construction or a nonexistence proof of the difference set. This shows the importance of the above theorem. In the application of Theorem 2.1.1, the following theorem due to McFarland and Rice is often used.

Theorem 2.1.2. Let $D$ be an abelian $(v, k, \lambda)$-difference set in $G$. Then there exists a translate of $D$ that is fixed by every numerical multiplier of $D$.

We refer the reader to [MR] for the proof of this theorem.

Example 2.1.1. We consider the existence question for a $(37, 9, 2)$-difference set $D$. Since 37 is a prime, we necessarily have $G = \mathbb{Z}_{37}$. Also, 7 has to be a multiplier by Theorem 2.1.1. Now, the subgroup of $G$ generated by 7 is $M = \{1, 7, 12, 10, 33, 9, 26, 34, 16\}$. Thus, up to equivalence, the only possible choice for $D$ is $D = M$. It is easily checked that this indeed works. We remark that this is the first nontrivial difference set in the family of biquadratic residue difference sets with parameters $(4x^2 + 1, x^2, \frac{x^2 - 1}{4})$, where $4x^2 + 1$ is a prime, $x$ is odd (see [BA]).

All known examples of abelian difference sets admit every prime divisor of $n$ as a multiplier, whether or not $p > \lambda$. This leads to the following long-standing conjecture.
The Multiplier Conjecture: The first multiplier theorem holds without the assumption $p > \lambda$.

Menon [ME] and Mann [MAH] [MAN] proved the following theorem which can be viewed as an attempt to resolve the above conjecture.

Theorem 2.1.3. (Second Multiplier Theorem) Let $D$ be an abelian $(v, k, \lambda)$-difference set in $G$, and let $m > \lambda$ be a divisor of $n$ which is co-prime to $v$. Moreover, let $t$ be an integer co-prime with $v$ satisfying the following condition: For every prime $p$ dividing $m$ there exists a nonnegative integer $f$ with $t \equiv p^f \pmod{e_G}$, where $e_G$ is the exponent of $G$. Then $t$ is a numerical multiplier of $D$.

McFarland [MC] defined an integral valued function $M(m), m \in N$, the set of positive integers, to obtain conditions for trivial solutions to the equation $F^{(-1)}F = m^2, F \in ZG$, which is also an attempt to resolve the multiplier conjecture. Qiu [QI] recently made some progress on the multiplier conjecture by partially improving McFarland's results.

Lander [LA] and also Arasu and Ray-Chaudhuri [AR] also proved a multiplier theorem for difference lists, which loosely speaking, are difference sets with possibly repeated elements. Jungnickel [JU] has given a simplified proof for that theorem.

An interesting generalization of difference set is divisible difference set, it can be defined as follows. Let $G$ be a finite group of order $v = mn$ with a normal subgroup $N$ of order $n$. A $k$-element subset $D$ of $G$ is called an $(m, n, k, \lambda_1, \lambda_2)$-divisible difference set in $G$ relative to $N$ if

$$DD^{(-1)} = k - \lambda_1 + \lambda_1N + \lambda_2(G - N) \text{ in } Z[G]. \quad (2.1.1)$$
If $\lambda_1 = 0$, then $D$ is called a relative difference set. When $N = \{1\}$, or $N = G$, or $\lambda_1 = \lambda_2$, then $D$ is just an ordinary difference set.

There are several generalizations of the first multiplier theorem to the divisible difference set case, these include Hoffman’s multiplier theorem for affine difference sets [H], Elliot and Butson’s multiplier theorem for relative difference sets [EB], and Ko and Ray-Chaudhuri’s multiplier theorem [KR] for elements of a group ring.

A multiplier theorem for $(m, n, k, 0, 1)$-relative difference sets by Ganley and Spence [GS] is of particular interest when $(mn, k) > 1$. Lam [L] generalized Ganley and Spence’s result to arbitrary $\lambda$.

Finally we mention that Ott [O] generalized the second multiplier theorem to non-abelian case but required $D$ to be central (i.e. $D$ is a union of some conjugacy classes of $G$).

In this section, we will prove a multiplier theorem for central elements of a group ring which generalizes most previously known multiplier theorems. Our multiplier theorem is substantially a generalization and improvement of Ganley, Spence and Lam’s results. The important thing here is, besides making use of the Frobenius automorphism, we also make use of automorphisms in another decomposition group. Our multiplier theorem also gives new multilpiers for some $(v, k, \lambda)$-difference sets with $(n, v) > 1$.

We begin with the following lemma. Before stating the lemma, we fix the following notation. $G$ is a finite group of order $mn$, $N$ a normal subgroup of $G$ of order $n$. $\text{Cent}(CG)$ is the center of the group algebra $CG$. We also remind the reader the following definitions and notation which were introduced
in Section 3 of Chapter I. \( \text{Irr}G = \{ \chi : \chi \text{ is an irreducible complex character of } G \} \), \( \text{Irr}(G|\theta_0) = \{ \chi \in \text{Irr}G : (\chi_N, \theta_0)_N \neq 0 \} \), where \( \theta_0 \) is the trivial character of \( N \) (see Section 3 of Chapter I for the definition of \((\chi_N, \theta_0)_N\)).

**Lemma 2.1.4.** If \( A \in \text{Cent}(CG) \), \( k_1 \) is a rational integer, \((k_1, mn) = a_1\), \( \chi_0 \) is the trivial character of \( G \),

\[
\begin{align*}
\chi_0(A) &\equiv bn + vc \pmod{k_1} \\
\chi(A) &\equiv bn\chi(1) \pmod{k_1} \text{ if } \chi \in \text{Irr}(G|\theta_0) \setminus \{\chi_0\}, \\
\chi(A) &\equiv 0 \pmod{k_1} \text{ if } \chi \in \text{Irr}G \setminus \text{Irr}(G|\theta_0),
\end{align*}
\]

then \( A = bN + cG + \frac{k_1}{a_1}F \), for some \( F \in CG \).

**Proof:** Assume that \( A = \sum_{g \in G} a_g g \in \text{Cent}(CG) \), by inversion formula, we have

\[
mna_g = \sum_{\chi \in \text{Irr}G} \chi(1)\chi(Ag^{-1}). \tag{2.1.2}
\]

By Lemma 1.2.5, and the assumption that \( A \) is central, one has

\[
mna_g = \sum_{\chi \in \text{Irr}G} \chi(A)\chi(g^{-1}) = bn + cv + \sum_{\chi \in \text{Irr}(G|\theta_0) \setminus \{\chi_0\}} bn\chi(1)\chi(g^{-1}) \pmod{k_1}
\]

If \( g \in N \), then \( \chi(g^{-1}) = \chi(1) \) for each \( \chi \in \text{Irr}(G|\theta_0) \). So

\[
mna_g = bn + cv + bn \sum_{\chi \in \text{Irr}(G|\theta_0) \setminus \{\chi_0\}} \chi(1)^2 \pmod{k_1} \tag{2.1.3}
\]

By Lemma 1.2.4, \( \text{Irr}(G|\theta_0) = \text{Irr}(G/N) \), so \( \sum_{\chi \in \text{Irr}(G|\theta_0)} \chi(1)^2 = |G/N| = m \).

Hence

\[
mna_g \equiv (b + c)mn \pmod{k_1} \tag{2.1.4}
\]
\[ a_g \equiv b + c \pmod{\frac{k_1}{a_1}} \] (2.1.5)

If \( g \notin N \), then \( g^{-1}N \neq N \). Notice that \( Irr(G|\theta_0) = Irr(G/N) \), by orthogonality relation, we have

\[ \sum_{\chi \in Irr(G|\theta_0)} \chi(1)\chi(g^{-1}) = \sum_{\chi \in Irr(G/N)} \chi(1)\chi(g^{-1}) = 0. \] (2.1.6)

Hence

\[ mna_g \equiv cmn \pmod{k_1} \]

\[ a_g \equiv c \pmod{\frac{k_1}{a_1}} \] (2.1.7)

Therefore, \( A = bN + cG + \frac{k_1}{a_1} F \), for some \( F \in CG \). The proof is completed. \( \square \)

**Lemma 2.1.5.** Let \( A, B \in ZG \), and \( A, B \in Cent(CG) \). If

\[
AA^{(-1)} = a + bN + cG, \\
BB^{(-1)} = a + bN + cG, \\
A^{(-1)}B = bg_1N + cG + k_2F, \\
BN = g_1AN, \] where \( g_1 \in G, k_2|a, a \neq 0, \)

\[ \chi_0(A) = \chi_0(B), \]

and one of the following conditions is satisfied:

1. All coefficients of \( A \) and \( B \) are nonnegative, \( k_2 > b + c, k_2 > c \).
2. \( (M(\frac{n}{k_1}), v) = 1 \), where \( M(m) \) is defined as follows: \( M(2) = 2 \cdot 7, M(3) = 2 \cdot 3 \cdot 11 \cdot 13, M(4) = 2 \cdot 3 \cdot 7 \cdot 31 \) and recursively, \( M(z) \) for \( z \geq 5 \) is the product of the distinct prime divisors of the numbers \( z, M(\frac{z^2}{p^v}), p - 1, p^{v_2} - 1, \ldots, p^{u(z)} - 1 \), where \( p \) is a prime dividing \( m \) with \( p^v || m \) and \( u(z) = \frac{z^2 - z}{2} \).

Then \( B = Ag_2, g_2 \in g_1N \).
Proof: Let \( S = A^{-1}B - cG = bg_1N + k_2F \) and \( \sigma : G \to G/N \) be the natural homomorphism. We use \( \overline{M} \) to denote the image of \( M \) under \( \sigma \). So \( \overline{A}^{-1} \overline{B} = b\sigma(g_1) + k_2\overline{F} + cnG/N \). Since \( BN = g_1AN \), we have \( \overline{B} = \sigma(g_1)\overline{A} \) and \( \sigma(g_1)\overline{A}^{-1} = \sigma(g_1)(a + bn + cnG/N) \). So \( \overline{F} = \frac{a}{k_2}\sigma(g_1) \), i.e. \( FN = \frac{a}{k_2}g_1N \).

Hence

\[
F^{-1}N = \frac{a}{k_2}Ng_1^{-1},
\]

(2.1.8)

\[
SS^{-1} = (A^{-1}B - cG)(AB^{-1} - cG)
\]

\[
= (k_2F + bNg_1)(k_2F^{-1} + bNg_1^{-1}).
\]

By direct computation, and noting that \( N \in \text{Cent}(CG) \), \( \chi_0(A) = \chi_0(B) \), we have

\[
F^{-1}F = (\frac{a}{k_2})^2.
\]

(2.1.9)

If (1) is satisfied, then \( F \) has nonnegative coefficients, so

\[
F = \frac{a}{k_2}g_2,
\]

(2.1.10)

\( g_2 \in g_1N \). Therefore \( B = Ag_2, g_2 \in g_1N \).

If (2) is satisfied, by a result of McFarland [MC], we have

\[
F = \pm \frac{a}{k_2}g_2,
\]

(2.1.11)

\( g_2 \in g_1N \). But \( \chi_0(A) = \chi_0(B) \), hence \( F = \frac{a}{k_2}g_2 \), therefore \( B = Ag_2, g_2 \in g_1N \).

This completes the proof. \( \square \)

Before we state the main theorem, we introduce the notion of \( \sigma \)-multiplier. Let \( G, N \) be the same as before, \( A \) an element of \( ZG \), \( \sigma : G \to G/N \)
the natural homomorphism. If $t$ is a multiplier of $\sigma(A)$, then we say that $t$ is a $\sigma$-multiplier of $A$.

**Theorem 2.1.6.** Let $G$ be a finite group of order $v = mn$ and exponent $e_G$, $N$ be a normal subgroup of $G$ of order $n$. Suppose $A \in ZG$, $A \in \text{Cent}(CG)$ satisfies $AA^{(-1)} = a + bN + cG$ for some integers $a, b, c, a \neq 0$. Let $t$ be a positive integer relatively prime to $u$, $k_1|a$, $k_1 = p_1^{e_1}p_2^{e_2} \cdots p_s^{e_s}$, $a_1 = (v, k_1)$, $k_2 = \frac{k_1}{a_1}$. For each $p_i$, we define

$$q_i = \begin{cases} p_i & \text{if } p_i \not\in e_G \\ l_i & \text{if } e_G = p_i^l u, (p_i, u) = 1, r \geq 1, l_i \text{ satisfies } (l_i, p_i) = 1 \text{ and } l_i \equiv p_i^l (\text{mod } u). \end{cases}$$

Assume that for each $i$, $1 \leq i \leq s$, there exists an integer $f_i$ such that either

1. $q_i^{f_i} \equiv t (\text{mod } e_G)$ or
2. $q_i^{f_i} \equiv -1 (\text{mod } e_G)$

Also we assume that one of the following conditions is satisfied

3. All coefficients of $A$ are nonnegative, $k_2 > b + c$, $k_2 > c$,

4. $(M(\frac{a}{k_2}), v) = 1$, where $M(m)$ is defined in Lemma 2.1.5.

Finally, assume that $t$ is a $\sigma$-multiplier of $A$. Then $t$ is a multiplier of $A$.

**Proof:** Since $A \in \text{Cent}(CG)$, $AA^{(-1)} = a + bN + cG$, by Lemma 1.2.5, we have

$$\omega(A)\omega(A^{(-1)}) = a + b\omega(N) + c\omega(G), \quad (2.1.12)$$

where $\omega : g \mapsto \chi(g)\chi(1)$, $g \in G$, $\chi \in \text{Irr}(G)$.

Simplifying the above equation, one has

$$\chi_0(A)\overline{\chi_0(A)} = a + bn + cv,$$
\[ \chi(A)\overline{\chi(A)} = (a + bn)\chi(1)^2, \quad \text{if} \quad \chi \in \text{Irr}(G|\theta_0) \setminus \{\chi_0\}, \]
\[ \chi(A)\overline{\chi(A)} = a\chi(1)^2, \quad \text{if} \quad \chi \in \text{Irr}(G) \setminus \text{Irr}(G|\theta_0), \quad (2.1.13) \]

where \( \chi_0 \) is the trivial character of \( G \) and \( \theta_0 \) is the trivial character of \( N \).

Since \( t \) is a \( \sigma \)-multiplier of \( A \), we have
\[ A^{(t)}N = g_1AN \quad \text{for some} \quad g_1 \in G. \quad (2.1.14) \]

Let \( S = g_1^{-1}A^{(t)}A^{(-1)} \). Then \( SS^{(-1)} = (a + bN + cG)^2 \).

\[ \chi_0(S) = a + bn + cw \equiv bn + cv \quad (mod \ p_i^{e_i}), \quad i = 1, 2, \ldots, s. \quad (2.1.15) \]

For \( \chi \in \text{Irr}(G|\theta_0) \setminus \{\chi_0\} \), \( \omega(S) = \omega(g_1^{-1}A^{(t)})\omega(A^{(-1)}) \). But \( \omega(A^{(t)}N) = \omega(g_1AN) \), so \( \omega(g_1^{-1}A^{(t)}) = \omega(A) \). Hence \( \omega(S) = \omega(A)\omega(A^{(-1)}) \), i.e.
\[ \chi(S) = \frac{\chi(A)\chi(A^{(-1)})}{\chi(1)} = (a + bn)\chi(1) \equiv bn\chi(1) \quad (mod \ p_i^{e_i}) \quad (2.1.16) \]
for \( i = 1, 2, \ldots, s \).

For \( \chi \in \text{Irr}(G) \setminus \text{Irr}(G|\theta_0) \), we claim that \( \chi(S) \equiv 0 \quad (mod \ p_i^{e_i}), \quad i = 1, 2, \ldots, s \). We prove this claim by distinguishing two cases.

Case I. There exists \( f_i \) such that \( q_i \equiv t \quad (mod \ e_G) \).

From Theorem 1.3.4, we know that in the cyclotomic field \( \mathbb{Q}(\xi_{eG}) \), if \( p \not| e_G \), then the Frobenius automorphism \( \xi_{eG} \mapsto \xi_{eG}^p \) leaves all prime ideal factors of \( (p) \) invariant; if \( p|e_G \), then the mapping \( \xi_{eG} \mapsto \xi_{eG}^l \) (where \( l = p^l + xu, (x, p) = 1 \)) also fixes all prime ideal factors of \( (p) \). So
\[ (\chi(A), p_i^{e_i}) = (\sigma_t(\chi(A)), p_i^{e_i}) = (\chi(A^{(t)}), p_i^{e_i}), \quad (2.1.17) \]

where \( \sigma_t : \xi_{eG} \mapsto \xi_{eG}^l \). Noting that \( \chi(A)\chi(A^{(-1)}) = \chi(A^{(t)})\chi(A^{(-t)}) \equiv 0 \quad (mod \ p_i^{e_i}) \) for \( 1 \leq i \leq s \) when \( \chi \in \text{Irr}(G) \setminus \text{Irr}(G|\theta_0) \), we have \( \chi(A^{(t)})\chi(A^{(-1)}) \equiv 0 \quad (mod \ p_i^{e_i}) \), i.e. \( \chi(S) \equiv 0 \quad (mod \ p_i^{e_i}) \), for \( i = 1, 2, \ldots, s \).
Case II. There exists \( f_i \) such that \( q_i^{f_i} \equiv -1 \pmod{e_G} \).

For each \( \chi \in \text{Irr}(G) \setminus \text{Irr}(G|\theta_0) \), we claim that \( \chi(S)\chi(S^{-1}) = a^2 \chi(g_1)\overline{\chi(g_1)} \).

We prove the claim as follows. Since \( SS^{-1} = (a + bN + cG)^2 \), applying \( \omega : g \mapsto \frac{\chi(g)}{\chi(1)} \) to both sides of this equation, we get \( \omega(SS^{-1}) = \omega((a + bN + cG)^2) = (\omega(a + bN + cG))^2 = a^2 \). On the other hand, \( \omega(SS^{-1}) = \omega(A^{(t)}A^{(-t)}A) = \omega(A^{(t)}A^{(-t)}A)(A^{(-t)}A) \), by \( S = g_1^{-1}A^{(t)}A^{(-t)} \), we have \( \omega(S) = \omega(g_1^{-1})\omega(A^{(t)}A^{(-t)}) A \), \( \omega(A^{(t)}A^{(-t)}) = \frac{\omega(S)}{\omega(g_1)} \), also \( S^{-1} = g_1A^{(-t)}A \), so \( \omega(S^{-1}) = \omega(g_1)\omega(A^{-t}A), \omega(A^{-t}A) = \frac{\omega(S^{-1})}{\omega(g_1)} \), hence \( \omega(SS^{-1}) = \frac{\omega(S)}{\omega(g_1)} \frac{\omega(S^{-1})}{\omega(g_1)} \), therefore

\[
\frac{\omega(S)}{\omega(g_1)} = a^2, \\
\omega(S)\omega(S^{-1}) = a^2\omega(g_1^{-1})\omega(g_1), \\
\frac{\chi(S)\chi(S^{-1})}{\chi(1)} = a^2\frac{\chi(g_1^{-1})\chi(g_1)}{\chi(1)}, \\
\chi(S)\chi(S^{-1}) = a^2\chi(g_1)\overline{\chi(g_1)}. \tag{2.1.18}
\]

This completes the proof of the above claim.

Assume that \( a^2\chi(g_1)\overline{\chi(g_1)} = p_i^{2\epsilon_i}w \), where \( w \) is an algebraic integer.

Subcase 1. \( (p_i, e_G) = 1 \).

By Theorem 1.3.4, \( (\chi(S))(\overline{\chi(S)}) = (P_1P_2\cdots P_g)^{2\epsilon_i}(w) \), hence

\( P_j^{\epsilon_i}|(\chi(S)) \text{ or } P_j^{\epsilon_i}|(\overline{\chi(S)}) \quad j = 1, 2, \ldots, g. \)

Noting that \( P_j \) is invariant under the mapping \( \xi_{e_G} \mapsto \xi_{e_G}^{-1} = \xi_{e_G}^{-1} \), so in either case, we always have \( P_j^{\epsilon_i}|(\chi(S)), j = 1, 2, \cdots, g \). Therefore \( \chi(S) \equiv 0 \pmod{p_i^{\epsilon_i}} \).

Subcase 2. \( (p_i, e_G) \neq 1 \).

By Theorem 1.3.4, \( (\chi(S))(\overline{\chi(S)}) = (\pi_1\pi_2\cdots\pi_g)^{2\phi(p_i^{\epsilon_i})}(w), \)

\( \pi_j^{\phi(p_i^{\epsilon_i})}|(\chi(S)) \text{ or } \pi_j^{\phi(p_i^{\epsilon_i})}|(\overline{\chi(S)}) \quad j = 1, 2, \cdots, g. \)
Noting that $\pi_j$ is invariant under the mapping $\xi_{eG} \mapsto \xi_{eG}^{l_i}$, where $l_i$ is defined in the statement of the theorem, thus $\pi_j$ is invariant under the map $\xi_{eG} \mapsto \xi_{eG}^{l_i} = \xi_{eG}^{-1}$. Hence in either case we have $\pi_j^{\phi(l_i)} \mid \chi(S)$, $j = 1, 2, \ldots, g$. Therefore $\chi(S) \equiv 0 \pmod{p_i^{\ell_i}}$. This completes the proof of the claim.

By Lemma 2.1.4, we have $A^{(l)}A^{(-1)} = bg_1N + cG + \frac{p_i^{\ell_i}}{b_i}F_i$, $b_i = (p_i^{\ell_i}, v)$, $F_i \in ZG$, $1 \leq i \leq s$. This implies that $(\frac{p_i^{\ell_i}}{b_i})F_i = (\frac{p_i^{\ell_i}}{b_j})F_j$, $F_i \equiv 0 \pmod{\frac{p_i^{\ell_i}}{b_j}}$, $j \neq i$, $1 \leq i, j \leq s$. Hence $(\frac{p_i^{\ell_i}}{b_i})F_i = k_2F_i$ for all $i = 1, 2, \ldots, s$, $F \in ZG$, therefore

$$A^{(l)}A^{(-1)} = bg_1N + cG + k_2F_i, \quad k_2 = k_1/a_1. \quad (2.1.19)$$

By Lemma 2.1.5, we have $A^{(l)} = Ag_2$, for some $g_2 \in g_1N$, so $t$ is a multiplier of $A$. This completes the proof. □.

**Corollary 2.1.7.** Let $G$ be an abelian group of order $v = mn$, and exponent $e_G$, $N$ be a subgroup of $G$ of order $n$, $D$ an $(m, n, k, \lambda_1, \lambda_2)$-divisible difference set in $G$ relative to $N$. Assume that $k_1|k - \lambda_1$, $k_1 = p_1^{\ell_1}p_2^{\ell_2}\cdots p_s^{\ell_s}$, $a_1 = (v, k_1)$, $k_2 = \frac{k_1}{a_1}$, for each $p_i$, we define $q_i = \begin{cases} p_i & \text{if } p_i \nmid e_G, \\ l_i & \text{if } e_G = p_i^{r_i}u, (p_i, u) = 1, r \geq 1, \text{ there exists } l_i \text{ satisfies } (l_i, p_i) = 1 \text{ and } l_i \equiv p_i^{r_i} \pmod{u}. \end{cases}$

For each $i$, $1 \leq i \leq s$, there exists $f_i$ such that either

1. $q_i^{f_i} \equiv t \pmod{e_G}$ or

2. $q_i^{f_i} \equiv -1 \pmod{e_G}$

and assume that one of the following conditions is satisfied

3. $k_2 > \lambda_1, k_2 > \lambda_2$. 

(4). \((M\left(\frac{k-\lambda_1}{k_2}\right), v) = 1\), where \(M(m)\) is defined in Lemma 2.1.5.

Finally, assume that \(t\) is a \(\sigma\)-multiplier of \(D\). Then \(t\) is a multiplier of \(D\).

**Proof:** This follows immediately from Theorem 2.1.6.

**Corollary 2.1.8.** Let \(D\) be an \((m, n, k, \lambda_1, \lambda_2)\)-abelian divisible difference set in \(G\) relative to \(N\). If \(p^j|k - \lambda_1, p^r|m\) and \(p^{j-r} > \lambda_1, p^{j-r} > \lambda_2, t = p^r + \frac{mn}{p^r}\) is a \(\sigma\)-multiplier of \(D\). Then \(t\) is a multiplier of \(D\).

**Proof.** In Corollary 2.1.7, set \(k_1 = p^j\), then \(a = (mn, k_1) = p^r\) and \(k_2 = \frac{k_1}{a} = p^{j-r}\).

Since \(p|e_G\), we choose \(q = p^r + \frac{mn}{p^r}\) which satisfies \((q, p) = 1\) and \(q \equiv p^r (mod u)\), where \(u = \frac{mn}{p^r}\). Noting that \(q = t, k_2 = p^{j-r} > \lambda_1\) and \(k_2 > \lambda_2\), \(t\) is a \(\sigma\)-multiplier of \(D\), by Corollary 2.1.7, \(t\) is a multiplier of \(D\). This completes the proof.

Several remarks about Theorem 2.1.6 and Corollaries 2.1.7 and 2.1.8 are in order.

**Remarks:** (1). Theorem 2.1.6 is a general multiplier theorem of group ring, all multiplier theorems (First multiplier theorem, Second multiplier theorem, McFarland’s multiplier theorem, etc.) mentioned at the beginning of this section but Qiu’s results can be obtained from it, so we may view it as a unification of most previously known multiplier theorems.

(2). Corollary 2.1.7 is essentially a generalization of Ganley, Spence and Lam’s multiplier theorems for relative difference sets, it also improves their results in the following ways, first we can choose \(l_i\) to be any integer such that \((l_i, p_i) = 1\) and \(l_i \equiv p_i^f (mod u)\), not necessarily to be \(p_i^f + u\); secondly we just
require $q_i$ satisfy either (1) or (2) while Ganley, Spence and Lam's multiplier theorems always require the validity of (1). We will see that these improvements do help in the nonexistence proof of relative difference sets which we give as an application of our multiplier theorem.

(3). Corollary 2.1.7 is also applicable to difference sets. In some cases, it can give new multiplier for abelian difference sets. For example, assume that $D$ is an abelian $(v, k, 2)$-difference set, $8|k - 2$, then $2 + \frac{v}{2}$ is a multiplier of $D$. This result can not be obtained by any previous multiplier theorem. The proof of this result follows immediately from the fact $8|k - 2$ implies that $v \equiv 2 \pmod{4}$ and Corollary 2.1.7.

As an application of our multiplier theorem, we prove a nonexistence result for relative difference sets with parameters

$$(\frac{q^n - 1}{q - 1}, q^{n-2}(q - 1), q^{n-1}, 0, 1)$$

by using multiplier argument. The above parameters of relative difference sets correspond to the so-called elliptic semiplane, whose existence is quite rare. The following theorem rules out the existence of certain of those that admit a regular automorphism group.

**Theorem 2.1.9.** Let $D$ be a $(\frac{q^n - 1}{q - 1}, q^{n-2}(q - 1), q^{n-1}, 0, 1)$-relative difference set in abelian group $G$ relative to $N$. If $q = p^\alpha$, $p$ is a prime, $\alpha$ is a positive integer, then $p = 2$. Moreover if $q|e_G$, then $q = 2$, $n$ is odd; in this case if $G = Z_{2^n-1} \times Z_{2^n-1}$, then $n = 3$. 
Proof: Since $D$ is a $\left(\frac{q^n-1}{q-1}, q^{n-2}(q-1), q^{n-1}, 0, 1\right)$-relative difference set in abelian group $G$ relative to $N$, we have

$$DD^{(-1)} = q^{n-2} + (G - N). \quad (2.1.20)$$

Let $\sigma : G \rightarrow G/N$ be the natural homomorphism and $\sigma(D) = \overline{D}$. Then

$$\overline{DD}^{(-1)} = q^{n-2} + q^{n-2}(q-1)G/N, \quad (2.1.21)$$

i.e. $\overline{D}$ is a $\left(\frac{q^n-1}{q-1}, q^{n-1}, q^{n-2}(q-1)\right)$-difference set in $G/N$, and $k - \lambda = q^{n-2}$. If $q = p^n$, $p$ is a prime, by the second multiplier theorem, $q^n$ is a multiplier of $\overline{D}$.

Now we choose $t = q^n + (q^n - 1)$, so $(t, p) = 1$, $t \equiv p^{\alpha(n)} \pmod{q^n - 1}$ and $t$ is a $\sigma$-multiplier of $D$ because of $t \equiv q^n \pmod{\frac{q^n-1}{q-1}}$. By Corollary 2.1.7, $t$ is a multiplier of $D$.

Let $m = |G/N|$, $m^* =$the exponent of $G/N$. $m = \frac{q^n-1}{q-1}$, so $m^* | \frac{q^n-1}{q-1}$.

Now $t \equiv 1 \pmod{q^n - 1}$, so $t \equiv 1 \pmod{m^*}$, by Theorem 8.4 [EB], we have $t \equiv 1 \pmod{e_G}$. Note that $|G| = p^{(n-1)\alpha}(p^{\alpha} - 1)$, $G$ has an element of order $p$, so $t \equiv 1 \pmod{p}$. On the other hand, $t \equiv -1 \pmod{q}$, so $t \equiv -1 \pmod{p}$, hence $p = 2$.

If $q|e_G$, then $t \equiv 1 \pmod{e_G}$ implies that $t \equiv 1 \pmod{q}$, note that $t \equiv -1 \pmod{q}$, so $q = 2$.

In the following we show that $n = 3$ when $G = Z_{2^n-1} \times Z_{2^n-2}$. We remark that if $n = 3$, $\{1, 2, 4, 6\}$ is a $(7, 2, 4, 0, 1)$-relative difference set in $Z_7 \times Z_2$, so in this case, there does exist a $(7, 2, 4, 0, 1)$-relative difference set.

Since $2^n - 1$ is odd, $2^{n-2}$ is even. By Bose-Connor Theorem [BC], $2^{n-1}$ must be a perfect square, hence $n$ is odd.
Assume that $D$ is a $(2^n - 1, 2^{n-2}, 2^{n-1}, 0, 1)$-relative difference set in $Z_{2^{n-1}} \times Z_{2^{n-2}}$ with $n > 3$, $n$ odd. By Corollary 2.1.8, $t = 2^{n-2} + 2^n - 1$ is a multiplier of $D$. Since $t \equiv 2^{n-2} \pmod{2^n - 1}$ and the congruence $x \equiv 2^{n-2}x \pmod{2^n - 1}$ has only one solution $x \equiv 0 \pmod{2^n - 1}$, the orbits of $Z_{2^{n-1}}$ under $< x \mapsto tx >$ are one singleton $\{0\}$ and orbits of size $\geq 2$. Since $t \equiv 1 \pmod{2^{n-2}}$, the orbits of $Z_{2^{n-2}}$ under $< x \mapsto tx >$ are two singletons $\{0\}, \{2^{n-3}\}$ and $2^{n-3} - 1$ orbits of size 2: $\{1, 2^{n-2} - 1\}, \{2, 2^{n-2} - 2\}, \ldots, \{2^{n-3} - 1, 2^{n-3} + 1\}$. Hence the orbits of $Z_{2^{n-1}} \times Z_{2^{n-2}}$ under $< x \mapsto tx >$ are

1. two singletons: $\{(0,0)\}, \{(0,2^{n-3})\}$.
2. size 2 orbits: Type A. $\{(0,1), (0,2^{n-2} - 1)\}, \{(0,2), (0,2^{n-2} - 2)\}, \ldots, \{(0,2^{n-3} - 1), (0,2^{n-3} + 1)\}$. Type B. The direct products of size 2 orbits of $Z_{2^{n-1}}$ with the singleton orbits of $Z_{2^{n-2}}$.
3. orbits of size greater than 2.

$D$ must be a union of some of these orbits. However, the orbits of size greater than 2 and size 2 orbits of Type A can not be in $D$, otherwise a non-identity element in $\{0\} \times Z_{2^{n-2}}$ can be expressed as difference of two elements in $D$. So $D$ can only be a union of some singletons and size 2 orbits of Type B, but in this way, differences of any two elements in $D$ can not yield the elements of the form $(x, y)$, $x \neq 0, y \neq \pm 2^{n-3}$, $x \in Z_{2^{n-1}}$, $y \in Z_{2^{n-2}}$. This contradicts that $D$ is a relative difference set in $Z_{2^{n-1}} \times Z_{2^{n-2}}$. Therefore in this case, $n = 3$. This completes the proof. □
2. Numerical Multiplier Groups of Difference Sets

As we have seen in section 1, given a \((v, k, \lambda)\)-abelian difference set \(D\) in 
\(G\), the set \(M\) of all numerical multipliers of \(D\) forms a group, and we may view it as a subgroup of \((Z/(e_G))^*\), which is the group of units of the ring \(Z/(e_G)\). In this section, we take the approach of realizing \(M\) as the Galois group of certain number field extension and use number theoretic methods to study multipliers of abelian difference sets.

We begin with the definition of strong multiplier of a subset in an abelian group. Let \(G\) be an abelian group of order \(v\), with exponent \(e_G\), let \(E\) be an arbitrary proper subset in \(G\). For any integer \(t\), \((t, v) = 1\), if \(E^{(t)} = \{x^t | x \in E\} = E\), then \(t\) is called a strong multiplier of \(E\). We use \(S\) to denote the set of all strong multipliers of \(E\), it is easy to see that \(S\) forms a subgroup of \((Z/(e_G))^*\). For any \(\chi \in G^*\), we have the following tower of field extensions

\[ Q \subseteq Q(\chi(E)) \subseteq Q(\xi_{e_G}). \]

Let \(K_{\chi(E)} = Q(\chi(E)), K_G = Q(\xi_{e_G}), K_E = Q(\chi_0(E), \chi_1(E), \ldots, \chi_{v-1}(E))\), where \(\{\chi_0, \chi_1, \ldots, \chi_{v-1}\} = G^*\), and let \(G_{\chi(E)} = GalK_G/K_{\chi(E)}\). We will call \(K_E\) the field of \(E\). If we identify \(GalQ(\xi_{e_G})/Q\) with \((Z/(e_G))^*\), then we have the following lemma.

**Lemma 2.2.1.** If \(S\) is the strong multiplier group of \(E\), then \(S = \bigcap_{\chi \in G^*}G_{\chi(E)} = GalK_G/K_E\).

**Proof:** If \(t \in S\), then \(E^{(t)} = E\). For any \(\chi \in G^*\), we have \(\chi(E^{(t)}) = \chi(E)\), i.e. \(\sigma_t(\chi(E)) = \chi(E)\), where \(\sigma_t : \xi_{e_G} \mapsto \xi_{e_G}^t\). Since we identify \(GalQ(\xi_{e_G})/Q\) with \((Z/(e_G))^*\), we have \(t \in G_{\chi(E)}\) for any \(\chi \in G^*\).
Conversely, if \( t \in \cap_{\chi \in G} G\chi(E) \), then \( \sigma_t(\chi(E)) = \chi(E) \) for any \( \chi \in G^* \). That is \( \chi(E^{(t)}) = \chi(E) \), for any \( \chi \in G^* \). Hence \( E^{(t)} = E \), i.e. \( t \) is a strong multiplier of \( E \). The second equality in the lemma is clear. This completes the proof. \( \square \)

Using this lemma and a deep theorem of S. D. Cohen [CO], we can get an upper bound for the size of the multiplier group of a cyclic difference set.

**Theorem 2.2.2.** Let \( D \) be a \((v,k,\lambda)\)-difference set in a cyclic group \( G \) of order \( v \), and \( M \) the multiplier group of \( D \). If \( D \neq \pm\{3,6,7,12,14\} \) in \( \mathbb{Z}_{21} \), then \( |M| \leq k \).

**Proof:** By Theorem 2.1.2, there is a translate of \( D \) which is fixed by every multiplier of \( D \), since \( D \) and its translates have the same multiplier group, we may assume that \( D \) is fixed by all of its multipliers. Let \( \chi \) be a generator of the character group of \( G \), \( K_D = Q(\chi(D), \chi^2(D), \ldots, \chi^{n-1}(D)) \). Then by Lemma 2.2.1, \( \text{Gal}(\xi_v)/K_D = M \).

Now assume that \( D = \{d_1, d_2, \ldots, d_k\} \), we consider the following polynomial,

\[
f(X) = \prod_{i=1}^{k} (X - \chi(d_i)) = X^k - (\sum_{i=1}^{k} \chi(d_i))X^{k-1} + \cdots + (-1)^k \prod_{i=1}^{k} \chi(d_i). \quad (2.2.1)
\]

For any \( t \) such that \( D^{(t)} = D \), let \( \sigma_t : \xi_v \rightarrow \xi_v^t \), we have

\[
\sigma_t(\sum_{1 \leq i_1 < i_2 < \ldots < i_r \leq k} \chi(d_{i_1})\chi(d_{i_2})\cdots\chi(d_{i_r}))
= \sum_{1 \leq i_1 < i_2 < \ldots < i_r \leq k} \chi(d_{i_1})\chi(d_{i_2})\cdots\chi(d_{i_r})
= \sum_{1 \leq i_1 < i_2 < \ldots < i_r \leq k} \chi(d_{i_1})\chi(d_{i_2})\cdots\chi(d_{i_r})
\]

Therefore \( f(X) \in K_D[X] \).
By a result of Cohen [CO], if $D \neq \pm \{3, 6, 7, 12, 14\}$ in $\mathbb{Z}_2$, then $D$ contains a generator $d$ of the cyclic group $G$, hence $\chi(d)$ is a primitive $v$-th root of unity, that is to say, $f(X)$ has a root which is a primitive $v$-th root of unity, therefore $|M| = [Q(\xi_v) : K_D] \leq \deg f(X) = k$. This completes the proof. □

Remarks (1). There are cyclic $(v, k, \lambda)$-difference sets such that the size of the multiplier groups of the difference sets is $k$. For example, the quadratic residue difference sets in $\mathbb{Z}_p$ (see Example 1.1.2), where $p$ is a prime, $p \equiv 3 (mod 4)$.

(2). The above theorem generalizes a result of Ho [HO] on the multiplier groups of cyclic projective planes to arbitrary $\lambda$. Ho also gave a simple proof for the above theorem which does not use the Galois extension in the proof of Theorem 2.2.2.

(3). It is an interesting question to characterize those cyclic difference sets whose multiplier groups are as large as possible. For cyclic projective plane, Ho [HO] recently proved that if the multiplier group $M$ of a cyclic $(n^2 + n + 1, n + 1, 1)$-difference set has size $n + 1$, then $n$ is even, and $n^2 + n + 1$ is a prime. In general, we conjecture that if the multiplier group $M$ of a cyclic $(v, k, \lambda)$-difference set has size $k$, then $v$ is a prime. This conjecture seems to be open at present.

We continue to consider the decomposition of a prime $p$, $(p, v) = 1$ in $Q(\chi(E))$, where $E$ is a proper subset of an abelian group $G$ of exponent $e_G$.

In $K_{\chi(E)} = Q(\chi(E))$, we have $(p) = \pi_1 \pi_2 \cdots \pi_{g_1}$. In $K_G = Q(\xi_{e_G})$, we have $\pi_i = P_{g_1}^{(i)} P_{g_2}^{(i)} \cdots P_{g_{g_1}}^{(i)}$, $1 \leq i \leq g_1$. Let $D_{p(K_{\chi(E)}/Q)}$ be the decomposition group of $(p)$ with respect to the abelian extension $K_{\chi(E)}/Q$ (see Section 3 of
Chapter I for the definition of decomposition group). Then we have

**Lemma 2.2.3.** \( D_p(K_{x(E)}/Q) = D_p G_{x(E)}/G_{x(E)}, |D_p(K_{x(E)}/Q)| = f(\pi_i/(p)) = f_1, \) where \( D_p \) is the decomposition group of \( p \) with respect to \( Q(\xi_{e_G})/Q. \)

**Proof:** The first part follows from the fact that \( D_p(K_{x(E)}/Q) \) is just the image of \( D_p \) under the restriction map \( Res : Gal(Q(\xi_{e_G})/Q \to G_{x(E)}. \) The second part follows from Theorem 1.3.3 and Theorem 1.3.4. This completes the proof. □

Let \( f_{x(E)}(X) \) be the minimal polynomial of \( \chi(E) \) over \( Q. \) Since \( \chi(E) \) is an algebraic integer, \( f_{x(E)}(X) \in Z[X]. \) Also we use \( \overline{f_{x(E)}(X)} \) to denote the polynomial obtained from \( f_{x(E)}(X) \) by reducing its coefficients mod \( p. \) With all these notations, we have the following characterization of strong multipliers.

**Theorem 2.2.4.** Let \( G \) be an abelian group of order \( v, \) with exponent \( e_G, \) and let \( E \) be a proper subset of \( G. \) Assume that \( p \) is a prime, \( (p, v) = 1. \) Then the following are equivalent:

1. \( p \) is a strong multiplier of \( E. \)
2. \( p \) splits completely in \( K_{x(E)} \), for every \( \chi \in G^*. \)
3. \( \overline{f_{x(E)}(X)} = (X - a_1)^{i_1}(X - a_2)^{i_2} \cdots (X - a_s)^{i_s}, a_i \in Z/(p), i = 1, 2, \cdots, s \) for every \( \chi \in G^*. \)

**Proof.** (1)⇒(2): Since \( p \) is a strong multiplier of \( E, \) by Lemma 2.2.1, we have \( p \in G_{x(E)} \) for any \( \chi \in G^*. \) From Theorem 1.3.4, \( D_p \) consists of \( p \) powers, hence \( D_p \subseteq G_{x(E)} \) for any \( \chi \in G^*. \) By Lemma 2.2.3, we have \( D_p(K_{x(E)}/Q) = 1 \) and \( f_1 = 1. \) We also know that \( e(\pi_i/(p)) = e_1 = 1 \) from \( (p, v) = 1. \) Therefore \( (p) \) splits completely in \( K_{x(E)} \) for any \( \chi \in G^*. \)
(2)⇒(3): Since $f_{\chi(E)}(X)$ is the minimal polynomial of $\chi(E)$, $f_{\chi(E)}(X)$ is irreducible in $\mathbb{Z}[X]$. $f_{\chi(E)}(X)$ has the following decomposition in $\mathbb{Q}_p[X]$(see [J], $\mathbb{Q}_p$ is the $p$-adic completion of $\mathbb{Q}$)

$$f_{\chi(E)}(X) = f_1(X)f_2(X)\cdots f_g(X) \tag{2.2.2}$$

where $f_i(X)$ is monic and irreducible in $\mathbb{Q}_p[X]$,

$$f_i(X) \neq f_j(X)$$

$$\deg f_i(X) = n_i \text{(local degree)}$$

$$n_i = e_1 f_1 \tag{2.2.3}$$

By assumption, $(p)$ splits completely in $K^{(\chi(E))}$, hence $e_1 = f_1 = 1$, therefore $n_i = 1$, $i = 1, 2, \ldots, g$. So $\bar{f_i}(X)$ is monic, degree 1 polynomial in $\mathbb{Z}/(p)[X]$, but it may happen that $\bar{f_i}(X) = \bar{f_j}(X)$. Thus we have

$$\bar{f_{\chi(E)}}(X) = (X - a_1)^{\ell_1}(X - a_2)^{\ell_2}\cdots(X - a_s)^{\ell_s} \tag{2.2.4}$$

with $a_i \in \mathbb{Z}/(p)$, $i = 1, 2, \ldots, s$.

(3)⇒(1): Let $O_{\chi(E)}$ be the algebraic integer ring of $K_{\chi(E)}$. In $K_{\chi(E)}$, we have

$$(p) = \pi_1\pi_2\cdots\pi_{g_1}. \tag{2.2.5}$$

We know that $O_{\chi(E)}/\pi_i$ is a finite field and $[O_{\chi(E)}/\pi_i : \mathbb{Z}/(p)] = f_1$ which is the residue class degree of $p$ with respect to the extension $K_{\chi(E)}/\mathbb{Q}$. Let $\rho : \alpha \mapsto \rho(\alpha)$ be the natural homomorphism from $O_{\chi(E)}$ to $O_{\chi(E)}/\pi_i$. Now $\chi(E) \in O_{\chi(E)}$ for any $\chi \in G^*$. Also
Applying $\rho$ to both sides of the above equation, we have

$$f_{\chi(E)}(\chi(E)) = 0$$  \hspace{1cm} (2.2.6)$$

By assumption, $f_{\chi(E)}(X) = (X - a_1)^i (X - a_2)^{i_2} \cdots (X - a_s)^{i_s}$, $a_i \in Z/(p)$. So $\rho(\chi(E)) = a_i$ for some $i$, $1 \leq i \leq s$. Hence $\rho(\chi(E)) \in Z/(p)$, and

$$\rho(\chi(E))^p = \rho(\chi(E)).$$  \hspace{1cm} (2.2.8)$$

That is to say

$$\chi(E)^p \equiv \chi(E)(\text{mod } \pi_i).$$  \hspace{1cm} (2.2.9)$$

Noticing that $\pi_i$ is arbitrary, one has

$$\chi(E)^p \equiv \chi(E)(\text{mod } p)$$  \hspace{1cm} (2.2.10)$$

Hence $\chi(E^{(p)}) \equiv \chi(E)(\text{mod } p)$. Also note that this is true for all $\chi \in G^*$ because of the hypothesis. Assume that $E^{(p)} = \sum_{g \in G} a_g g$, $E = \sum_{g \in G} b_g g$, by Fourier inversion formula, $a_g = \frac{1}{v} \sum_{\chi \in G^*} \chi(E^{(p)}) \chi(g^{-1}) \equiv \frac{1}{v} \sum_{\chi \in G^*} \chi(E) \chi(g^{-1})(\text{mod } p)$, hence $a_g \equiv b_g(\text{mod } p)$, but both $a_g$, $b_g$ are $0$ or $1$. Thus $a_g = b_g$ for any $g \in G$. Therefore $E^{(p)} = E$. This completes the proof. $\square$

Let us apply the above theorem to difference sets. First we note that if $D$ is a $(v, k, \lambda)$-difference set in an abelian group $G$, by Theorem 2.1.2, there is a translate of $D$ which is fixed by all of its numerical multipliers. It is easy to see that $D$ and any translate of $D$ have the same numerical multiplier group.
Hence $M = S$, where $M$ is the group of numerical multipliers of $D$ and $S$ is the group of strong multipliers of some translate of $D$. Therefore, we can apply Theorem 2.2.4 to get results on multipliers of difference sets. We need the following lemma.

**Lemma 2.2.5.** Let $D$ be a $(v, k, \lambda)$-difference set in an abelian group $G$. For any $\chi \in G^*$, $\chi \neq \chi_0$, if $\chi(D) \notin Q$, then the minimal polynomial $f_{\chi(D)}(X)$ of $\chi(D)$ takes the following form

$$f_{\chi(D)}(X) = X^m + a_1 X^{m-1} + \cdots + a_{\frac{m}{2}} X^{\frac{m}{2}} + a_{\frac{m}{2}-1} n X^{\frac{m}{2}-1} + a_{\frac{m}{2}-2} n^2 X^{\frac{m}{2}-2} + \cdots + n^\frac{m}{2}.$$

**Proof:** Let $\chi$ be an arbitrary nonprincipal character of $G$, and let $\theta = \chi(D)$. Since $D$ is a difference set, by Theorem 1.2.2, one has $\theta \overline{\theta} = n$.

Assume that $f_{\chi(D)}(X) = X^m + a_1 X^{m-1} + \cdots + a_{m-1} X + a_m, a_i \in Z$. From $\theta \overline{\theta} = n$, we know that $Q(\theta) = Q(\overline{\theta})$, and it is easy to see that the minimal polynomial of $\overline{\theta}$ is also $f_{\chi(D)}(X)$. Multiplying both sides of the equation $\theta^m + a_1 \theta^{m-1} + \cdots + a_{m-1} \theta + a_m = 0$ by $\overline{\theta}^m$, we have

$$n^m + a_1 n^{m-1} \overline{\theta} + \cdots + a_{m-1} n \overline{\theta}^{m-1} + a_m \overline{\theta}^m = 0 \quad (2.1.11)$$

Let $g_{\chi(D)}(X) = a_m X^m + a_{m-1} n X^{m-1} + \cdots + a_1 n^{m-1} X + n^m$. Then $g_{\chi(D)}(\overline{\theta}) = 0$. Hence $f_{\chi(D)}(X)|g_{\chi(D)}(X)$. This implies that

$$g_{\chi(D)}(X) = a_m f_{\chi(D)}(X) \quad (2.2.12)$$

We claim that $m$ is even. Let $Gal K_{\chi(D)}/Q = \{h_1 = 1, h_2, \cdots, h_m\}$. Then $f_{\chi(D)} = (X - \theta)(X - h_2(\theta)) \cdots (X - h_m(\theta))$. If $m$ is odd, then there is an $i, 1 \leq i \leq m$ such that $h_i(\theta)$ is real. Since $h_i \in Gal K_{\chi(D)}/Q$, there exists $t, (t, v) = 1$ such that $h_i(\theta) = \chi^t(D)$. Hence $h_i(\theta)\overline{h_i(\theta)} = h_i(\theta)^2 = n$, also we note
that if $m$ is odd, then $n$ is a square by equation (2.2.12), hence $h_4(\theta)$ is a rational number, this contradicts the assumption that $\chi(D)$ is not in $Q$. This completes the proof of the claim. Now we have that $m$ is even, comparing coefficients of both sides of (2.2.12), we have

$$a_m = n^{\frac{m}{2}}, a_{m-1} = a_1 n^{\frac{m}{2}-1}, \ldots, a_{\frac{m}{2}+1} = a_{\frac{m}{2}-1}n$$ (2.2.13)

Therefore $f_{\chi(D)}(X)$ takes the required form. This completes the proof of the lemma. □

Now if there is a prime $p$, $(p, v) = 1$, $p | n$. Then the minimal polynomial $f_{\chi(D)}(X)$ of $\chi(D)$, as in the last lemma, has the following factorization in $\mathbb{Z}/(p)[X]$

$$f_{\chi(D)}(X) = X^{\frac{m}{2}} + a_1 X^{\frac{m}{2}-1} + \cdots + a_{\frac{m}{2}}$$ (2.2.14)

At this point, we want to give some remarks on the connection between the above observation and Theorem 1.3.5 (sometimes it is called Kummer’s theorem). Given any prime $p$, $p | n$, $(p, v) = 1$, for any nonprincipal character $\chi$ of $G$, by (2.2.14), $\overline{f_{\chi(D)}(X)}$ has a linear factor in $\mathbb{Z}/(p)[X]$. Let $O_{\chi(D)}$ be the integer ring of $\mathbb{Q}(\chi(D))$. Since $Q(\chi(D))/Q$ is an abelian extension, if $p | O_{\chi(D)}/\mathbb{Z}[\chi(D)]$ for every $\chi \in G^*$, then Kummer’s theorem in particular would imply that $\overline{f_{\chi(D)}(X)}$ splits into linear factors for any $\chi$, by Theorem 2.2.4, $p$ is a strong multiplier of $D$, hence a multiplier of $D$.

But the condition $p \nmid |O_{\chi(D)}/\mathbb{Z}[\chi(D)]|$ is seldom satisfied for some $\chi \in G^*$ if we assume that -1 is not a multiplier of $D$ (in the case -1 is a multiplier
multiplier of $D$, every integer $t$, $(t, v) = 1$ is a multiplier of $D$, and $K_D$ is not a quadratic extension of $Q$.

we prove this claim as follows. Let $\sigma : \xi_{vG} \mapsto \xi_{vG}^{-1}$ be the complex conjugation. If $-1$ is not a multiplier of $D$, then $\sigma \not\in \cap_{x \in G^* \setminus \{x_0\}} G_{x(D)}$. So there is a nontrivial $\chi$ of $G$ such that $\sigma \not\in G_{x(D)}$. That is to say, $\sigma|_{Q(x(D))}$ is not identity. Assume that $G_{x(D)} = \{\sigma_0 = \text{identity}, \sigma_1 = \sigma|_{Q(x(D))}, \ldots, \sigma_{m-1}\}$, where $m = \text{deg} f_{x(D)}(X)$, then

$$\text{disc}(\chi(D)) = (-1)^{\frac{m(m-1)}{2}} f'_{x(D)}(\chi(D)) f'_{x(D)}(\overline{\chi(D)}) \cdots f'_{x(D)}(\sigma_{m-1}(\chi(D))).$$

(2.2.15)

From Lemma 2.2.5, We have $f'_{x(D)}(\chi(D)) = \chi(D)w + a_1 n^{\frac{m}{2}} - 1$ and $f'_{x(D)}(\overline{\chi(D)}) = \overline{\chi(D)}w + a_1 n^{\frac{m}{2}} - 1$. If a prime $p$ divides $n$ and $m > 2$, then $p|\text{disc}(\chi(D))$. Also if $(p, v) = 1$, then $p \nmid \text{disc}(K_{x(D)})$ because $p$ is unramified in $Q(x(D))$. But $\text{disc}(\chi(D)) = |O_{x(D)} / Z[x(D)]|^2 \text{disc}(K_{x(D)})$ (see [MAR] for a proof of this relation). Hence $p||O_{x}/Z[\chi(D)]|.$

By the above remark, in order to resolve the multiplier conjecture by this number theoretic approach, we have to study the decomposition of those primes $p$, $p||O_{x(D)} / Z[\chi(D)]|$ in $K_{x(D)}$, but so far, this leaves much to be desired.

In a special case, we have the following.

**Corollary 2.2.6.** Let $D$ be a $(v, k, \lambda)$-difference set in an abelian group $G$. If for any $\chi \in G^*$, $\chi(D) + \overline{\chi(D)}$ is a rational integer, then any prime divisor $p$ of $n$ which is coprime to $v$ is a multiplier of $D$.

**Proof.** Since $D$ is a $(v, k, \lambda)$-difference set in an abelian group $G$, we have $\chi(D) + \overline{\chi(D)} = n$ for any nonprincipal character $\chi \in G^*$. By assumption, $\chi(D) + \overline{\chi(D)}$ is a rational integer, $\chi(D)$ satisfies a minimal polynomial $f_{x(D)}(X)$
of degree 1 or degree 2. If \( f_{\chi(D)}(X) \) is of degree 1, of course \( f_{\chi(D)}(X) \) is of degree 1 in \( \mathbb{Z}/(p)[X] \) for any \( p|n \), \( (p,v) = 1 \). If \( f_{\chi(D)}(X) \) is of degree 2, then 
\[
 f_{\chi(D)}(X) = X^2 - (\chi(D) + \overline{\chi(D)})X + n,
\]
hence for any \( p|n \), \( (p,v) = 1 \), we have 
\[
 f_{\chi(D)}(X) = (X - a)X,
\]
where \( a \equiv \chi(D) + \overline{\chi(D)}(mod \ p) \). Hence by Theorem 2.2.4, \( p \) is a multiplier. This completes the proof. □

**Remark:** In fact, in the above corollary, \( p \) is a multiplier if and only if \( (\chi(D) + \overline{\chi(D)})^2 - 4n \) is a square in \( \mathbb{Z}/(p) \), where \( p \) is a prime, \( (p,v) = 1 \).

A natural question related to the above corollary is: Does there exist a difference set satisfying the hypothesis in Corollary 2.2.6? The answer is yes. For example, the Paley-Hadamard difference sets and twin prime difference sets both satisfy the condition in Corollary 2.2.6 (for the definitions of Paley-Hadamard and twin prime difference sets, we refer the reader to [JU1]).

Finally, we apply Theorem 2.2.4 to difference sets with multiplier 2. Before stating the theorem, we give a definition.

A difference set \( D \) in a finite group \( G \) is called skew Hadamard if \( G \) is the disjoint union of \( D, D^{(-1)} \), and \( \{1\} \).

**Theorem 2.2.7.** Let \( D \) be a \((v,k,\lambda)\) difference set in an abelian group \( G \). If \( 2 \) is a multiplier of \( D \), assume that \( D \) is fixed by \( 2 \), and \( k - \lambda \equiv 2(mod \ 4) \), then \( D \) or its complement in \( G \) is a skew Hadamard difference set.

**Proof.** For each \( \chi \in G^* \), \( \chi \neq \chi_0 \), let \( K_{\chi(D)} = Q(\chi(D)) \). Assume that 
\[
(2) = \prod_{i=1}^{m} \varphi_i \text{ in } K_{\chi(D)},
\]
by Lemma 1.2.2, we have 
\[
(\chi(D))(\overline{\chi(D)}) = (k - \lambda) = (n_0) \prod_{i=1}^{m} \varphi_i \tag{2.2.16}
\]
where \( k - \lambda = 2n_0 \) with \( n_0 \) odd.
From (2.2.16), we see that exactly one of each pair \( \varphi_i, \varphi_j \) divides \( (\chi(D)) \). Hence \( \chi(D) + \overline{\chi(D)} \not\equiv 0 (mod \varphi_i) \). By assumption, 2 is a strong multiplier of \( D \), from Theorem 2.2.4, we know that 2 splits completely in \( K_{\chi(D)} \), hence 2 has residue class degree 1 with respect to \( K_{\chi(D)}/Q \). Therefore \( \chi(D) + \overline{\chi(D)} + 1 \equiv 0 (mod \varphi_i) \) for all \( i = 1, 2, \ldots, g_1 \). This implies that \( \chi(D) + \overline{\chi(D)} + 1 \equiv 0 (mod 2) \) for all \( \chi \in G^* \), \( \chi \neq \chi_0 \). Let \( A = D + D^{(-1)} + 1 = \sum_{g \in G} a_g g \). By Fourier inversion formula, we have

\[
a_g = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(A) \chi(g^{-1}) \equiv 1 (mod 2) \tag{2.2.17}
\]

for all \( g \in G \). Therefore, if \( 1 \not\in D \), then \( D + D^{(-1)} + 1 = G \); if \( 1 \in D \), let \( D' = G \setminus D \), then \( D' + D'^{(-1)} + 1 = G \). This completes the proof. □

**Remark:** The above theorem was first proved in Arasu [A] by using Wilbrink's identity. The above proof uses the idea in [F], and it is completely number theoretic.
Chapter III

Skew Hadamard Difference Sets

1. Introduction and A Summary of Old Results

As we have seen at the end of Chapter II, if an abelian \((v,k,\lambda)\)-difference set \(D\) is fixed by the multiplier 2, then \(D\) or the complement of \(D\) is a skew Hadamard difference set. Also given an abelian skew Hadamard difference set \(D\), the field \(K_D\) is a quadratic extension of \(Q\), which is one of the easiest extensions among all the abelian extensions of \(Q\). So in this chapter, we study skew Hadamard difference sets in more detail. In the next chapter, we will consider the case \(K_D = Q\).

We begin by recalling that a difference set \(D\) in an abelian group \(G\) is called skew Hadamard if \(G\) is the disjoint union of \(D\), \(D(-1)\), and \(\{1\}\). The definition gives:

\[
1 \notin D, k = \frac{v-1}{2}, \lambda = \frac{v-3}{4}, n = \frac{v+1}{4}
\]  

(3.1.1)

where \(v\) is the order of the group \(G\), and \(k\) is the size of \(D\).

Using group ring notations, then in \(Z[G]\), we have

\[
DD(-1) = \frac{v+1}{4} + \frac{v-3}{4}G
\]  

(3.1.2)
\[ D + D^{(-1)} = G - 1 \quad (3.1.3) \]

Applying any non-principal character \( \chi \) of \( G \) to the above two equations, one has

\[ \chi(D) = \frac{-1 \pm \sqrt{-v}}{2} \quad (3.1.4) \]

This is an important property of skew Hadamard abelian difference sets of which we will make use later.

Skew Hadamard difference sets were studied by E.C. Johnsen [JO], P. Camion and H. Mann [CM], and also by Jungnickel [JU2] in connection with \( \lambda \)-ovals. The results of Johnson, Camion and Mann were summarized in [JU1] as follows:

**Theorem 3.1.1.** Let \( D \) be a skew Hadamard difference set in an abelian group \( G \). Then \( v \) is a prime power \( p^m \equiv 3 (\text{mod } 4) \), and the quadratic residues mod \( v \) are multipliers for \( D \). Moreover, if \( G \) has exponent \( p^s \) with \( s \geq 2 \), then any basis of \( G \) contains at least two elements of order \( p^s \), and hence one has \( m \geq 2s + 1 \). In particular, if \( v = p^3 \) for a prime \( p \), then \( G \) is elementary abelian.

We give the following proof of the theorem due to Camion and Mann [CM].

**Proof:** First we show that \( v \) is not a square. If \( v \) is a square, since \( v \) is odd, then \( v \equiv 1 (\text{mod } 8) \), this implies that \( \lambda = \frac{v-3}{4} \) is not an integer, a contradiction. Hence \( v \) is not a square. If \( v \) is composite we may choose \( v_1 \) such that \( v_1 \) is not a square and \( v = p^j v_1 \), \( (v_1, p) = 1 \), \( j \geq 1 \), \( p \) a prime. Choose \( \chi \neq \chi_0 \) of order \( p \), then \( \chi(g) \) is a \( p \)-th root of unity for all \( g \in G \). Then (3.1.4)
implies that \( \sqrt{v_1} \in Q(\xi_p) \) or \( \sqrt{-v_1} \in Q(\xi_p) \), where \( \xi_p \) denotes a primitive \( p \)-th root of unity. But this is impossible since neither \( \sqrt{v_1} \) nor \( \sqrt{-v_1} \) are in \( Q(\xi_p) \) (The discriminant of \( Q(\xi_p) \) is prime to \( v_1 \)). This shows that \( v \) is a prime power \( p^m \equiv 3 \mod 4 \). Let \( \xi \) be a \( p^m \)-th root of unity and \( (\frac{\xi}{p^m}) = 1 \) (where \( (\frac{\cdot}{p^m}) \) is the Legendre symbol) then the automorphism \( \xi \mapsto \xi^4 \) leaves \( \sqrt{-v} \) invariant. Hence

\[
\chi(D^{(i)}) = \chi(D)
\]

for all characters \( \chi \) of \( G \). Therefore \( D^{(i)} = D \). Finally, assume that \( G \) has exponent \( p^s \) with \( s \geq 2 \), write \( g = (a_1, a_2, \cdots, a_t) \), where \( a_i \) is a residue mod \( p^l \). Assume \( l_1 = s \) and \( l_i < s \) for \( i \geq 2 \). By the fact that the quadratic residues mod \( v \) are multipliers of \( D \), if \( g \in D \) then \( (1 + \mu p^s)g \in D \). Choosing \( a_1 \neq 0 \mod p \) and \( \mu = a_1^{-1} \), we see that \( (p^s-1,0,\cdots,0) \), arises as a difference of two elements of \( D \) at least as often as there are elements in \( D \) for which \( a_1 \neq 0 \mod p \). But by the definition of skew Hadamard difference set there are exactly \( \frac{p^m - p^{m-1}}{2} \) such elements in \( D \); hence

\[
\frac{p^m - p^{m-1}}{2} \leq \frac{v - 3}{4} = \frac{p^m - 3}{4}
\]

or

\[
p^m \leq 2p^{m-1} - 3
\]

which is impossible. This completes the proof of the theorem. \( \square \)

The only known examples of skew Hadamard difference sets are the Paley-Hadamard difference sets formed by the (nonzero) quadratic residues in \( GF(q) \), where \( q \) is a prime power congruent to \( 3 \mod 4 \) (see Example 1.1.2). It is conjectured that there are no further examples. The exponent bound in
Theorem 3.1.1 can be viewed as evidence for this conjecture. In Section 2, we obtain an exponent bound which improves the one in Theorem 3.1.1. In particular, we prove that if \( v = p^5 \), for a prime \( p \) congruent to 3 (mod 4), then \( G \) is elementary abelian.

2. A New Exponent Bound

In this section, we first prove a result concerning subsets \( D \) in abelian \( p \)-groups with the property that \( D + D^{(-1)} = G - 1 \) and \( D^{(t)} = D \) for any nonzero quadratic residue \( t \) (mod \( p \)), then we will use it to get a new exponent bound on skew Hadamard difference sets.

**Lemma 3.2.1.** Let \( G \) be an abelian \( p \)-group of order \( p^m \), where \( p \) is a prime, \( p \equiv 3 \) (mod 4), \( m \) is a positive integer, and let \( D \subset G \). Suppose that \( D + D^{(-1)} = G - 1, D^{(t)} = D \) for any nonzero quadratic residue \( t \) (mod \( p \)). Then

1. There exists a non-principal character \( \chi \) of \( G \) such that \( \chi(D) \not\equiv \frac{t^{(m+1)} - 1}{2} \) (mod \( p^m \)).

2. If \( m \) is odd, and for any non-principal character \( \chi \) of \( G \), \( \chi(D) \equiv \frac{t^{(m+1)} - 1}{2} \) (mod \( p^{m-1} \)), then \( D \) is a difference set in \( G \).

**Proof:** Since \( D^{(t)} = D \), for any nonzero quadratic residue \( t \) (mod \( p \)), (note that \( t \) is a quadratic residue mod \( p \) if and only if it is a quadratic residue mod \( p^m \)), we have \( \sigma_t(\chi(D)) = \chi(D) \), where \( \sigma_t \) is the Galois automorphism \( \xi_{p^m} \mapsto \xi_{p^m}^t, \xi_{p^m} \) is a primitive \( p^m \)-th root of unity, \( \chi \) is any non-principal character of \( G \), by Galois theory, we have \( \chi(D) \in \mathbb{Z}[\omega] \), where \( \omega = \frac{-1 + \sqrt{-p}}{2} \) and \( \mathbb{Z}[\omega] \) is the integer ring of \( \mathbb{Q}(\sqrt{-p}) \) (see [MAR]). Assume that \( \chi(D) = a_x + b_x \omega, a_x, b_x \in \mathbb{Z} \). Since \( D + D^{(-1)} = G - 1 \), applying \( \chi \) to this equation, we get \( \chi(D) + \chi(D^{(-1)}) = \).
-1. Therefore $2a_\chi + 1 = b_\chi$ and hence $\chi(D) = \frac{-1+(2a_\chi+1)\sqrt{-p}}{2}$.

If $\chi(D) \equiv p^{[\frac{m+1}{2}]} \pmod{p^{[\frac{m+1}{2}]}},$ for any non-principal character $\chi$ of $G$, then $p^{[\frac{m+1}{2}]} | (2a_\chi + 1)$. Let $2a_\chi + 1 = p^{[\frac{m+1}{2}]} c_\chi$, where $c_\chi$ is a non-zero integer. We have

$$\chi(D) \chi(D^{(-1)}) = 1 + p^{[\frac{m+1}{2}]+1} c_\chi^2$$  \hspace{1cm} (3.2.1)

Calculating the coefficient of 1 in $DD^{(-1)}$ in two ways, one by Fourier inversion formula, the other by direct calculation, we have

$$\frac{p^m - 1}{2} = \frac{1}{p^m} \left( \frac{(p^m - 1)^2}{4} + p^m - 1 + p^{[\frac{m+1}{2}]+1} \sum_{\chi \neq \chi_0} c_\chi^2 \right)$$  \hspace{1cm} (3.2.2)

Simplifying this equation,

$$p^m(p^m - 1) = p^{[\frac{m+1}{2}]+1} \sum_{\chi \neq \chi_0} c_\chi^2.$$  \hspace{1cm} (3.2.3)

But, this is impossible because $2[\frac{m+1}{2}] + 1 \geq m + 1$, we thus deduce a contradiction. This finishes the proof of (1).

For the proof of (2), we simply let $2a_\chi + 1 = p^{[\frac{m-1}{2}]} d_\chi$, then

$$\chi(D) \chi(D^{(-1)}) = \frac{1 + p^m d_\chi^2}{4}.$$  \hspace{1cm} (3.2.4)

Similarly, by calculating the coefficient of 1 in $DD^{(-1)}$ in two ways, we have

$$p^m(p^m - 1) = p^m \sum_{\chi \neq \chi_0} d_\chi^2.$$  \hspace{1cm} (3.2.5)
This forces \( d_x^p = 1 \) for all \( \chi \neq \chi_0 \). Hence \( \chi(D)\chi(D^{(1)}) = \frac{1 + p^n}{4} \), for all \( \chi \neq \chi_0 \). By Fourier inversion formula, \( D \) is a skew Hadamard difference set in \( G \). This completes the proof. □

**Lemma 3.2.2.** Let \( G = \mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n} \), where \( m, n \) are positive integers, \( p \) is a prime, \( p \equiv 3 (mod \ 4) \), and let \( D \subset G \). If \( D + D^{(-1)} = G - 1 \), \( D^{(t)} = D \) for any \( t, t \equiv a^2 (mod \ p) \), for some \( a, (a, p) = 1 \), then there is a non-principal character \( \chi \) of \( G \) such that \( \chi(D) \neq \frac{p-1}{2} (mod \ p) \).

**Proof:** Define \( \phi : G \to G \) via \( x \mapsto x^p \). It is easy to see that \( \phi \) is a homomorphism and \( K = Ker\phi \cong \mathbb{Z}_p \times \mathbb{Z}_p \). Let \( D_0 = D - D \cap K \). Then \( D_0^{(t)} = D_0 \) for any \( t, t \equiv a^2 (mod \ p) \), for some \( a, (a, p) = 1 \). Noting that \( D_0 \) has no element of order \( p \), we have

\[
D_0 = \bigcup_{i=1}^{p-1} x_i < x^i >,
\]

where \( x \) runs through a complete set of representatives of the orbits of \( D_0 \) under \( \{t | t \equiv a^2 (mod \ p) \} \), for some \( a, (a, p) = 1 \), and \( < x^p > \neq \{1\} \).

Since \( \chi(< x^p >) = 0 \) if \( \chi \) is non-principal on \( < x^p > \), and \( \chi(< x^p >) = | < x^p > | \) if \( \chi \) is principal on \( < x^p > \), we have \( \chi(D_0) \equiv 0 (mod \ p) \), for any non-principal character \( \chi \) of \( G \). If for any \( \chi \neq \chi_0 \), \( \chi(D) \equiv \frac{p-1}{2} (mod \ p) \), then \( \chi(D \cap K) \equiv \frac{p-1}{2} (mod \ p) \), for any \( \chi \neq \chi_0 \). But this contradicts (1) of Lemma 3.2.1, therefore, there is a non-principal character \( \chi \) of \( G \) such that \( \chi(D) \neq \frac{p-1}{2} (mod \ p) \). This completes the proof. □

Now we are in the position to state the main theorem.

**Theorem 3.2.3.** Let \( G \) be an abelian \( p \)-group for some prime \( p \equiv 3 (mod \ 4) \), and let \( |G| = p^n, expG = p \). If \( G \) admits a skew Hadamard difference
set $D$, and $s \geq 2$, then $s \leq \frac{n+1}{4}$.

**Proof:** By Theorem 3.1.1, we can assume that $G = G' \times Z_{p^s} \times Z_{p^s}$.

By equation (3.1.1), if $\chi \neq \chi_0$, then

$$
\chi(D) = \frac{-1 \pm \sqrt{-p^m}}{2} = \frac{p^{\frac{m-1}{2}} - 1}{2} + p^{\frac{m-1}{2}} \frac{1 \pm \sqrt{-p}}{2}
$$

Let $D_1 = D \cap (Z_{p^s} \times Z_{p^s})$, $G' = \{g_1 = 1, g_2, \cdots, g_l\}$. Then

$$D = D_1 + D_2g_2 + \cdots + D-lg_l \quad (3.2.7)$$

where $D_i \subset Z_{p^s} \times Z_{p^s}, i = 1, 2, \cdots, l$.

For each non-principal character $\chi'$ of $Z_{p^s} \times Z_{p^s}$, we can extend it to $G$ in $l$ ways, assume the extensions are $\chi'_1, \chi'_2, \cdots, \chi'_l$, then $\{\chi'_i|G', i = 1, 2, \cdots, l\} = (G')^*$.

Applying these characters to equation (3.2.7), one has

$$
\chi'_1(D) = \chi'(D_1) + \chi'(D_2)\chi'_1(g_2) + \cdots + \chi'(D_l)\chi'_1(g_l)
$$

$$
\chi'_2(D) = \chi'(D_1) + \chi'(D_2)\chi'_2(g_2) + \cdots + \chi'(D_l)\chi'_2(g_l)
$$

$$
\vdots
$$

$$
\chi'_i(D) = \chi'(D_1) + \chi'(D_2)\chi'_i(g_2) + \cdots + \chi'(D_l)\chi'_i(g_l) \quad (3.2.8)
$$

Since $\sum_{i=1}^{l} \chi'_i(g_j) = 0, j = 2, 3, \cdots, l$, we get

$$
|G'|\chi'(D_1) = \sum_{i=1}^{l} \chi'_i(D)
$$
where $\delta \in \mathbb{Z}[\omega]$. Therefore

$$\chi'(D_1) = \frac{p^{m-1}}{2} - \frac{1}{2} + \frac{p^{m-1}}{|G'|} \delta$$

Noting that $|G'| = p^{m-2s}$, one has

$$\chi'(D_1) = \frac{p^{m-1}}{2} - \frac{p}{2} + p^{2s-\frac{m+1}{2}} \delta + \frac{p-1}{2}.$$  \hspace{1cm} (3.2.10)

By the definition of skew Hadamard difference set, and Theorem 3.1.1, it is easy to see that $D_1$ satisfies the hypotheses of Lemma 3.2.2, so by Lemma 3.2.2, there is a non-principal character $\chi'$ of $\mathbb{Z}_p^s \times \mathbb{Z}_p^s$ such that $\chi'(D_1) \neq \frac{p^{m-1}}{2} (mod p)$, therefore $2s - \frac{m+1}{2} \leq 0$, so $s \leq \frac{m+1}{4}$. This completes the proof. \hfill $\Box$

**Corollary 3.2.4.** If an abelian group $G$ admits a skew Hadamard difference set, and $|G| = p^5$, then $G$ is elementary abelian.

The proof of this corollary is immediate from Theorem 3.2.3 by letting $m = 5$.

**Corollary 3.2.5.** If $G$ is an abelian group which admits a skew Hadamard difference set, and $G$ is not elementary abelian, then $p$-rank$(G) \geq 4$.

This is an immediate consequence of Theorem 3.2.3.

In view of Theorem 3.2.3, the first open cases for testing whether an abelian $p$-group admits a skew Hadamard difference set or not are: $G = \mathbb{Z}_p \times (\mathbb{Z}_p^3)^3$, and $G = (\mathbb{Z}_p)^3 \times (\mathbb{Z}_p^3)^2$. These two cases seem to be more difficult than the case $|G| = p^5$. 
Chapter IV

Reversible Difference Sets

1. Definitions and Introduction

Let $D$ be a $(v, k, \lambda)$-difference set in $G$, if $D^{(-1)} = Dg$ for some $g \in G$, then $D$ is called a difference set with multiplier $-1$. By Theorem 2.1.2, if $G$ is abelian, we may assume that the difference set $D$ is fixed by $-1$, i.e. $D^{(-1)} = D$, then $D$ is called a reversible or symmetric difference set.

We note that if $D^{(-1)} = D$ in an abelian group $G$ with exponent $e_G$, then any integer $t$, $(t, e_G) = 1$, is a multiplier of $D$ (see Hughes, van Lint and Wilson [HLM]). Hence the multiplier group $M$ of $D$ is $\text{Gal}Q(\xi_{e_G})/Q$, and the field $K_D = Q$.

Reversible abelian difference sets have been studied extensively. The following theorem summarizes most of the known necessary conditions on reversible difference set.

**Theorem 4.1.1.** Let $D$ be a reversible abelian $(v, k, \lambda)$-difference set in $G$. Then the following hold.

(1) $v$ and $\lambda$ are even and $n$ is a square.

(2) $v$ and $n$ have the same odd prime divisors.
(3) If $p$ is a prime divisor of $n$, then $D(p) \equiv 0 \pmod{p}$.

(4) Every integer $t$ relatively prime to $v$ is a multiplier for $D$.

(5) Let $p$ be a prime dividing $v$ and let $s$ be the rank of the Sylow $p$-subgroup of $G$. Then one has $k(p - 1) \leq \lambda(p^s - 1)$. In particular, the Sylow subgroups of $G$ are not cyclic.

(6) If $p_{|n}$ divides $n$ for some prime $p$, then $p_{|v}$ divides $v$ and $p_{|v}$ divides both $k$ and $\lambda$. Moreover, if $p_{|v}$ is the highest power of $p$ dividing $v$, then $k(p_{|v} - 1) \leq \lambda(p_{|v} - 1)$.

(7) $D$ has parameters $v = m(m + a + 1)(m + a - 1)/a$, $k = m(m + a)$, and $\lambda = ma$, where $a$ and $m$ have opposite parity and $a|m^2 - 1$.

We refer the reader to McFarland and Ma [MM] for a complete (and relatively short) proof of Theorem 4.1.1.

It turns out that reversible abelian difference sets split naturally into two classes, those satisfying $v \neq 4n$ and those with $v = 4n$ (i.e. Hadamard difference sets), where $n = k - \lambda$. So far, there is only one known example for the first case.

Example 4.1.1. There exists a reversible $(4000, 775, 150)$-difference set in $Z_2^5 \times Z_3^3$. This example is due to McFarland who gave a very general construction for non-cyclic difference sets in 1973 [MC1]. We describe the construction of this special example as follows.

Let $V$ be the additive group of a vector space over $GF(5)$ of dimension 3 and $H_1, H_2, \cdots, H_{31}$ be all hyperplanes of the vector space. Let $K = \{g_0, g_1, \cdots, g_{31}\}$ be an elementary abelian group of order 32. Then $D = \{(g_i, H_i) | i = 1, 2, \cdots, 31\}$ is a $(4000, 775, 150)$-reversible abelian difference set in
Regarding the case \( v = 4n \), things are more interesting, we will devote Sections 3, 4 and 5 of this chapter to discuss the known constructions and necessary conditions.

Based on the above observation, McFarland proposed the following conjecture.

**McFarland's Conjecture.** If \( D \) is a reversible abelian \((v, k, \lambda)\)-difference set, then either \( v = 4000, k = 775, \lambda = 150 \) (as in Example 4.1.1) or \( v = 4n \).

McFarland and Ma [MM] and Ma [MA] have shown that the above conjecture is true for \( n \leq 10^8 \).

In the study of reversible difference sets, it is possible to show that if an abelian group \( G \) contains a reversible difference set, then certain subgroup \( H \) of \( G \) also contains a reversible difference set, which is usually called a sub-difference set of the original difference set. The following theorem was first proved by McFarland [MC2] for reversible Hadamard difference sets and later generalized to all abelian reversible difference sets by Ma [MA].

**Theorem 4.1.2.** Suppose there exists a nontrivial reversible difference sets of order \( n \) in an abelian group \( G \), and let \( H \) be a subgroup of \( G \) such that \((|H|, |G/H|) = 1 \) and \(|H|\) is even. Then there exists a reversible difference set in \( H \) of order \( n_1 = (|H|^2, n) \).

Using this theorem successively, one can reduce the order of the group \( G \) in the above theorem to \( 2^np^b \), where \( p \) is an odd prime. Based on this observation and the basic parameter condition \( \lambda (v - 1) = k(k - 1) \) for difference
sets, Ma [MA] proposed the following conjecture which implies McFarland's Conjecture.

**Ma's Conjecture.** Let $p$ be an odd prime, $a \geq 0$, and $b, m, r \geq 1$. Then

1. $Y = 2^{2a+r}p^{2m} - 2^{2a+2}p^{m+r} + 1$ is a square if and only if $m = r$ (i.e. $Y = 1$).
2. $Z = 2^{2b+2}p^{2m} - 2^{b+2}p^{m+r} + 1$ is a square if and only if $p = 5, b = 3, m = 1, r = 2$ (i.e. $Z = 2401$).

2. A Result on Ma's Conjecture

In this section, we give a proof for part (1) of Ma's conjecture.

Let $Z, N, P$ be the sets of integers, positive integers and odd primes respectively. The following lemmas will be used in the proof of our main theorem.

**Lemma 4.2.1.** Let $D \in N$. If $(u_1, v_1)$ is the fundamental solution of Pell's equation

$$u^2 - Dv^2 = 1, u, v \in N$$  \hspace{1cm} (4.2.1)

then every solution $(u, v)$ of (4.2.1) can be expressed as

$$u + v\sqrt{D} = (u_1 + v_1\sqrt{D})^t, t \in N$$ \hspace{1cm} (4.2.2)

**Lemma 4.2.2.** Let $D, D_1, D_2 \in N$ with $D = D_1D_2$. If $\min\{D_1, D_2\} > 1$ and the equation

$$D_1U^2 - D_2V^2 = 1, U, V \in N$$  \hspace{1cm} (4.2.3)
has a solution \((U,V)\), then it has a unique solution \((U_1,V_1)\) such that
\[ U_1 \sqrt{D_1} + V_1 \sqrt{D_2} \leq U \sqrt{D_1} + V \sqrt{D_2}, \]
where \((U,V)\) runs over all solutions of (4.2.3). Moreover, the fundamental solution \((u_1,v_1)\) of (4.2.1) satisfies
\[ u_1 + v_1 \sqrt{D} = (U_1 \sqrt{D_1} + V_1 \sqrt{D_2})^2. \]

For the proofs of Lemma 4.2.1 and Lemma 4.2.2, we refer the reader to [P].

Now we state our main theorem.

**Theorem 4.2.3.** The equation

\[ x^2 = 2^{2a+2}p^m - 2^{2a+2}p^{m+r} + 1, \quad x, m, r \in \mathbb{N}, x > 1, a \in \mathbb{Z}, a \geq 0, p \in \mathbb{P} \]  

(4.2.4)

has no solution \((x, p, a, m, r)\).

**Proof:** Let \((x, p, a, m, r)\) be a solution of (4.2.4). If \(a = 0\), then
\[ x^2 - 1 = 4p^m - 4p^{m+r}. \]
From this, it is easy to see that \(m > r\). Factorizing both sides of this equation, we have
\[ \frac{x + 1}{2} \cdot \frac{x - 1}{2} = p^{m+r}(p^{m-r} - 1) \]  

(4.2.5)

Since \(\gcd\left(\frac{x+1}{2}, \frac{x-1}{2}\right) = 1\), we have \(\frac{x+1}{2} = p^{m+r}x_1, \frac{x-1}{2} = y_1\), where \(x_1y_1 = p^{m-r} - 1\), and \(\gcd(x_1, y_1) = 1\). But this is absurd because \(\frac{x+1}{2} = \frac{x-1}{2} + 1\), and \(p^{m+r}x_1\) is much bigger than \(y_1\). Thus from now on we may assume that \(a > 0\).

Let \(D_1 = p^{m-r}, D_2 = p^{m-r} - 1\) and \(D = D_1D_2\). Since \(D_1 - D_2 = 1\), by Lemma 4.2.2, \((2p^{m-r} - 1, 2)\) is the fundamental solution of (4.2.1). By (4.2.4), \((u, v) = (x, 2^{a+1}p^r)\) is a solution of (4.2.1). Since \(2^{a+1}p^r > 2\), by Lemma 4.2.1, we have
\[ x + 2^{a+1}p^r \sqrt{D} = (2p^{m-r} - 1 + 2\sqrt{D})^t; t \in \mathbb{N}, t > 1 \]  

(4.2.6)
If $2|t$, from (4.2.6), we have

$$2^{a+1}p^r \equiv 0 \pmod{2p^{m-r} - 1}. \quad (4.2.7)$$

Since $gcd(2^{a+1}p^r, 2p^{m-r} - 1) = 1$ and $2p^{m-r} - 1 > 1$, the above congruence is impossible, therefore $t$ is odd. Again from (4.2.6), we have

$$2^{a}p^r = \sum_{i=0}^{(t-1)/2} \binom{t}{2i+1}(2p^{m-r} - 1)^{t-1-2i}(4D)^i \quad (4.2.8)$$

Noting that the right hand side of (4.2.8) is odd, we have $a = 0$, this contradicts our assumption that $a > 0$. Hence the proof is complete. \(\Box\)

In view of the above theorem, in order to prove McFarland's conjecture on abelian difference sets with multiplier -1, all we need to do is to prove part (2) of Ma's conjecture. This remains open at present.

3. Hadamard Difference Sets

Once McFarland’s conjecture is proved, the study of abelian difference sets with multiplier -1 is reduced to the case when $v = 4n$.

A $(v, k, \lambda)$-difference set satisfying $v = 4n$ is called a Hadamard difference set (HDS), alternative names used by other authors are Menon difference set or H-set. By part (1) of Theorem 1.1.4, a symmetric design with $v = 4n$ can only exist if $n$ is a perfect square. It is then easily seen that the parameters of a Hadamard difference set have the form $(4u^2, 2u^2 \pm u, u^2 \pm u)$. Hadamard difference sets have been extensively studied because of their close connection to Hadamard matrices and perfect binary arrays. We refer the reader to [D.J] for a detailed survey of this subject. In this paper, we mainly discuss reversible Hadamard difference sets.
We begin by recalling a theorem of McFarland [MC2] which is a special case of Theorem 4.1.2.

**Theorem 4.3.1.** Suppose there exists a reversible HDS in an abelian group $H \times K$, where $|H|$ is even and $(|H|, |K|) = 1$. Then there exists a reversible HDS in $H$.

On the other hand, the following theorem due to Menon [ME1] tells us how to compose two Hadamard difference sets.

**Theorem 4.3.2.** Let $D_1$ and $D_2$ be two Hadamard difference sets of orders $u_1^2$ and $u_2^2$ in groups $G_1$ and $G_2$ respectively. Then $D = \{D_1 \times (G_2 \setminus D_2)\} \cup \{(G_1 \setminus D_1) \times D_2\}$ is a Hadamard difference set of order $4u_1^2u_2^2$ in $G_1 \times G_2$. Moreover if $D_1$ and $D_2$ are reversible, then $D$ is also reversible.

We remark there are more complicated composition theorems in the papers by Turyn [TU] and Xia [X].

By Theorem 4.3.1 and 4.3.2, in order to study reversible abelian HDS, we need to consider two basic cases first:

1. $v = 2^{2d+2}$,
2. $v = 4p^{2\alpha}$, where $p$ is an odd prime.

There is extensive literature on Hadamard difference sets in 2-groups. The existence problem for difference sets in abelian 2-groups is completely solved. We quote the following theorem from the survey paper [JU1].

**Theorem 4.3.3.** Let $G$ be an abelian group of order $2^{2d+2}$. Then $G$ contains a difference set if and only if $G$ satisfies Turyn's exponent bound $e_G \leq 2^{d+2}$.
We remark that a difference set in a 2-group is necessarily a Hadamard difference set by a theorem of Mann [MAN].

Although the existence problem for difference sets in abelian 2-groups is completely solved, it is not yet known which abelian 2-groups admit \textit{reversible} difference sets. The trivial difference sets in elementary abelian group of order 4 and $\mathbb{Z}_4$ together with Theorem 4.3.2 show that any abelian group of order $2^{2d+2}$ with exponent 2 or 4 contains a reversible difference set. On the other hand, a construction of Dillon [DI] shows that $\mathbb{Z}_{2^{d+1}} \times \mathbb{Z}_{2^{d+1}}$ contains a reversible difference set. The examples due to Leung and Ma [LM] are likewise reversible. Besides these examples, we do not know any more examples of reversible difference sets in abelian 2-groups.

In this work, we will concentrate on the second case, i.e. $v = 4p^{2\alpha}$, where $p$ is an odd prime.

We first mention that Ma [MA1] proved the following theorem on the structure of certain Sylow $p$-subgroups of an abelian group containing a reversible HDS.

\textbf{Theorem 4.3.4.} Let $D$ be a reversible HDS in an abelian group $G$, and let $p^{2\alpha}$ and $p^e$ be the order and exponent of the Sylow $p$-subgroup of $G$ respectively, where $p$ is a prime and $p^e \neq 4$. Then $G$ contains a subgroup isomorphic to $\mathbb{Z}_{p^e} \times \mathbb{Z}_{p^e}$.

This theorem, in particular gives an exponent bound on the Sylow $p$-subgroup, i.e. $e \leq s$, for the Sylow $p$-subgroup of $G$ admitting a reversible HDS. It seems that this bound can be improved. For example, we can prove the following result.
Theorem 4.3.5. There is no reversible HDS in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_9$.

We postpone the proof of this theorem to Section 4 because we need some lemmas as preparation.

We remark that this case was listed as open in Ma's 1990 paper [MA1] and the recent survey of Davis and Jedwab [DJ]. Also we remind the reader that there exist Hadamard difference sets (not reversible) in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_9$ (see [ADJS]).

When the Sylow $p$-subgroups of $G$ are elementary abelian, things are more interesting because we have more examples, and this is the place where we can relate difference sets to codes and point sets in projective geometry.

4. New Necessary Conditions For HDSs

In this section, we began by considering the existence of an arbitrary Hadamard difference sets (not necessarily reversible) with $u = p^n$, where $p$ is an odd prime, and $\alpha$ is a positive integer, then we will prove a characterization theorem for reversible HDS in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_p^{2\alpha}$. We need the following two lemmas.

Lemma 4.4.1. Let $D$ be a Hadamard difference set in the direct product group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times P$, $|P| = p^{2\alpha}$, where $p$ is an odd prime, $\alpha$ is a positive integer and $P$ is an abelian group with exponent $p^\varphi$. Then for any $\chi \in G^* \setminus \{\chi_0\}$, $\chi(D) = p^{\alpha} \eta$, where $\eta$ is a $2p^\varphi$th root of unity.

The proof of this lemma is closely parallel to that of Lemma 4 in [MC3]. For the convenience of the reader, we include the proof here.
Proof. Since $D$ is a Hadamard difference set in $G$, we have

$$DD^{(-1)} = p^{2\alpha} + (p^{2\alpha} - p^\alpha)G$$  \hfill (4.4.1)

Applying any $\chi \in G^* \setminus \{\chi_0\}$ to the above equation, one has

$$\chi(D)\overline{\chi(D)} = p^{2\alpha}$$  \hfill (4.4.2)

Noting that here the exponent of $G$ is $2p^\alpha$, so $\chi(D) \in \mathbb{Q}(\xi_{p^\alpha})$, where $\xi_{p^\alpha}$ is a primitive $p^\alpha$th root of unity. The principal ideal generated by $p$ has the prime ideal factorization $< 1 - \xi_{p^\alpha} > ^{p^\alpha-1(p-1)}$ in $\mathbb{Q}(\xi_{p^\alpha})$. Therefore (4.4.2) implies that $\chi(D) = p^\alpha \eta$ for some unit $\eta$ in $\mathbb{Q}(\xi_{p^\alpha})$ with absolute value 1. But then all conjugates of $\eta$ have absolute value 1, so a theorem of Kronecker (see [MAR]) implies $\eta$ is a root of unity. Also we know that all roots of unity in $\mathbb{Q}(\xi_{p^\alpha})$ form a cyclic group of order $2p^\alpha$, hence $\eta$ is a $2p^\alpha$th root of unity. This completes the proof. $\Box$

Lemma 4.4.2. Let $D$ be a Hadamard difference set in abelian group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times P$, $|P| = p^{2\alpha}$, where $p$ is an odd prime, and $\alpha$ is a positive integer. Let the Sylow 2-subgroup of $G$ be $\{1, a, b, ab\}$. Then $\{|D \cap P|, |D \cap aP|, |D \cap bP|, |D \cap abP|\} = \{|p^n(p^n-1)/2, p^{n}(p^n-1)/2, p^{n}(p^n-1)/2, p^{n}(p^n+1)/2\}$.

This lemma is well known, we include the proof here for the convenience of the reader.

Proof. Let $\rho : G \to G/P$ be the canonical epimorphism. We have

$$\rho(D)(\rho(D))^{(-1)} = p^{2\alpha} + (p^{2\alpha} - p^\alpha)p^{2\alpha}G/P.$$

Assume that $\rho(D) = t_0 + t_1a + t_2b + t_3ab$, where $t_0 = |D \cap P|$, $t_1 = |D \cap aP|$, $t_2 = |D \cap bP|$, and $t_3 = |D \cap abP|$. Applying each of the four characters
of $G/P$ to the above equation, we have

$$
t_0 + t_1 + t_2 + t_3 = 2p^{2\alpha} - p^\alpha
$$

$$
t_0 - t_1 + t_2 - t_3 = \pm p^\alpha
$$

$$
t_0 + t_1 - t_2 - t_3 = \pm p^\alpha
$$

$$
t_0 - t_1 - t_2 + t_3 = \pm p^\alpha
$$

Noting that all $t_i$’s are integers, we have

$$
\{t_0, t_1, t_2, t_3\} = \left\{\frac{p^\alpha(p^\alpha - 1)}{2}, \frac{p^\alpha(p^\alpha - 1)}{2}, \frac{p^\alpha(p^\alpha - 1)}{2}, \frac{p^\alpha(p^\alpha + 1)}{2}\right\}. \tag{4.4.4}
$$

\[\Box\]

**Theorem 4.4.3.** Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times P$ be an abelian group, $|P| = p^{2\alpha}$, where $p$ is an odd prime, and $\alpha$ is a positive integer. If $p \equiv 1 (mod\ 4)$, and $\alpha$ is odd, then $G$ cannot contain a Hadamard difference set.

**Proof.** Assume that $G$ contains a Hadamard difference set $D$, we are going to deduce a contradiction. We denote the Sylow 2-subgroup of $G$ by $\{1, a, b, ab\}$, by translating $D$ if necessary and using Lemma 4.4.2, we may assume that

$$
D = D_0 + aD_1 + bD_2 + abD_3 \tag{4.4.5}
$$

where $D_i \subset P$, $|D_i| = \frac{p^\alpha(p^\alpha - 1)}{2}$, $i = 0, 1, 2$, and $D_3 \subset P$, $|D_3| = \frac{p^\alpha(p^\alpha + 1)}{2}$.

For any nonprincipal $\chi \in P^*$, we can extend it to $G$ in four different ways to get $\chi_1$, $\chi_2$, $\chi_3$, $\chi_4$ such that $\chi_1 : a \mapsto 1, b \mapsto 1$, $\chi_2 : a \mapsto -1, b \mapsto 1$, $\chi_3 : a \mapsto 1, b \mapsto -1$, $\chi_4 : a \mapsto -1, b \mapsto -1$. Then

$$
\chi_1(D) = \chi(D_0) + \chi(D_1) + \chi(D_2) + \chi(D_3)
$$
\[ \chi_2(D) = \chi(D_0) - \chi(D_1) + \chi(D_2) - \chi(D_3) \]
\[ \chi_3(D) = \chi(D_0) + \chi(D_1) - \chi(D_2) - \chi(D_3) \]
\[ \chi_4(D) = \chi(D_0) - \chi(D_1) - \chi(D_2) + \chi(D_3) \]  
(4.4.6)

Adding these four equations, we have
\[ \chi(D_0) = \frac{1}{4} \left( \sum_{i=1}^{4} \chi_i(D) \right). \]  
(4.4.7)

By Lemma 4.4.1, \( \chi_i(D) = p^{\alpha} \eta_i, \ i = 1, 2, 3, 4, \) where \( \eta_i \)'s are \( 2p^\alpha \)th roots of unity, and \( p^\alpha \) is the exponent of \( P \). Hence
\[ \chi(D_0) = \sum_{i=1}^{4} \frac{\eta_i}{4} p^\alpha. \]  
(4.4.8)

Since \( \chi(D_0) \) is an algebraic integer, and \( p \) is odd, we have that \( \sum_{i=1}^{4} \frac{\eta_i}{4} \) is an algebraic integer. A well known result in number theory (for example see Lemma 2.1 in [KA]) implies that either \( \eta_1 = \eta_2 = \eta_3 = \eta_4 = \epsilon_0 \) or \( \sum_{i=1}^{4} \eta_i = 0 \). Hence \( \chi(D_0) = 0 \) or \( p^\alpha \epsilon_0 \). Similarly we can show that \( \chi(D_i) = 0 \) or \( p^\alpha \epsilon_i, \ i = 1, 2, 3 \). Let \( D_i^* = \{ \chi \in P^* \setminus \{ \chi_0 \} | \chi(D_i) \neq 0 \} \). Since \( D \) is a Hadamard difference set, we have \( DD^{-1} = p^{2\alpha} + (p^{2\alpha} - p^\alpha)G \). Using (4.4.5), we have the following equation
\[ D_0 D_0^{-1} + D_1 D_1^{-1} + D_2 D_2^{-1} + D_3 D_3^{-1} = p^{2\alpha} + (p^{2\alpha} - p^\alpha)P \]  
(4.4.9)

Applying any \( \chi \in P^* \setminus \{ \chi_0 \} \) to this equation, one has
\[ \sum_{i=0}^{3} |\chi(D_i)|^2 = p^{2\alpha}. \]  
(4.4.10)

From this equation, we see that if \( \chi(D_i) \neq 0 \) for some \( i, \ 0 \leq i \leq 3 \), then \( \chi(D_j) = 0, \ j \neq i \). Hence \( D_0^*, D_1^*, D_2^*, D_3^* \) are mutually disjoint, and \( P^* \setminus \{ \chi_0 \} = D_0^* \cup D_1^* \cup D_2^* \cup D_3^* \). Now we want to calculate \( |D_i^*|, i = 0, 1, 2, 3 \).
Calculating the coefficient of the identity in $D_iD_i^{(-1)}$ in two ways, one way by direct calculation, the other by using the inversion formula, we have

$$\frac{p^{2\alpha} - p^\alpha}{2} = \frac{1}{p^{2\alpha}}((\frac{p^{2\alpha} - p^\alpha}{2})^2 + |D_i^*|p^{2\alpha}). \quad (4.4.11)$$

Simplifying this equation, we get

$$|D_i^*| = \frac{p^{2\alpha} - 1}{4}, i = 0, 1, 2. \quad (4.4.12)$$

A similar calculation yields $|D_3^*| = \frac{p^{2\alpha} - 1}{4}$.

Let $\chi$ be an arbitrary character in $D_0^*$. Assume that $\chi$ has order $p^{e_1}$, where $1 \leq e_1 \leq e$, and $\sigma$ is an element in $GalQ(\xi_{p^{e_1}})/Q$, then $\chi^\sigma(D_0) = \sigma(\chi(D_0)) \neq 0$. Hence $\chi^\sigma \in D_0^*$. Also if $\chi = \chi^\sigma$, for some $\sigma \in GalQ(\xi_{p^{e_1}})/Q$, then for any $g \in P$, $\chi(g) = \chi^\sigma(g) = \sigma(\chi(g))$. Since $\chi$ has order $p^{e_1}$, there is an element $h \in P$ such that $\chi(h)$ is a primitive $p^{e_1}$th root of unity, therefore $\sigma$ is the identity map because it fixes a primitive $p^{e_1}$th root of unity. Hence $\{\chi^\sigma|\sigma \in GalQ(\xi_{p^{e_1}})/Q\} \subset D_0^*$, and $|\{\chi^\sigma|\sigma \in GalQ(\xi_{p^{e_1}})/Q\}| = |GalQ(\xi_{p^{e_1}})/Q| = p^{e_1-1}(p - 1)$. Repeating this process, we see that $D_0^*$ is decomposed into a disjoint union of these orbits, the size of each orbit is divisible by $p - 1$, therefore $p - 1||D_0^*|$. But $|D_0^*| = \frac{p^{2\alpha} - 1}{4}$, so $p - 1|\frac{p^{2\alpha} - 1}{4}$, i.e. $4|\frac{p^{2\alpha} - 1}{p - 1}$, but this is impossible because by the hypotheses

$$\frac{p^{2\alpha} - 1}{p - 1} \equiv 2\alpha \equiv 2(mod4).$$

Hence we get the desired contradiction. This completes the proof. □

Remarks (1). This theorem in particular says that there is no Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^6$. 
(2). In the above theorem, if \( \alpha = 1 \), then by a theorem of McFarland [MC3], the condition \( p \equiv 1 (mod 4) \) can be dropped. But if \( \alpha \geq 3 \), the condition \( p \equiv 1 (mod 4) \) seems to be important in the proof of Theorem 4.4.3. In particular, we do not know whether there is a Hadamard difference set in \( \mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_p)^6 \), where \( p \) is a prime congruent to 3 (mod 4), \( p > 3 \).

Combining the above theorem and a technique of Chan [CH], we obtain the following more general nonexistence result.

**Theorem 4.4.4.** Let \( G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times G_p \times G_q \), where \( G_p \) is an elementary abelian group of order \( p^{2^{\alpha}} \), \( p \equiv 1 (mod 4) \), \( \alpha \) is odd, and \( G_q \) is an abelian \( q \)-group with \( |G_q| = q^{2^\beta} \), \( q \) is an odd prime. If the order \( f \) of \( q(mod p) \) is odd, and \( p > 2eq^d \) where \( ef = p - 1 \), then \( G \) cannot contain a Hadamard difference set.

The following proof is closely parallel to that of Theorem 2.1 in [CH].

**Proof.** Assume to the contrary that \( G \) contains a Hadamard difference set \( D \), then

\[
DD^{(-1)} = p^{2^{\alpha}}q^{2^\beta} + (p^{2^{\alpha}}q^{2^\beta} - p^\alpha q^\beta)G. \tag{4.4.13}
\]

Let \( \rho \) be the projection of \( G \) onto \( H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times G_p \). Then

\[
\rho(D)(\rho(D))^{(-1)} = p^{2^{\alpha}}q^{2^\beta} + (p^{2^{\alpha}}q^{2^\beta} - p^\alpha q^\beta)q^{2^\beta}H. \tag{4.4.14}
\]

\( \chi_0(\rho(D)) = 2p^{2^{\alpha}}q^{2^\beta} - p^\alpha q^\beta \), where \( \chi_0 \) is the principal character of \( H \);
\( \phi(\rho(D)) = \pm p^\alpha q^\beta \), where \( \phi \) is any character of \( H \) of order 2. Let \( \phi_p \) be a character of \( H \) of order \( p \) or \( 2p \), and let \( \gamma = \phi_p(\rho(D)) \). Then \( \gamma^p = p^{2^{\alpha}}q^{2^\beta} \), and \( \gamma \in \mathbb{Z}[\xi_p] \), where \( \mathbb{Z}[\xi_p] \) is the integer ring of \( Q(\xi_p) \), and \( \xi_p \) is a primitive \( p \)th root of unity. The prime ideal factors of \( (q) \) are fixed by the Galois automorphism \( \sigma : \xi_p \mapsto \xi_p^q \), since \( q \) is an element of multiplicative order \( f \) modulo \( p \). Hence \((\gamma^p) = (\gamma)\),
therefore \( \gamma^\sigma = \eta \gamma \), where \( \eta \) is a unit in \( Z[\xi_p] \). Since \( |\gamma'| = p^\alpha q^\beta = |\gamma'^\sigma| \) for every algebraic conjugate \( \gamma' \) of \( \gamma \), the moduli of \( \eta \) and all of its conjugates are equal to 1, so a theorem of Kronecker implies that \( \eta \) is a root of unity. Hence \( \eta = \pm (\xi_p)^j \). Noting that \( f \) is odd, by exactly the same argument as that in Lemma 2.4 of [CH], we may assume that \( \gamma^\sigma = \gamma \). Let \( \gamma_i = \sum_{t=0}^{\ell-1} \xi_p^{at+i} \), where \( i = 0, 1, \ldots, e - 1 \). Since \( \{\xi_p^i | i = 1, 2, \ldots, p - 1\} \) is an integral basis of \( Z[\xi_p] \) and \( \gamma^\sigma = \gamma \), we have \( \gamma = \sum_{i=0}^{e-1} a_i \gamma_i \), where \( a_i \in Z \). Hence

\[
(\sum a_i \gamma_i)(\sum a_i \gamma_i) = p^{2a} q^{2\beta} + \lambda(1 + \xi_p + \xi_p^2 + \cdots + \xi_p^{p-1}) \tag{4.4.15}
\]

where \( \lambda \) is any integer. We view \( \gamma \) as an element in the group ring of the cyclic group \( \{1, \xi_p, \ldots, \xi_p^{p-1}\} \). Comparing the coefficients of the identity on both sides of (4.4.15) and applying the principal character to (4.4.15), one has

\[
p^{2a} q^{2\beta} + \lambda = f(\sum a_i^2)
\]

\[
p^{2a} q^{2\beta} + p\lambda = f^2(\sum a_i)^2 \tag{4.4.16}
\]

So

\[
p^{2a} q^{2\beta} = \frac{p(\sum a_i^2) - f(\sum a_i)^2}{e} \tag{4.4.17}
\]

Let \( S_2 = \sum_{i=0}^{e-1} a_i^2 \), \( S_1 = \sum_{i=0}^{e-1} a_i \). By Cauchy-Schwarz inequality, we have \( |S_1| \leq ep^\alpha q^\beta \). Since \( p^\alpha | \gamma |, p^\alpha | a_i, i = 0, 1, 2, \ldots, e - 1 \), we have \( p^\alpha | S_1 \), and \( p^{2\alpha} | S_2 \). Let \( |S_1| = xp^\alpha \), where \( 0 \leq x \leq eq^\beta \). Substituting \( |S_1| = xp^\alpha \) into (4.4.17), we get \( |S_2| = p^{2\alpha - 1}(eq^{2\beta} + fx^2) \). Therefore \( x = \pm eq^\beta (mod p) \). Since \( 0 \leq x \leq eq^\beta \) and \( p > 2eq^\beta \), we have \( x = eq^\beta \). In this case \( |S_1| = ep^\alpha q^\beta \) and \( S_2 = ep^{2\alpha} q^{2\beta} \). But then \( S_2 = S_2^2 / e \) and hence all \( a_i \)'s are equal to either \( S_1 / e \) or \( -S_1 / e \). Therefore \( \gamma = \pm p^\alpha q^\beta \equiv 0(mod p^\alpha q^\beta) \). In summary, \( \chi(\rho(D)) \equiv 0(mod \)
For any $x^D$, by the inversion formula, the coefficients of $\rho(D)$ are all divisible by $q^\beta$. Define $E = q^{-\beta} \rho(D) - \frac{1}{2}(q^\beta - 1)H$. Then

$$EE^{(-1)} = q^{-2\beta} \rho(D)\rho(D)^{(-1)} - \frac{q^\beta - 1}{q^\beta} (2p^{2\alpha}q^{2\beta} - p^\alpha q^\beta)H + (q^\beta - 1)^2p^{2\alpha}H$$

$$= p^{2\alpha} + (p^{2\alpha} - p^\alpha)H$$

Also

$$\chi_0(E) = q^{-\beta}(2p^{2\alpha}q^{2\beta} - p^\alpha q^\beta) - \frac{1}{2}(q^\beta - 1)4p^{2\alpha}$$

$$= 2p^{2\alpha} - p^\alpha$$

$$= \text{coefficient of 1 in } EE^{(-1)}$$

Hence all coefficients of $E$ are either 0 or 1. This shows that $E$ is a Hadamard difference set in $H$. However Theorem 3.1 in particular says that $H$ cannot contain an HDS. This is a contradiction. Therefore $G$ cannot contain an HDS. This completes the proof. □

Theorem 4.4.3 can also be extended to larger groups by using McFarland's sub-difference set technique in [MC2]. We state the following theorem whose proof is straightforward by Theorem 3.1 in [MC2].

**Theorem 4.4.5.** Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times P$, where $|P| = p^{2\alpha}$, $P$ is an abelian group with exponent $p^\nu$, $p$ is a prime congruent to 1 (mod 4), $\alpha$ is odd. Let $H$ be an abelian group of odd order such that for each prime divisor $q$ of the order of $H$, there is an integer $t$ satisfying $q^t \equiv -1 (mod p^\nu)$. Then there cannot exist an Hadamard difference set in the direct product group $G \times H$. 
Proof. The hypothesis of the theorem implies that the order of $H$ is self-conjugate mod $p^e$. Hence by Theorem 3.1 in [MC2], if there existed a HDS in $G \times H$, there would exist a HDS in $G$; this contradicts Theorem 4.4.3. The proof is complete. □

We now return to reversible Hadamard difference sets and prove a characterization theorem for reversible HDS in the abelian groups $Z_2 \times Z_2 \times (Z_p)^{2a}$. We will see that this characterization will be very useful in next section when we give a new proof for Xia's construction.

We state our theorem in terms of projective $(n, k, h_1, h_2, h_3)$ sets (see Section 5 of Chapter I). The translation from projective $(n, k, h_1, h_2, h_3)$ sets into projective 3-weight codes is obvious by Proposition 1.5.1.

Theorem 4.4.6. There is a reversible Hadamard difference set $D$ in an abelian group $G = Z_2 \times Z_2 \times (Z_p)^{2a}$, $p$ an odd prime, $\alpha$ even, if and only if there are four projective $(n, 2\alpha, \frac{n}{p} - p^{\alpha-1}, \frac{n}{p}, \frac{n}{p} + p^{\alpha-1})$ sets $\mathcal{O}_i$, $i = 0, 1, 2, 3$, in $PG(2\alpha-1, p)$ with $n = \frac{\nu(p^{\alpha-1})}{2(p-1)}$ such that for any hyperplane $H$ in $PG(2\alpha-1, p)$, there is a unique $i$, $0 \leq i \leq 3$, such that $|H \cap \mathcal{O}_i| \neq \frac{n}{p}$, and $|H \cap \mathcal{O}_j| = \frac{n}{p}$, if $j \neq i$.

Proof. Let $D$ be a Hadamard difference set in $G = Z_2 \times Z_2 \times (Z_p)^{2a}$, where $p$ is an odd prime, $\alpha$ is even. Let the Sylow 2-subgroup of $G$ be $\{1, a, b, ab\}$, and $P = (Z_p)^{2a}$. As in the proof of Theorem 4.4.3, by translating $D$ if necessary, we may decompose $D$ into four parts

$$D = D_0 + aD_1 + bD_2 + abD_3 \tag{4.4.18}$$

where $D_i \subset P$, $|D_i| = \frac{\nu(p^{\alpha-1})}{2}$, $i = 0, 1, 2$, and $D_3 \subset P$, $|D_3| = \frac{\nu(p^{\alpha-1})}{2}$. We set $E_i = D_i$, $i = 0, 1, 2$. $E_3 = P \setminus D_3$. Then $|E_i| = \frac{\nu(p^{\alpha-1})}{2}$, $i = 0, 1, 2, 3$. 
If \( D \) is reversible, then \( D_i^{(-1)} = D_i, \ i = 0, 1, 2, 3. \) Therefore \( E_i^{(-1)} = E_i, \ i = 0, 1, 2, 3. \) Hence \( \chi(E_i) \) is real, where \( \chi \) is any character of \( P. \) From the proof of Theorem 4.4.3, we see that \( \chi(E_i) = 0, \) or \( \pm p^\alpha, \ i = 0, 1, 2, 3, \) for any \( \chi \in P^* \setminus \{ \chi_0 \} \) (here we used the fact that \( \chi(E_3) = -\chi(D_3) \) if \( \chi \) is nonprincipal on \( P). \) Hence for any integer \( t \) relatively prime to \( p, \) \( \chi(E_i) = \sigma_t(\chi(E_i)) = \chi(E_i^{(t)}), \) \( i = 0, 1, 2, 3. \) If we use additive notation for the abelian group \( P, \) this means that if \( y \in E_i, \) then \( ty \in E_i, \) for \( t = 1, 2, \ldots, p - 1. \) From this we claim that \( 0 \not\in E_i \) (from now on we will use additive notation for the abelian group \( P) \) because if \( 0 \in E_i, \) then \( p - 1 | \frac{p^{2\alpha} - p^\alpha}{2} - 1, \) which is impossible. This shows that

\[
E_i = (< y_{i1} > \setminus \{0\}) \cup (< y_{i2} > \setminus \{0\}) \cup \cdots \cup (< y_{in} > \setminus \{0\}) \tag{4.4.19}
\]

where \( < y_{ij} > = \{ ty_{ij} \mid t \in GF(p) \}, \ y_{ij} \in GF(p^{2\alpha}) \setminus \{0\}, \ n = \frac{p^{\alpha}(p^{\alpha} - 1)}{2(p - 1)}, \ i = 0, 1, 2, 3, j = 1, 2, \ldots, n. \) Let \( O_i = \{ < y_{i1} >, < y_{i2} >, \ldots, < y_{in} > \}, \ i = 0, 1, 2, 3. \) We claim that \( O_i \) is an \((n, 2\alpha, \frac{n}{p^\alpha} - p^{\alpha - 1}, \frac{n}{p^\alpha} + p^{\alpha - 1})\) set in \( PG(2\alpha - 1, p). \) Let \( H \) be an arbitrary hyperplane of \( GF(p^{2\alpha}) \) which is regarded as a \( 2\alpha \)-dimensional vector space over \( GF(p). \) Assuming that \( \chi \) is an additive character of \( GF(p^{2\alpha}) \) such that \( \ker \chi = H, \) then

\[
\chi(E_i) = (p - 1)h + (-1)(n - h) \tag{4.4.20}
\]

where \( h \) is the number of \( y_{ij} \)'s in \( H, \ j = 1, 2, \ldots, n. \)

On the other hand, we also know that \( \chi(E_i) = 0 \) or \( \pm p^\alpha, \) hence

\[
(p - 1)h + (-1)(n - h) = 0, -p^\alpha, p^\alpha \tag{4.4.21}
\]
Solving this equation, we have
\[ h = \frac{n}{p} + (j - 2)p^{\alpha - 1}, \ j = 1, 2, 3. \]
Therefore \( \mathcal{O}_i \) is a projective \((n, 2\alpha, \frac{n}{p} - p^{\alpha - 1}, \frac{n}{p}, \frac{n}{p} + p^{\alpha - 1})\) set in \( PG(2\alpha - 1, p) \). Also the multiplicities can be calculated. We use \( m_{ij} \) to denote the number of hyperplanes in \( PG(2\alpha - 1, p) \) which meet \( \mathcal{O}_i \) in \( \frac{n}{p} + (j - 2)p^{\alpha - 1} \) points, \( i = 0, 1, 2, 3, \ j = 1, 2, 3 \). We define
\[ E^*_i = \{ \chi \in P^* \setminus \{ \chi_0 \} | \chi(E_i) \neq 0 \}, \ i = 0, 1, 2, 3. \]
It is easy to see that \( E^*_i = D^*_i, \ i = 0, 1, 2, 3 \). Since \( |D^*_i| = \frac{p^{2\alpha - 1} - 1}{4(p - 1)} \), we have
\[ m_{i2} = \frac{3(p^{2\alpha - 1})}{4(p - 1)}. \]
Let \( E^*_i = E^*_{i+} \cup E^*_{i-} \), where \( E^*_{i+} = \{ \chi \in E^*_i | \chi(E_i) = p^\alpha \} \), and \( E^*_{i-} = \{ \chi \in E^*_i | \chi(E_i) = -p^\alpha \} \). Since \( 0 \not\in E_i \), by the inversion formula, we have
\[ 0 = \frac{1}{p^\alpha} \frac{(p^{2\alpha} - p^\alpha)}{2} + (|E^*_{i+}| - |E^*_{i-}|)p^\alpha. \] (4.4.22)

Hence \( -\frac{p^\alpha - 1}{2} = |E^*_{i+}| - |E^*_{i-}| \), also \( |E^*_{i+}| + |E^*_{i-}| = \frac{p^{2\alpha} - 1}{4} \). Solving these two equations, \( |E^*_{i+}| = \frac{(p^\alpha - 1)^2}{8}, \ |E^*_{i-}| = \frac{(p^\alpha + 3)(p^\alpha - 1)}{8(p - 1)} \), hence \( m_{i1} = \frac{(p^\alpha + 3)(p^\alpha - 1)}{8(p - 1)} \), \( m_{i3} = \frac{(p^\alpha - 1)^2}{8(p - 1)}. \)

Since \( P^* \setminus \{ \chi_0 \} = E^*_0 \cup E^*_1 \cup E^*_2 \cup E^*_3, \ E_i^* \cap E_j^* = \emptyset, 0 \leq i < j \leq 3, \) we conclude that for each hyperplane \( H \), there is a unique \( i, 0 \leq i \leq 3, \) such that \( |H \cap \mathcal{O}_i| \neq \frac{n}{p}, \) and \( |H \cap \mathcal{O}_j| = \frac{n}{p}, \) if \( j \neq i. \)

Conversely, if there are four projective \((n, 2\alpha, \frac{n}{p} - p^{\alpha - 1}, \frac{n}{p}, \frac{n}{p} + p^{\alpha - 1})\) sets \( \mathcal{O}_i, i = 0, 1, 2, 3, \) in \( PG(2\alpha - 1, p) \) with \( n = \frac{p^{\alpha}(p^{\alpha - 1})}{4(p - 1)} \) satisfying the condition in the theorem, assume that \( \mathcal{O}_i = \{ < y_{ij} > | j = 1, 2, \ldots, n \}, \ i = 0, 1, 2, 3, \) define

\[ E_i = ( < y_{i1} > \setminus \{ 0 \}) \cup ( < y_{i2} > \setminus \{ 0 \}) \cup \cdots \cup ( < y_{in} > \setminus \{ 0 \}) \] (4.4.23)
and
\[ D = E_0 + aE_1 + bE_2 + ab\overrightarrow{E_3}, \] (4.4.24)
then it is easy to see that $D$ is a reversible Hadamard difference set in $G = Z_2 \times Z_2 \times (Z_p)^{2\alpha}$. This completes the proof of the theorem. □

**Remarks:**

1. McFarland [MC2] proved that if $D$ is a reversible HDS in an abelian group of order $4u^2$, then the square-free part of $u$ divides 6. That is the reason why we only consider the case $\alpha$ is even in Theorem 4.4.6.

2. The above theorem is useful in either construction or nonexistence proof of reversible HDS. On the construction side, we will see in next section that the point view we have taken in Theorem 4.4.6 can be used to give a new proof for Xia’s construction.

We conclude this section by proving Theorem 4.3.5 as we promised at the end of Section 3. Before preceding, we prove the following lemma.

**Lemma 4.4.7.** Let $D$ be a reversible $(4p^{2\alpha}, 2p^{2\alpha} - p^\alpha, p^{2\alpha} - p^\alpha)$-abelian difference set in $G = Z_2 \times Z_2 \times P$, where $|P| = p^{2\alpha}$, $p$ is an odd prime. Assume that the exponent of $P$ is $p^e$, $K$ is a subgroup of $P$ of order greater than $p^e$, and $E(K)$ is the subgroup of $K$ generated by all order $p$ elements of $K$. Then $|D \cap E(K)| = p(p - 1)m_1$, where $m_1$ is a nonnegative integer.

**Proof:** Assume that the Sylow 2-subgroup of $G$ is $\{1, a, b, ab\}$, taking a translate of $D$ by an element in $\{1, a, b, ab\}$ if necessary, we may write

$$D = D_0 + aD_1 + bD_2 + abD_3,$$

where $D_i \subset P$, $|D_i| = \frac{p^{(p^\alpha - 1)}}{2}$, $i = 0, 1, 2$, and $D_3 \subset P$, $|D_3| = \frac{p^n(p^\alpha + 1)}{2}$.

Since $D$ is reversible, we have $D_i^{(-1)} = D_i$, $i = 0, 1, 2, 3$, also from the proof of Theorem 4.4.3, we know that $\chi(D_i) = 0$ or $\pm p^\alpha$, $i = 0, 1, 2, 3$, for each nonprincipal character $\chi$ of $P$. Hence $D_i^{(t)} = D_i$ for all $t$, $(t, p) = 1$. We claim that the identity element is not in $D_0$. We prove the claim as follows.
Let $x \in D_0$, $\text{ord}(x) = p^\alpha$. Then $\{x^t | 1 \leq t \leq p^\alpha, (t,p) = 1\} \subset D_0$. We note that $|\{x^t | 1 \leq t \leq p^\alpha, (t,p) = 1\}| = \phi(p^\alpha) = p^\alpha - 1$. Iterating this procedure, $D_0$ is partitioned into a disjoint union of the orbits as above, each orbit has size divisible by $p - 1$. If the identity element is in $D_0$, then it is a singleton orbit, hence

$$p - 1 \left\lfloor \frac{p^\alpha(p^\alpha - 1)}{2} \right\rfloor - 1 = \frac{(p^\alpha - 2)(p^\alpha + 1)}{2}$$

(4.4.26)

which is impossible. Therefore the claim is proved.

Let $D \cap K = C_1$, $H = \{1, g_2, \ldots, g_h\}$ be a complete set of coset representatives of $K$ in $P$. We write

$$D_0 = C_1 + g_2 C_2 + \cdots + g_h C_h$$

(4.4.27)

where $C_i \subset K$, $i = 1, 2, \ldots, h$.

For any nonprincipal character $\chi$ of $K$, we can extend it in $h$ ways to $P$. Assume that the extensions are $\chi_1, \chi_2, \ldots, \chi_h$, applying these characters to (4.4.27), we have

$$\chi_i(D_0) = \chi(C_1) + \chi_i(g_2)\chi(C_2) + \cdots + \chi_i(g_h)\chi(C_h)$$

(4.4.28)

$i = 1, 2, \ldots, h$.

Hence $\sum_{i=1}^h \chi_i(D_0) = \chi(C_1)h$, therefore

$$\chi(C_1) = \frac{1}{h} \sum_{i=1}^h \chi_i(D_0)$$

$$= \frac{1}{h} (A - B) p^\alpha$$

$$= (A - B) \frac{|K|}{p^\alpha}$$

where $A = |\{\chi_i| \chi_i(D_0) = p^\alpha, 1 \leq i \leq h\}|$, $B = |\{\chi_i| \chi_i(D_0) = -p^\alpha, 1 \leq i \leq h\}|$. 

Since $|K| > p^a$, we have

$$\chi(C_i) \equiv 0 \pmod{p}. \quad (4.4.29)$$

On the other hand, $(D \cap K) \setminus (D \cap E(K))$ has no element of order $p$, and $(D \cap K) \setminus (D \cap E(K))^{(t)} = (D \cap K) \setminus (D \cap E(K))$ for all $t, (t, p) = 1$. So

$$(D \cap K) \setminus (D \cap E(K)) = \bigcup_{x} \bigcup_{1 \leq i \leq (p-1)} x^i < x^p. \quad (4.4.30)$$

Hence for each $\chi$ nonprincipal on $K$, we have

$$\chi(D \cap K) \equiv \chi(D \cap E(K)) \pmod{p}. \quad (4.4.31)$$

But $\chi(C_i) \equiv 0 \pmod{p}$, it follows that $\chi(D \cap E(K)) \equiv 0 \pmod{p}$. Noting that $(D \cap E(K))^{(t)} = D \cap E(K)$, for all $t, (t, p) = 1$, we have $D \cap E(K) = \bigcup_{i=1}^{m} L_i$, where $L_i = \{x, x^2, \ldots, x_i\}$, $x_i$ is an order $p$ element in $K$. $\chi(\bigcup_{i=1}^{m} L_i) = -a + (m-a)(p-1) = p(m-a) - m$, if $\chi$ is nonprincipal on a $L_i$'s. Recall that $\chi(D \cap E(K)) \equiv 0 \pmod{p}$, we have $p|m$, and the lemma follows. This completes the proof. □

**Proof of Theorem 4.3.5:** Let $D$ be a reversible Hadamard difference set in $Z_2 \times Z_2 \times Z_9 \times Z_9$, and $\{1, a, b, ab\}$ be the Sylow 2-subgroup. Without loss of generality, we assume that

$$D = D_0 + aD_1 + bD_2 + abD_3, \quad (4.4.32)$$

where $D_i \subset Z_9 \times Z_9$, $|D_i| = 36$, $i = 0, 1, 2$, and $D_3 \subset Z_9 \times Z_9$, $|D_3| = 45$. $\chi(D_i) = 0$ or $\pm 9$ for each nonprincipal character $\chi$ of $Z_9 \times Z_9$.

Let $P = Z_9 \times Z_9$, $E(P)$ be the subgroup of $P$ generated by all order 3 elements of $P$. Then $E(P) \cong Z_3 \times Z_3$. By Lemma 4.4.7, $|D_0 \cap E(P)| = 0$ or $3(3-1) = 6$. We distinguish two cases.
Case 1. $D_0 \cap E(P) = \emptyset$. In this case every $x \in D_0$ has order 9. Since $D_0^{(t)} = D_0$ for all $t$, $(t, 3) = 1$. So

$$D_0 = \bigcup_{i=1}^{6} < x_i > \setminus < x_i^3 >,$$

(4.4.33)

where $x_i$, $1 \leq i \leq 6$, are 6 distinct elements in $P$ of order 9. We will call $< x_i > \setminus < x_i^3 >$ a building block of $D_0$.

Let $P^*$ be the character group of $P$. Define $P_{3i}^* = \{ \chi \in P^* | \text{ord}(\chi) = 3^i \}$, $i = 1, 2$. It is easy to see that $|P_{3i}^*| = 3^{2i} - 3^{2(i-1)}$, $i = 1, 2$. Let $\xi_{3^i}$ be a primitive $3^i$-th root of unity. Then $\text{Gal}(Q(\xi_{3^i}))/Q$ acts on $P_{3i}^*$ via $g \mapsto \sigma(\chi(g))$, $g \in P$, where $\sigma \in \text{Gal}(Q(\xi_{3^i}))/Q$ and $\chi \in P_{3i}^*$, $i = 1, 2$. $P_{3i}^*$ is thus partitioned into $\frac{3^{2i} - 3^{2(i-1)}}{\phi(3^i)} = 4 \cdot 3^{i-1}$ orbits under this action. Say $P_{3i}^* = O_1 \cup O_2 \cup O_3 \cup O_4$ and $P_{3i}^* = O_{11} \cup O_{12} \cup O_{13} \cup \cdots \cup O_{43}$. Any two characters in the same orbit have the same kernel. Let $H_i$ be the kernel of $\chi \in O_i$, $i = 1, 2, 3, 4$, and $H_{ij}$ be the kernel of $\chi \in O_{ij}$, $1 \leq i \leq 4$, $1 \leq j \leq 3$. It is easy to see that $H_i \cong Z_9 \times Z_3$, also each $H_i$ contains 3 distinct subgroups isomorphic to $Z_9$, we call those 3 subgroups $H_{i1}, H_{i2},$ and $H_{i3}$. It is helpful to summarize the above information in the following diagram (Diagram 4.4.1).

\[
\begin{array}{cccc}
H_1 & H_2 & H_3 & H_4 \\
\cup & \cup & \cup & \cup \\
H_{11} & H_{21} & H_{31} & H_{41} \\
H_{12} & H_{22} & H_{32} & H_{42} \\
H_{13} & H_{23} & H_{33} & H_{43}
\end{array}
\]
We consider the following cases.

Case 1a. Every column in the above diagram contributes at least one block to $D_0$. WLOG we assume that

$$D_0 = \bigcup_{i=1}^{4} (H_{i1} \setminus H_{i1}^{(3)}) \cup (H_{i2} \setminus H_{i2}^{(3)}) \cup (H_{i3} \setminus H_{i3}^{(3)})$$

(4.4.34)

or

$$D_0 = \bigcup_{j=1}^{3} (H_{1j} \setminus H_{1j}^{(3)}) \cup (H_{21} \setminus H_{21}^{(3)}) \cup (H_{31} \setminus H_{31}^{(3)}) \cup (H_{41} \setminus H_{41}^{(3)})$$

(4.4.35)

where $H_{ij}^{(3)}$ is the unique subgroup of order 3 in $H_{ij}$.

In the first case, we choose $\chi \in P^*$ such that $ord(\chi) = 9$ and $ker\chi = H_{11}$, we have $\chi(D_0) = (-2)3 + 9 = 3$, contradicting $\chi(D_0) = 0$ or $\pm 9$. In the second case, choosing $\chi \in P^*$ such that $ord(\chi) = 9$, $ker\chi = H_{21}$, we have $\chi(D_0) = -3 + 9 = 6$, again contradicting $\chi(D_0) = 0$ or $\pm 9$.

Case 1b. Only three columns in Diagram 4.4.1 contribute at least one block to $D_0$. WLOG we assume that

$$D_0 = \bigcup_{i=1}^{3} \bigcup_{j=1}^{2} (H_{ij} \setminus H_{ij}^{(3)})$$

(4.4.36)

or

$$D_0 = \bigcup_{j=1}^{3} (H_{1j} \setminus H_{1j}^{(3)}) \cup (H_{21} \setminus H_{21}^{(3)}) \cup (H_{31} \setminus H_{31}^{(3)}) \cup (H_{41} \setminus H_{41}^{(3)})$$

(4.4.37)

In both cases, choosing $\chi \in P^*$, $ord(\chi) = 3$, $ker\chi = H_4$, we have $\chi(D_0) = (-3)6 = -18$, contradicting $\chi(D_0) = 0$ or $\pm 9$.

Case 1c. Only two columns in Diagram 4.4.1 contribute at least one block to $D_0$. WLOG we assume that

$$D_0 = \bigcup_{i=1}^{2} \bigcup_{j=1}^{3} (H_{ij} \setminus H_{ij}^{(3)})$$

(4.4.38)
choosing $\chi \in P^*$, $\text{ord}(\chi) = 3$, $\text{ker} \chi = H_4$, we have $\chi(D_0) = (-3)6 = -18$, contradicting $\chi(D_0) = 0$ or ±9.

Case 2. $|D_0 \cap E(P)| = 6$. We assume that $D_0 \cap E(P) = \cup_{i=1}^3 (H_{4i}^{(3)} \setminus \{1\})$. Since $|D_0| = 36$, we have $|D_0 \setminus D_0 \cap E(P)| = 30$.

Case 2a. If $H_{4i} \setminus H_{4i}^{(3)} \subset D_0$, $i = 1, 2, 3$, then we may assume that either $H_{4i} \setminus H_{4i}^{(3)} \subset D_0$, $i = 1, 2$, or $H_{4j} \setminus H_{4j}^{(3)} \subset D_0$, $j = 1, 2$. In both cases, choosing $\chi \in P^*$, $\text{ord}(\chi) = 3$, $\text{ker} \chi = H_4$, we have $\chi(D_0) = 18$, contradicting $\chi(D_0) = 0$ or ±9.

Case 2b. If $H_{4i} \setminus H_{4i}^{(3)} \subset D_0$, $i = 1, 2, 3$, then we need three more blocks for $D_0$ from the first three columns in Diagram 4.4.1.

Case 2c. If $H_{4i} \setminus H_{4i}^{(3)} \subset D_0$, then we need four more blocks for $D_0$ from the first three columns in Diagram 4.4.1.

Case 2d. The last column in Diagram 4.4.1 does not contribute to $D_0$. We need five blocks for $D_0$ from the first three columns in Diagram 4.4.1.

In these three cases, by choosing an appropriate character of $P$ and calculating the corresponding character value of $D_0$, we also reach a contradiction. This completes the proof. □

5. On Xia’s Construction

Recently Xia [X] constructed Hadamard difference sets in groups $H \times Z_{p_1}^4 \times \cdots \times Z_{p_t}^4$, where $H$ is either the Klein 4-group or the cyclic group of order 4 and each $p_j$ is a prime congruent to 3 modulo 4. This is a major advance in the field of difference sets. But Xia’s construction depends on very complicated calculations involving cyclotomic classes of high orders, therefore it is not clear
why the construction works.

In this section, based on Theorem 4.4.6, we present a new way of viewing Xia's construction, which allows us to give a character theoretic proof for Xia's construction that is more transparent than the original proof in [X].

Assume that $p$ is a prime congruent to 3 (mod 4). Let $q = p^{2s}$, where $s$ is a positive even integer. Applying Theorem 1.4.1 to the case $e = 4$, $j = 1$, $\gamma = s$, we have

$$\eta_0 = \frac{p^s - 1}{4} - p^s, \eta_i = \frac{p^s - 1}{4}, i \neq 0 \quad (4.5.1)$$

Let $B_i = \{ \chi_{g^k} \in G^* : k \equiv i (\text{mod } 4) \}, i = 0, 1, 2, 3$, where $g$ is a fixed primitive element of $GF(q)$, $G^*$ is the group of additive characters on $GF(q)$. Also the subscript in $B_i$ is to be interpreted modulo 4. Then

$$\chi_{g^i}(C_0) = \begin{cases} \frac{p^s - 1}{4} - p^s, & \text{if } \chi_{g^i} \in B_0; \\ \frac{p^s - 1}{4}, & \text{if } \chi_{g^i} \not\in B_0. \end{cases} \quad (4.5.2)$$

We now regard $GF(q)$ as a 2-dimensional vector space over $GF(p^s)$. Then any 1-dimensional subspace of $GF(q)$ over $GF(p^s)$ has the form $\{g^{(p^s+1)t+i} : t = 0, 1, 2, \ldots, p^s - 2 \} \cup \{0\}$ for some $i$. We will use $H_i = \langle g^i \rangle$ to denote the punctured line $\{g^{(p^s+1)t+i} : t = 0, 1, 2, \ldots, p^s - 2 \}$. Let $L_0 = \langle g^1 \rangle \cup \langle g^5 \rangle \cup \cdots \cup \langle g^{(\frac{p^s-1}{4})} \rangle$. Then for any nontrivial $\chi_\beta \in G^*$, $\chi_\beta$ is either nontrivial on every $H_{4i+1}, i = 0, 1, \ldots, \frac{p^s-1}{4} - 1$, or trivial on exactly one $H_{4k+1}$ for some $k, 0 \leq k \leq \frac{p^s-1}{4} - 1$. Hence by Lemma 1.4.3, we have

$$\chi_\beta(L_0) = \begin{cases} -\frac{p^s-1}{4}, & \text{if } \chi_\beta \in N; \\ p^s - \frac{p^s-1}{4}, & \text{if } \chi_\beta \in T. \end{cases} \quad (4.5.3)$$

where $T = \{ \chi_\beta \in G^* : \chi_\beta \text{ is trivial on exactly one } H_{4k+1}, \text{ for some } k, 0 \leq k \leq \frac{p^s-1}{4} - 1 \}.$
Let $D_0 = C_0 \cup L_0$, and $D_0^* = \{\chi_{\beta} \in G^* \setminus \{\chi_0\} : \chi_{\beta}(D_0) \neq 0\}$. It is easy to see that $D_0$ has no repeated elements, and $|D_0| = \frac{q^s - \sqrt{q}}{2}$. Furthermore, we have the following lemma.

**Lemma 4.5.1.** $\chi_{\beta}(D_0) = 0$ or $\pm p^s$ for every $\beta \neq 0$, and $D_0^* = (T \cap B_2) \cup (N \cap B_0)$, $|D_0^*| = \frac{q-1}{4}$.

**Proof:** For any $\beta \neq 0$, $\chi_{\beta}(D_0) = \chi_{\beta}(C_0) + \chi_{\beta}(L_0)$. Combining (4.5.2) and (4.5.3), we see that

$$\chi_{\beta}(D_0) = 0, \text{or } \pm p^s$$

(4.5.4)

Now let us write out the elements of $T$ explicitly. Recall that $T = \{\chi_{g^t} \in G^* : \chi_{g^t}$ is trivial on exactly one $H_{4k+1}$, for some $k$, $0 \leq k \leq \frac{p^s-1}{4} - 1\}$.

$\chi_{g^t}$ is trivial on $H_{4k+1} = \{g^{(p^s+1)t+4k+1} : t = 0, 1, 2, \ldots, p^s - 2\}$

$\Leftrightarrow T_r(g^{(p^s+1)t+4k+1+i}) = 0$ for all $t = 0, 1, \ldots, p^s - 2$. and by Lemma 1.4.5.

$\Leftrightarrow \beta^{p^s-1} = -1, \text{ where } \beta = g^{i+4k+1}$

$\Leftrightarrow i + 4k + 1 = j\frac{p^s+1}{2}, 1 \leq j \leq 2(p^s - 1), \text{ } j \text{ is odd.}$

Therefore $T = \{\chi_{g^t} \in G^* : i = j\frac{p^s+1}{2} - (4k + 1), 1 \leq j \leq 2(p^s - 1), 0 \leq k \leq \frac{p^s-1}{4} - 1, \text{ } j \text{ is odd}\}$. $|T| = \frac{(p^s-1)^2}{4}$. Also we note that if $\chi_{g^t} \in T$, then

$i = \frac{p^s+1}{2}j - (4k + 1) \equiv 0 \text{ or } 2(\text{mod } 4)$, and $|T \cap B_0| = |T \cap B_2| = \frac{|T|}{2}$.

From (4.5.2) and (4.5.3), we see that $D_0^* = (T \cap B_2) \cup (N \cap B_0)$.

Therefore $|D_0^*| = |T \cap B_2| + |N \cap B_0| = |T \cap B_2| + |B_0| - |T \cap B_0| = |B_0| = \frac{q-1}{4}$.

This completes the proof. □
Let \( D_2 = g^{(p^s+1)}D_0 = C_2 \cup L_0, \quad D_2^* = \{ \chi_\beta \in G^* \setminus \{ \chi_0 \} : \chi_\beta(D_2) \neq 0 \} \).

Then we have

**Lemma 4.5.2.** \( \chi_\beta(D_2) = 0, \) or \( \pm p^s \) for every \( \beta \neq 0, \) and \( D_2^* = (T \cap B_0) \cup (N \cap B_2), \quad |D_2^*| = \frac{q-1}{4}. \)

The proof of this lemma is similar to that of Lemma 4.5.1, therefore we omit the proof.

Now let \( D_1 = g^tD_0 = C_t \cup L_1, \) where \( t \) is a positive odd integer,

\( L_1 = \langle g^{t+1} \rangle \cup \langle g^{t+5} \rangle \cup \cdots \cup \langle g^{t+1+\left(\frac{p^s-1}{4}\right)} \rangle, \) and let \( D_3 = g^{(p^s+1)}D_1 = C_{t+2} \cup L_1. \quad D_3^* \) and \( D_3^* \) are similarly defined as \( D_0^* \) and \( D_2^*. \) Also we set \( T' = \{ \chi_{g^i} \in G^* : \chi_{g^i}(L_1) = p^s - \frac{p^s-1}{4} \}, \quad N' = \{ \chi_{g^j} \in G^* : \chi_{g^j}(L_1) = -\frac{p^s-1}{4} \}. \) We have

the following lemma

**Lemma 4.5.3.** \( \chi_\beta(D_i) = 0, \) or \( \pm p^s \) for every \( \beta \neq 0, \) \( i = 1, 3. \) And \( D_1^* = (T' \cap B_1) \cup (N' \cap B_{t+2}), \quad D_3^* = (T' \cap B_{t+2}) \cup (N' \cap B_t), \quad |D_1^*| = |D_3^*| = \frac{q-1}{4}. \)

**Proof:** The proof for the first part is obvious from (4.5.1) and (4.5.2). For the proof of the second part, we note that \( T' = \{ \chi_{g^i} \in G^* : i = j\frac{p^s+1}{2} - (4k+1) - t, 1 \leq j \leq 2(p^s - 1), 0 \leq k \leq \frac{p^s-1}{4} - 1, \) \( j \) is odd\}; if \( \chi_{g^i} \in T', \) then \( i \equiv \pm 1 (mod 4). \) The rest of the proof is the same as that of Lemma 4.5.1. \( \square \)

We are now ready to construct HDS in \( K \times G \) and \( C \times G, \) where \( K = \{ 1, a, b, ab \} \) is the elementary 2-group of order 4, and \( C = \{ 1, c, c^2, c^3 \} \) is the cyclic group of order 4. We use multiplicative notation for the group operation even though \( G \) is the additive group of \( GF(q), \) \( q = p^{2s}, \) \( s \) is even. Also we use \( 1_G \) to denote the identity element of \( G. \)

Let \( D = D_0 + aD_1 + bD_2 + ab\overline{D}_3, \) and \( E = D_0 + cD_1 + c^2D_2 + c^3\overline{D}_3, \) where \( \overline{D}_3 = G \setminus D_3. \) Then we have
**Theorem 4.5.4.** \(D\) is a \((4p^{2s}, 2p^{2s} - p^s, p^{2s} - p^s)\)-difference set in \(K \times G\), \(D(-1) = D\). \(E\) is a \((4p^{2s}, 2p^{2s} - p^s, p^{2s} - p^s)\)-difference set in \(C \times G\), where \(p\) is a prime congruent to 3 (mod 4) and \(s\) is even.

**Proof:** From the three lemmas above, we see that \(D_0^*, D_1^*, D_2^*, D_3^*\) form a partition of \(G^* \setminus \{x_0\}\). Also \(\chi_{\beta}(D_i) = 0\) or \(\pm p^s\) for every \(\beta \neq 0, i = 0, 1, 2, 3\). Therefore \(\chi_{\beta}(\sum_{i=0}^{3} D_i D_i^{(-1)}) = q, \chi_{\beta}(D_i D_j^{(-1)}) = 0, i \neq j\) for every \(\beta \neq 0\). By Lemma 1.4.4, we have

\[
\sum_{i=0}^{3} D_i D_i^{(-1)} = q_1 G + \lambda_1 G \quad (4.5.5)
\]

\[
D_i D_j^{(-1)} = \frac{\lambda_2}{4} G, 0 \leq i \neq j \leq 3 \quad (4.5.6)
\]

where \(\lambda_1, \lambda_2\) are two integers.

Applying \(\chi_0\) to the above two equations, we get

\[
\lambda_1 = q - 2\sqrt{q}, \lambda_2 = q - 2\sqrt{q} + 1 \quad (4.5.7)
\]

Changing \(D_3\) to its complement \(D_3^*\) in \(G\), it is easy to see that

\[
D_0 D_0^{(-1)} + D_1 D_1^{(-1)} + D_2 D_2^{(-1)} + D_3 D_3^{(-1)} = p^{2s} 1_G + (p^{2s} - p^s)G
\]

\[
D_0 D_1^{(-1)} + D_1 D_0^{(-1)} + D_2 D_3^{(-1)} + D_3 D_2^{(-1)} = (p^{2s} - p^s)G
\]

\[
D_0 D_2^{(-1)} + D_2 D_0^{(-1)} + D_1 D_3^{(-1)} + D_3 D_1^{(-1)} = (p^{2s} - p^s)G
\]

\[
D_0 D_3^{(-1)} + D_3 D_0^{(-1)} + D_1 D_2^{(-1)} + D_2 D_1^{(-1)} = (p^{2s} - p^s)G \quad (4.5.8)
\]

Hence \((D_0 + a D_1 + b D_2 + ab D_3)(D_0^{(-1)} + a D_1^{(-1)} + b D_2^{(-1)} + ab D_3^{(-1)}) = p^{2s} + (p^{2s} - p^s)(K \times G)\). This shows that \(D\) is \((4p^{2s}, 2p^{2s} - p^s, p^{2s} - p^s)\)-difference set \(K \times G\). Since -1 is a 4-th power in \(GF(q)\), \(q = p^{2s}, s\) is even, we have \(D_i^{(-1)} = D_i\).
thus $D^{(-1)} = D$. Similarly, it is easy to show that $E$ is a $(4p^{2s}, 2p^{2s} - p^s, p^{2s} - p^s)$-difference set in $C \times G$. This completes the proof. □

Remarks: (1). We note that in the above construction, $D_1 = g^tD_0$, where $t$ is any odd integer, while the construction in [X] chose $t$ to be $\frac{p^t+1}{2}$ (Prof. Xia also pointed out this improvement to us in [XI]). Also we have some freedom in choosing $L_0$. For example, if we choose $L_0$ to be $g^\alpha > \cup g^{\alpha+4} > \cup \ldots \cup g^{\alpha+\left(\frac{p^t-1}{4}-1\right)4}$, where $\alpha$ is any odd integer, the above construction still works.

(2). When $p$ is a prime congruent to 1 (mod 4), the 4-th cyclotomic periods of $GF(q)$, $q = p^r$, take 4 different values. In this case, if we still use the same method as above to construct $D_0$, the character values of $D_0$ will take more than 3 distinct values, so this $D_0$ can not be used to construct an Hadamard difference set.

(3). If we do not switch $D_3$ to its complement in $G$ in the above construction, we will get $(4, p^{2s}, 2(p^{2s} - p^s), \lambda_1, \lambda_2)$-divisible difference sets in $K \times G$, and $C \times G$, where $\lambda_1$ and $\lambda_2$ are the same as those in the proof of Theorem 4.5.4. In the first case, the divisible difference set is reversible (i.e. it is fixed by -1).

Finally, using a well known composition theorem of Hadamard difference sets (for example see [X]), it is now routine to construct Hadamard difference sets in $H \times Z_{p_1}^4 \times \cdots \times Z_{p_t}^4$, where $H$ is either group of order 4, and each $p_j$ is a prime congruent to 3 (mod 4).

In the following, we show that the above construction gives rise to a class of three-weight codes. Recall that we constructed a set $D_0 = C_0 \cup L_0$ in
$GF(q)$, $q = p^{2s}$, $s$ is even, $p \equiv 3 \pmod{4}$, $|D_0| = \frac{q-\sqrt{q}}{2}$. It is easily seen that $GF(p^*)D_0 = D_0$ (here we are using additive notation for $D_0$), where $GF(p^*) = GF(p) \setminus \{0\}$. Therefore we have

$$D_0 = (<y_1> \setminus \{0\}) \cup (<y_2> \setminus \{0\}) \cup \cdots \cup (<y_n> \setminus \{0\}) \quad (4.5.9)$$

where $<y_i> = \{sy_i : s \in GF(p)\}$, for some $y_i$'s in $GF(q)^*$, $n = \frac{p^s(p^s-1)}{2(p-1)}$.

Let $O = \{<y_1>, <y_2>, \ldots, <y_n>\}$, $C = \{(x \cdot y_1, x \cdot y_2, \ldots, x \cdot y_n) : x \in GF(p^{2s})\}$, where $x \cdot y_i$ is the dot product. We have the following proposition.

**Proposition 4.5.5.** $O$ is a projective $(n, 2s, \frac{n}{p} - p^{s-1}, \frac{n}{p}, \frac{n}{p} + p^{s-1})$ set in $PG(2s-1, p)$. $C$ is a projective three-weight $[n, 2s]$ code with nonzero weights $w_i = n - \frac{n}{p} - (i-2)p^{s-1}$, $i = 1, 2, 3$.

**Proof:** Let $H$ be an arbitrary hyperplane of $GF(p^{2s})$ which is regarded as a 2s-dimensional vector space over $GF(p)$. Assume that $\chi$ is an additive character of $GF(p^{2s})$ such that $Ker\chi = H$, then by Lemma 1.4.3, we have

$$\chi(D_0) = (p-1)h + (-1)(n-h) \quad (4.5.10)$$

where $h$ is the number of $y_i$'s in $H$.

By Lemma 4.5.1, we also know that $\chi(D_0) = 0$ or $\pm p^s$, hence

$$(p-1)h + (-1)(n-h) = 0, -p^s, p^s \quad (4.5.11)$$

Solving this equation, we have $h = \frac{n}{p} + (i-2)p^{s-1}$, $i = 1, 2, 3$. Therefore $O$ is a projective $(n, 2s, \frac{n}{p} - p^{s-1}, \frac{n}{p}, \frac{n}{p} + p^{s-1})$ set in $PG(2s-1, p)$. Also the multiplicities can be calculated. We use $m_i$ to denote the number of hyperplanes in $PG(2s-1, p)$ which meet $O$ in $\frac{n}{p} + (i-2)p^{s-1}$ points, $i = 1, 2, 3$. From the
proof of Lemma 4.5.1, we know that \(|D_0^*| = \frac{p^{2s} - 1}{4}, \ |T \cap B_2| = \frac{|T|}{2} = \frac{(p^s-1)^2}{8}, \ |N \cap B_0| = |B_0| - |T \cap B_0| = \frac{(p^s+3)(p^s-1)}{8}, \) hence \(m_2 = \frac{3(p^{2s}-1)}{4(p-1)}, \ m_1 = \frac{(p^s+3)(p^s-1)}{8(p-1)}, \ m_3 = \frac{(p^s-1)^2}{8(p-1)}.\)

From (4.5.9), we see that no two \(y_i\)'s are linearly dependent over \(GF(p),\) hence \(C\) is a projective code. Let \(x\) be any non-zero vector in \(GF(p^2).\) If \(x^\perp = \{y \in GF(p^2) : x \cdot y = 0\},\) then \(n - |x^\perp \cap \{y_1, y_2, \ldots, y_n\}|\) is the weight of the codeword \((x \cdot y_1, \ldots, x \cdot y_n),\) from the first part of the proof, we see that

\[
|x^\perp \cap \{y_1, y_2, \ldots, y_n\}| = \frac{n}{p} \pm \frac{p^s-1}{p}. \tag{4.5.12}
\]

Therefore \(C\) is a projective three-weight \([n, 2s]\) code with nonzero weights \(w_i = n - \frac{n}{p} - (i - 2)p^{s-1}, i = 1, 2, 3.\) The number \(A_{w_i}\) of codewords with weight \(w_i\) can also be calculated. From the \(m_i\)'s, we see that \(A_{w_2} = \frac{3(p^{2s}-1)}{4}, \ A_{w_1} = \frac{(p^s+3)(p^s-1)}{8}, \ A_{w_3} = \frac{(p^s-1)^2}{8}.\) This completes the proof. \(\Box\)

We conclude this section by remarking that Xia's construction also gives rise to non-abelian Hadamard difference sets fixed by -1.

For example, let \(G = \langle b \rangle \times H < a >, < b > \cong < a > \cong Z_2, \ H \cong (Z_p)^{2s}, [b, x] = 1, \) for all \(x \in G, \ aya^{-1} = y^{-1}, \) for all \(y \in H, \) where \(s\) is even, and \(p\) is a prime congruent to 3 (mod 4). Let \(D = D_0 + aD_1 + bD_2 + abD_3,\) where \(D_i, i = 0, 1, 2, 3,\) are same as those in Theorem 4.5.4. Then by (4.5.5) and (4.5.6), it is easy to see that \(D\) is a \((4p^{2s}, 2p^{2s} - p^s, p^{2s} - p^s)-\)difference set in \(G,\) and it is fixed by -1.
Chapter V

Further Research Problems

We conclude this work by presenting a few problems related to the materials treated in previous chapters.

Let $G$ be an abelian group of order $v$, with exponent $e_G$, $D$ a $(v, k, \lambda)$-difference set in $G$, and $M$ the numerical multiplier group of $D$. By a result of McFarland and Rice [MR], we may assume that $D$ is fixed by every element of $M$. Let $K_G = Q(\xi_{e_G})$, $K_D = Q(\chi_0(D), \chi_1(D), \cdots, \chi_{v-1}(D))$, where $\xi_{e_G}$ is a primitive $e_G$-th root of unity, and $\{\chi_0, \chi_1, \cdots, \chi_{v-1}\} = G^*$, the character group of $G$. Then by Lemma 2.2.1 in Chapter II, we have $M = \text{Gal} K_G/K_D$. In Chapter III and IV, we studied the cases $K_D$ a quadratic extension of $Q$, and $K_D = Q$ in some depth. Here we ask the following question.

**Research Problem 5.1.** Does there exist a nontrivial $(v, k, \lambda)$-difference set $D$ in an abelian group $G$ with trivial numerical multiplier group if $e_G > 6$ (In fact, we are more interested in whether there exists such a $D$ with $n \nmid v$, where $n = k - \lambda$)?

We notice that if such a $D$ exists, then $K_D = K_G$. If $e_G$ is small, there are abelian difference sets with trivial numerical multiplier group. For example, there exist many Hadamard difference sets in elementary abelian 2-groups, all
these difference sets have trivial numerical multiplier group. As another example, the Paley-Hadamard difference sets in the additive group of $GF(3^\alpha)$, $\alpha$ is odd, also have trivial numerical multiplier group.

This problem is clearly related to the multiplier conjecture, so it may be very difficult at present.

**Research Problem 5.2.** Classify all abelian difference sets with $K_D=$ a quadratic extension of $\mathbb{Q}$, in particular, prove that the only skew Hadamard difference sets in abelian $p$-groups are Paley-Hadamard.

So far, the known examples of abelian difference sets with $K_D=$ a quadratic extension of $\mathbb{Q}$ are Paley-Hadamard and twin prime power difference sets (see [JU1] for a description of twin prime power difference sets), are these the only examples?

In chapter II, we proved that if $D$ is a $(v, k, \lambda)$-difference set in a cyclic group $G$ of order $v$, $M$ is the multiplier group of $D$, and $D \neq \pm\{3, 6, 7, 12, 14\}$ in $\mathbb{Z}_{21}$, then $|M| \leq k$. We also pointed out that there are cyclic $(v, k, \lambda)$-difference sets such that the size of the multiplier groups of the difference sets is $k$. For example, the quadratic residue difference sets in $\mathbb{Z}_p$, where $p$ is a prime, $p \equiv 3(\text{mod } 4)$. Here we pose the following problem.

**Research Problem 5.3.** Characterize those cyclic $(v, k, \lambda)$-difference sets whose multiplier groups have size $k$. We conjecture that if $D$ is a cyclic $(v, k, \lambda)$-difference set, and the multiplier group of $D$ has size $k$, then $v$ is prime.

For $\lambda = 1$, we refer the reader to [HO], [HO1] for results related to the above problem. In particular, Ho [HO] proved the following theorem.
**Theorem 5.1.** Let $M$ be the group of multipliers of a cyclic planar difference set of order $n$. Then $|M| \leq n + 1$, unless $n = 4$ (where $|M| = 6$). Moreover, the following hold:

1. If $|M| = n + 1$, then $n$ is even and $n^2 + n + 1$ is a prime.
2. If $|M| = n$, then $n$ is an odd multiple of 3 and $n^2 + n + 1$ is a prime.
3. $|M| \neq n - 1$.
4. $|M| = n - 2$ if and only if $n = 5$, and $|M| = n - 3$ if and only if $n = 9$.

We remark that Problem 5.3 is also related to the following problem in finite geometry.

It is widely conjectured that a finite projective plane admitting a flag-transitive collineation group is desarguesian. Results of Kantor [K] and Feit [F] imply the following.

**Theorem 5.2.** Let $P$ be a projective plane of order $n$ admitting a flag-transitive collineation group $G$. Then either

1. $P$ is desarguesian and $PSL(3, n)$ is a subgroup of $G$, or
2. $G$ acts regularly on flags (and thus is a Frobenius group), and $n^2 + n + 1$ is a prime $p$. If $n \neq 2, 8$, then $P$ is a nondesarguesian cyclic plane. In this case, $n$ is divisible by 8 but $n$ is not a power of 2, and $P = d e v D$, where $D$ consists of the $n$th powers in $Z_p^*$; moreover, $D$ coincides with its multiplier group $M$ and contains all divisors of $n$.

If the conjecture that a finite projective plane admitting a flag-transitive collineation group is desarguesian is true, then we should be able to prove the difference set $D$ in Case (2) of Theorem 5.2 does not exist. This remains open.
at present. The connection of this problem with Problem 5.3 is obvious since the multiplier group $M$ of the difference set $D$ in Case (2) of Theorem 5.2 has size $|D| = n + 1$.

In Chapter IV, we proved that there does not exist a reversible Hadamard difference set in $Z_2 \times Z_2 \times Z_9 \times Z_9$. In general, we pose the following problem.

**Research Problem 5.4.** Let $D$ be a reversible HDS in an abelian group $G$, let $p^{2s}$ and $p^e$ be the order and exponent of the Sylow $p$-subgroup of $G$ respectively, where $p$ is an odd prime. Is it true that $e \leq s/2$?

Finally, in Chapter IV, we showed that certain reversible Hadamard difference sets can give rise to projective three-weight codes and vice versa. Also we gave a simple proof for Xia’s construction. Xia’s construction only works for primes congruent to 3 (mod 4). So far we do not know whether there exists a Hadamard difference set in $Z_2 \times Z_2 \times (Z_p)^4$, where $p$ is a prime congruent to 1 (mod 4), the smallest open case is $p = 5$. In view of Theorem 4.4.6, we ask the following question

**Research Problem 5.5.** Does there exist a 5-ary $[75, 4]$ linear code $C$ with weight enumerator

$$W_C(x, y) = x^{75} + 72x^{20}y^{55} + 468x^{15}y^{60} + 84x^{10}y^{65}?$$

In general, does there exist a $p$-ary $[n, 2s]$ linear code $C$ with weight enumerator

$$W_C(x, y) = x^n + A_1 x^{n-w_1} y^{w_1} + A_2 x^{n-w_2} y^{w_2} + A_3 x^{n-w_3} y^{w_3}?$$

where $n = \frac{p^{2s-1}}{2(p-1)}$, $w_i = n - \frac{n}{p} + (i - 2)p^{s-1}$, $i = 1, 2, 3$, $A_1 = \frac{(p^{s-1})^2}{8}$, $A_2 = \frac{3(p^{2s-1})}{4}$, $A_3 = \frac{(p^{s+3})(p^{s-1})}{8}$, $s$ is even and $p \equiv 1 \pmod{4}$. 
References


[ST] Storer, J., Cyclotomy and difference sets, Markham, Chicago (1967)


