The interplay of designs and difference sets

Huang, Yiwei

2011

Huang, Y. W. (2011). The interplay of designs and difference sets. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/43666>

<https://doi.org/10.32657/10356/43666>

**NANYANG
TECHNOLOGICAL
UNIVERSITY**

**THE INTERPLAY OF DESIGNS AND
DIFFERENCE SETS**

HUANG YIWEI

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

2010

THE INTERPLAY OF DESIGNS AND DIFFERENCE SETS

HUANG YIWEI

School of Physical and Mathematical Sciences

A dissertation submitted to the Nanyang Technological University in partial fulfillment of the
requirement for the degree of Doctor of Philosophy of Mathematics

2010

Acknowledgements

First of all, I own my deepest gratitude to my supervisor, Associate Professor Bernhard Schmidt, for his continuous support and encouragement throughout the Ph.D. program. He has stimulated my interests in the area of algebraic combinatorics by some amazing problems, to which I, even at the very beginning, could contribute. I am grateful that I have benefitted a lot from his critical thinking and insightful suggestions. He is also an excellent teacher, and without his clever instructions it would have been difficult for me to establish my computational skills, which play a key role in my research. Also many thanks to him for dedicating his precious time to help improve my dissertation structure and also proofread and mark up the errors carefully.

Besides my supervisor, I would like thank Dr. Tan Geok Choo, who has given me very helpful suggestions on my English writing. Thanks also to Dau Son Hoang for providing very nice comments for improving the dissertation. Special thanks go to Cassandra, for her great help on my dissertation issues, and for her everlasting kindness.

It was a pleasure to have smart friends and colleagues to discuss interesting problems with. Let me say "Thank you" to Ding Yang, Tan Yin, Zhang Xiande, and many others. Inspiration usually comes to the mind during the discussion with them. Some of the results in this dissertation were inspired by their suggestions.

During the course of my candidature, I was supported by NTU Research Scholarship. I appreciate very much the various academic events in our division in NTU, and the opportunities to be supported to attend oversea conferences.

Last, but not least, I thank my parents, who showed me the fascination of mathematics during my childhood. I would not have persisted in learning mathematics without their support and encouragement.

Contents

Acknowledgements	2
ABSTRACT	6
Chapter 1. Introduction	9
1.1. Relative Difference Sets and Divisible Designs	10
1.2. Projective Planes	17
1.3. Classical Examples of Relative Difference Sets	23
Chapter 2. Constructions of (p^a, p^b, p^a, p^{a-b}) -Relative Difference Sets	30
2.1. Introduction	30
2.2. A Construction of (p^a, p^b, p^a, p^{a-b}) -Relative Difference Sets	32
2.3. Classification of Groups and RDSs in Extra Special Groups	44
Chapter 3. Dillon-Davis' Construction of Relative Difference Sets and Automorphism Groups	54
3.1. Introduction	54
3.2. Dillon-Davis' Construction	55

3.3. An Example in $AGL(3, q)$	57
3.4. Automorphisms of $(16, 4, 16, 4)$ -Divisible Designs	65
Chapter 4. Uniqueness of Cyclic Projective Planes	74
4.1. Introduction	74
4.2. Preliminary Results	76
4.3. Cyclic Planes of Square Order	77
4.4. Cyclic Planes of Nonsquare Order	97
References	104

ABSTRACT

The Interplay of Designs and Difference Sets

Huang Yiwei

It is well known that a (divisible) design with a regular automorphism group (Singer group) is equivalent to a (relative) difference set in that group. Therefore, the results and tools in designs and difference sets sometimes can be transferred to each other. In this dissertation, we shall discuss three problems to illustrate how the two theories interplay with each other.

The first problem is about the construction of relative difference sets. The fascinating point is that one can see through it how various algebraic tools can be applied to combinatorial problems. There are many results on the construction of relative difference sets, see [7],[10],[29],[30],[35],[37]. Unfortunately, most of the constructions work for abelian groups, but few for non-abelian ones, since algebraic tools in the latter case are limited. By investigating the elements in affine general

linear groups, which are also automorphisms of some classical divisible designs, we obtain a new construction of infinite families of (p^a, p^b, p^a, p^{a-b}) -relative difference sets. This new construction shows that (p^a, p^b, p^a, p^{a-b}) -relative difference sets exist in many non-abelian groups which were not covered by previous constructions.

The second one is concerned with an important construction of infinite families of (p^a, p^b, p^a, p^{a-b}) -relative difference sets by Davis [7]. The developments of these sets are divisible designs. It is not clear whether these designs differ from the classical ones up to isomorphism. An example of relative difference sets is found in the subgroups of affine general linear group $AGL(3, q)$, which shows that these divisible designs are isomorphic to the classical ones in some cases. Furthermore, we study a special case, the automorphisms of $(16, 4, 16, 4)$ -divisible designs, with emphasis on design automorphisms induced by group automorphisms. The automorphisms are classified under some assumptions in the hope that it can be generalized.

Finally, we describe our work on a classical problem, the uniqueness of cyclic projective planes. Interesting results and remarks have been contributed to it by some well-known mathematicians, like R.H. Bruck [5] and M. Hall [18]. By combining tools from the theory of difference sets with a massive computer search, the uniqueness of cyclic projective planes is verified for prime power orders less than 41 and orders 121, 125, 128, 169, 256, 1024.

The study of all these three problems has benefitted from the interplay of the theory of designs and that of difference sets. We also highlight the importance of the of modern computational methods in combinatorial problems, which plays a crucial role in verifying conjectures, searching for examples, and sometimes as a source of inspiration.

CHAPTER 1

Introduction

Combinatorics is a fast growing area of modern mathematics. It is concerned with counting the structures of a given kind and size, deciding when certain criteria can be met simultaneously, with constructing and analyzing objects meeting the criteria, and finding "largest", "smallest", or "optimal" objects. In other words, there are three basic problems of combinatorics. They are the existence problem, the counting problem, and the optimization problem. One can find many applications of combinatorics in both pure mathematics and applied mathematics. Combinatorial problems also arise in various aspects of our lives. Here are some examples. A shop supervisor prepares assignments of workers to tools or to work areas. An electrical engineer considers configurations for a circuit. A university officer arranges class meeting times and students schedules. A statistician considers alternative designs for an experiment.

Design theory is one of the oldest parts of combinatorics; an early example is Kirkman's schoolgirl problem proposed in 1850. It is a study of collections of subsets with certain intersection properties. The notion of difference sets arose in

Singer's work [39] from the study of a particular type of combinatorial designs, the projective planes. Since then, these areas have developed fast into a theory, involving various algebraic methods. Designs and difference sets are closely related, and this connection has been used to solve many open problems. This dissertation contributes further along these lines.

In the first chapter, we shall introduce the notions and some basic results on relative difference sets, divisible designs and projective planes. The relation between relative difference sets and divisible designs will be discussed in Section 1.1. What follows is a short introduction to projective planes and related problems. Finally, a few examples of classical divisible designs will be presented, which inspired some of the main ideas of this dissertation. Most of our work will be briefly mentioned in this chapter, and we also include simple examples to illustrate some tools involved in our research.

1.1. Relative Difference Sets and Divisible Designs

In this section, we shall present the notions of (relative) difference sets and (divisible) designs, which are closely related to each other. Some basic results and examples will be included to illustrate their relation. A well-known theorem at the end reveals that either object can be utilized to construct the other.

We first introduce the notion of (relative) difference sets.

Definition 1. Let G be a finite group of order mn , written multiplicatively. Let N be a normal subgroup in G of order n . A k -subset $R = \{r_1, \dots, r_k\}$ of G is an $(\mathbf{m}, \mathbf{n}, \mathbf{k}, \lambda)$ -**relative difference set** in G relative to N if every element $g \in G \setminus N$ can be expressed in exactly λ ways as a "difference":

$$g = r_i r_j^{-1}, \quad r_i, r_j \in R,$$

and none of the nonidentity element in N has such an expression of difference.

When $n = 1$, we omit n , write v instead of m and speak of a $(\mathbf{v}, \mathbf{k}, \lambda)$ -**difference set**. In the case of a difference set in G , every nonidentity of G can be expressed in λ ways as a difference.

Counting the nonidentity differences in two ways yields the following basic necessary relation for the existence of a relative difference set.

$$k(k-1) = \lambda n(m-1).$$

A (relative) difference set is called **cyclic**, **abelian** or **non-abelian** when the group G is cyclic, abelian or non-abelian, respectively. Refer to the following examples of (relative) difference sets. What comes first is an example of cyclic relative difference set.

Example 2. $R = \{0, 1, 3\}$ is a $(4, 2, 3, 1)$ -relative difference set in $\mathbb{Z}_8$ relative to $N = \{0, 4\}$.

What follows is an example of the relative difference set in abelian group but not cyclic.

Example 3. In $\mathbb{Z}_3 \times \mathbb{Z}_3$, let $R = \{(0, 0), (1, 1), (2, 1)\}$. This is a $(3, 3, 3, 1)$ -relative difference set relative to $N = \{0\} \times \mathbb{Z}_3$.

We now give a non-abelian example.

Example 4. Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group. We have $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, and $ki = j = -ik$. Then $R = \{1, i, j, k\}$ is a $(4, 2, 4, 2)$ -relative difference set in G relative to $N = \{\pm 1\}$.

Here is an example of difference set.

Example 5. $R = \{1, 2, 4\}$ is a $(7, 3, 1)$ -difference set in $\mathbb{Z}_7$.

On one hand, lots of constructions for (relative) difference sets are known. On the other hand, many deep nonexistence theorems have been proven. However, the gap between the constructions and nonexistence theorems remains wide. Much work dealt with the construction of (relative) difference set in abelian groups while not much is known in non-abelian cases. One of the main results in this dissertation

is a construction of new infinite series of (p^a, p^b, p^a, p^{a-b}) -relative difference sets mostly in non-abelian groups. We have obtained the construction by investigating the automorphism groups of some classical divisible designs. The relation between divisible designs and relative difference sets plays a crucial role in the construction.

The following is the definition of divisible designs.

Definition 6. *An (m, n, k, λ) -divisible design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ consists of a set $\mathcal{P}$ of points with size mn , together with a set $\mathcal{B}$ of blocks such that the following conditions are satisfied.*

- *Each block in $\mathcal{B}$ is a subset of $\mathcal{P}$ with size k .*
- *The point set $\mathcal{P}$ can be partitioned into m classes of size n such that any two points from different classes are contained in exactly λ blocks, but two points from the same class not in any common block.*

*In the case $n = 1$, we omit n , write v instead of m and speak of a (v, k, λ) -**design**. In a (v, k, λ) -design, any two points are contained in exactly λ blocks. If a (divisible) design has the same number of points and blocks, we call it **symmetric**.*

Relative difference sets can be used to construct divisible designs. If $R = \{r_1, \dots, r_k\}$ is an (m, n, k, λ) -relative difference set in G relative to N , then for any $g \in G$, we call $Rg = \{r_1g, \dots, r_kg\}$ a **translate** of R . Define a point set $\mathcal{P} = \{g : g \in G\}$, and the block set $\mathcal{B} = \{Rg : g \in G\}$, which consists of all the

translates of R . We show that they form an (m, n, k, λ) -divisible design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$.

Suppose $g_1 \neq g_2$ are two points of $\mathcal{D}$. First we show that the number of blocks containing g_1, g_2 equals the number of pairs (r_i, r_j) with $r_i, r_j \in R$ such that

$$(1.1) \quad g_1 g_2^{-1} = r_i r_j^{-1}.$$

On one hand, if a block Rg contains g_1, g_2 , there are $r_i, r_j \in R$ such that $g_1 = r_i g$, $g_2 = r_j g$. Hence the pair $(r_i, r_j) = (g_1 g^{-1}, g_2 g^{-1})$ satisfies the Equation (1.1). Since for any two distinct blocks containing g_1, g_2 , the solutions $(r_i, r_j) = (g_1 g^{-1}, g_2 g^{-1})$ are different, the number of blocks containing g_1, g_2 is smaller than or equal to the number of solutions (r_i, r_j) for the Equation (1.1). On the other hand, if a pair (r_i, r_j) with $r_i, r_j \in R$ satisfies the equation (1.1), let $g = r_i^{-1} g_1 = r_j^{-1} g_2$, then the block Rg contains g_1, g_2 . This implies that the number of solutions (r_i, r_j) for the equation (1.1) is smaller than or equal to the number of blocks containing g_1, g_2 . Therefore the two numbers are equal.

Now we show that $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is an (m, n, k, λ) -divisible design. If two distinct points g_1, g_2 are in different cosets of N , i.e., $g_1 g_2^{-1} \in G \setminus N$, then there are exactly λ pairs of (r_i, r_j) satisfying condition (1.1) by definition of R . Hence exactly λ blocks contain g_1, g_2 . If $g_1 g_2^{-1} \in N$, then there is no pair (r_i, r_j) with $r_i, r_j \in R$ that satisfies (1.1). Thus no block contains both g_1, g_2 in this case. It is straightforward

to see that the cosets of N are the point classes of the divisible design. This construction is called the **development** of R , denoted by $Dev(R)$. The blocks in $Dev(R)$ can also be partitioned into classes such that two blocks from the same class do not intersect while two from difference classes intersect with λ points.

An **isomorphism** between two divisible designs $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$, $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2)$ is a bijection $\alpha : \mathcal{P}_1 \rightarrow \mathcal{P}_2$ such that $\{\alpha(p) : p \in B\}$ is a block in $\mathcal{B}_2$ for any $B \in \mathcal{B}_1$. Two divisible designs $\mathcal{D}_1, \mathcal{D}_2$ are said to be **isomorphic** if there is a isomorphism between $\mathcal{D}_1$ and $\mathcal{D}_2$. An **automorphism** of a divisible design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is an isomorphism between $\mathcal{D}$ and $\mathcal{D}$ itself. The set of all the automorphisms of a divisible design $\mathcal{D}$ forms a group under function composition, denoted by $Aut(\mathcal{D})$. A subgroup of $Aut(\mathcal{D})$ is called **an automorphism group** of $\mathcal{D}$.

Given an automorphism group G in $Aut(\mathcal{D})$, define the **group action** of G on the point set $\mathcal{P}$ as a binary function $G \times \mathcal{P} \rightarrow \mathcal{P}$ such that $(g, p) \mapsto g(p)$, $g \in G$, $p \in \mathcal{P}$. The group action is called **point regular** if for any two points p_1, p_2 in $\mathcal{P}$, there is exactly one $g \in G$, such that $g(p_1) = p_2$. Sometimes we write p_1^g instead of $g(p_1)$. Similarly, the group action of G on the block set $\mathcal{B}$ is a binary function $G \times \mathcal{B} \rightarrow \mathcal{B}$ such that $(g, B) \mapsto g(B) = \{g(p) : p \in B\}$, $g \in G$, $B \in \mathcal{B}$. The group action is called **block regular** if, given any two blocks $B_1, B_2 \in \mathcal{B}$, there is exactly one $g \in G$, such that $g(B_1) = B_1^g = B_2$. If an automorphism group is both point and block regular, it is said to be a **Singer group** of $\mathcal{D}$.

At last, we include an well-known theorem which describes the relation between (divisible) designs and (relative) difference sets.

Proposition 7. *Let G be a group of size mn , with a normal subgroup N of size n . The development of an (m, n, k, λ) -relative difference set R relative to N in G forms a divisible (m, n, k, λ) -design with the Singer group G and N acts regularly on each point class. Conversely, if a divisible (m, n, k, λ) -design admits G as a Singer group and N acts regularly on each point class of the design, then the divisible design leads to an (m, n, k, λ) -relative difference set in G relative to N .*

Proof. It has been already shown that the development of a relative difference set is a divisible design $\mathcal{D}$. Define the group action G on the point set and block set through the right multiplication using the group operation of G . Then it is easy to show that G is a Singer group of $\mathcal{D}$, and N acts regularly on each point class since the point classes are just the cosets of N . Conversely, given a divisible (m, n, k, λ) -design with a Singer group G , with N acting regularly on each point class, we fix a point p_0 from the point set, and identify each point p with the automorphism σ_p which maps p_0 to p . Then N will correspond to the point class which contains the identity σ_{p_0} . Let $\{b_1, \dots, b_k\}$ be any block of the divisible design. We shall show that $R = \{\sigma_{b_1}, \sigma_{b_2}, \dots, \sigma_{b_k}\}$ is an (m, n, k, λ) -relative difference set relative to

N in G . Since G acts regularly on the block set, the block set is $\{Rg : g \in G\}$. Pick an element h in $G \setminus N$. Then $h, 1$ are two points from different point classes, thus there are exactly λ blocks containing $h, 1$. Suppose $h, 1 \in Rg$, then $h = r_1g$, $1 = r_2g$ for some $r_1, r_2 \in R$. Therefore $h = r_1r_2^{-1}$. Since there are λ such blocks containing $h, 1$, there are exactly λ pairs of (r_1, r_2) with $h = r_1r_2^{-1}$. Hence R is an (m, n, k, λ) -relative difference set in G relative to N . $\square$

1.2. Projective Planes

One of the most beautiful and extensively studied designs are projective planes. A **projective plane** is an $(n^2 + n + 1, n + 1, 1)$ -design with $n \geq 2$. The parameter n is called the **order** of the projective plane. It has $n^2 + n + 1$ points and the same number of blocks. Any two distinct points (blocks) are incident with a unique block (point).

For a prime power order $n = q$, we have the following classical construction of projective plane of order n . Let $\mathbb{F}_q$ be a finite field of order q . Denote the vector space of dimension 3 over $\mathbb{F}_q$ by $\mathbb{F}_q^3$. Let the point set consist of all the one-dimensional subspaces of $\mathbb{F}_q^3$. The blocks are all the two-dimensional subspaces of $\mathbb{F}_q^3$. The incidence is given by set containment. By basic linear algebra, it can be shown that this yields a projective plane of order q , denoted by $PG(2, q)$. A projective plan isomorphic to $PG(2, q)$ is called **desarguesin**.

On the other hand, for an order which is not a prime power, not a single projective plane has been found yet. It is conjectured that a projective plane of order n exists if and only if n is a prime power. This famous conjecture is far from being resolved. The Bruck-Ryser theorem [4] implies that if a projective plane of order $n \equiv 1$ or $2 \pmod{4}$ exists, then n must be the sum of two squares. It eliminates the possibility of the existence of projective planes for some orders, such as 6 and 14. The smallest non-prime-power order which is not ruled out by the Bruck-Ryser theorem is 10. The non-existence of projective planes of order 10 was proved with massive help of computer [26]. The problem is extremely difficult since there are so many possibilities of combinations to check for the existence of a projective plane even for very small orders. The case $n = 12$ is still open. Aside from the Bruck-Ryser theorem and the nonexistence of a projective plane of order 10, not much is known about the existence of projective planes of non-prime-power order. More can be done if we assume additional structures to a projective plane. Because of this, we study the projective planes with some particular Singer groups.

Example 8. *Regard $\mathbb{F}_{q^3}$ as a 3-dimensional vector space over $\mathbb{F}_q$, thus we can define $PG(2, q)$, the classical plane of order q . Let α be the automorphism induced by multiplication with a primitive element of $\mathbb{F}_{q^3}$. Then $G = \langle \alpha \rangle$ is a Singer group of $PG(2, q)$.*

A projective plane is called **cyclic** if it has a cyclic Singer group. The above example shows that $PG(2, q)$ is a cyclic projective plane of order q . According to the last theorem of Section 1.1, the existence of a cyclic projective plane of order n is equivalent to that of an $(n^2 + n + 1, n + 1, 1)$ -difference set in a cyclic group of order $n^2 + n + 1$. This difference set is called a **Singer difference set**. Hence we can study cyclic difference sets instead of cyclic projective planes. This problem is translated into language of difference set so that tools from the theory of difference sets can be applied.

Now we introduce the language of group rings. Identify a subset A of a group G with the element $\sum_{g \in A} g$ of the integral group ring $\mathbb{Z}[G]$. For $\alpha \in \mathbb{Z}$ and the identity element 1 of G , simply write α for the group ring element $\alpha 1$. For $B = \sum_{g \in G} b_g g \in \mathbb{Z}[G]$, write $B^{(k)} = \sum_{g \in G} b_g g^k$, $k \in \mathbb{Z}$. In the language of group ring, an $(n^2 + n + 1, n + 1, 1)$ -difference set can be characterized as follows.

Proposition 9. *Let G be a cyclic group of order $n^2 + n + 1$. An $(n + 1)$ -subset D of G is a cyclic difference set if and only if*

$$DD^{(-1)} = n + G.$$

Let H be a subgroup of G . A **group homomorphism** $\rho : G \rightarrow H$ is a mapping such that $\rho(g_1 g_2) = \rho(g_1) \rho(g_2)$ for any $g_1, g_2 \in G$. Should $G = H$, and ρ

be a bijection from G to G , we call ρ an **automorphism** of G . The set of all the automorphisms of G is denoted by $\text{Aut}(G)$.

We can extend ρ to a homomorphism $\mathbb{Z}[G] \rightarrow \mathbb{Z}[H]$ by linearity. Then by applying the homomorphism to the group ring equation for difference sets, we obtain the following very useful result.

Proposition 10. *Let G be a cyclic group of order $n^2 + n + 1$, and D be an $(n^2 + n + 1, n + 1, 1)$ -difference set in G . Suppose U is a subgroup of G . Let*

$$\rho : G \rightarrow G/U$$

denote the natural epimorphism. Then

$$\rho(D)\rho(D)^{(-1)} = n + |U|(G/U).$$

Many new necessary group ring equations are obtained for the existence of such a difference set from this proposition and this reduces the search for a difference set considerably.

It is easy to see that a translate of a difference set D in G , which is $Dg = \{dg : d \in D\}$, $g \in G$, is also a difference set. Furthermore, if ρ is an automorphism of G , then $\rho(D) = \{\rho(d) : d \in D\}$ is also a difference set in G . Two difference sets

D_1, D_2 is said to be **equivalent** if $\rho(D_1) = D_2g$ for some $\rho \in \text{Aut}(G)$, and some $g \in G$. A group automorphism ρ of G is called a **multiplier** of D when $\rho(D)$ is a translate of D . It is not hard to see that a multiplier of D is an automorphism of $\text{Dev}(D)$. The multiplier theory of difference sets is very useful in the study of difference sets. For a good summary of multiplier theory, see [33]. In some cases, all the multipliers are known immediately from the parameters of difference sets. For example, by Hall [20], we know the following.

Theorem 11. *Let D be a (v, k, λ) -difference set in an abelian group G . Let p be a prime which divides $n = k - \lambda$ and suppose $p > \lambda$. Then p is a multiplier of D .*

Furthermore, we are able to find a translate of D , say Dg with $g \in G$, such that $\rho(Dg) = Dg$. Therefore, the problem is just restricted to exploring the combinations of the orbits under these multipliers. Here is a simple example to illustrate this idea.

Example 12. *Consider the construction of a $(7, 3, 1)$ -difference set in $\mathbb{Z}_7$. Then $\rho : g \rightarrow g^2$ is an automorphism of $\mathbb{Z}_7$. Moreover, by Theorem 11, we know ρ is a multiplier of the difference set D in $\mathbb{Z}_7$. Suppose*

$$\rho(D) = Dg_0.$$

Then the translate $D' = Dg_0^{-1}$ satisfies

$$\rho(D') = D'.$$

So if $a \in D'$, then the orbit of a under ρ satisfies

$$\{a, a^2, a^4\} \in D'.$$

This helps a lot in finding a difference set, since it is sufficient to check the combinations of orbits only. For example, let $a = 1$, then it is easy to see that the orbit $\{1, 2, 4\}$ is already a $(7, 3, 1)$ -difference set in $\mathbb{Z}_7$.

Since $PG(2, q)$ has a cyclic Singer group, there is also a cyclic $(q^2 + q + 1, q + 1, 1)$ -difference set. We call it a **Singer difference set**. It seems that all cyclic difference sets with $\lambda = 1$, called **planar difference sets**, are equivalent to Singer difference sets. If this is true, then finite cyclic projective planes are unique up to isomorphism. The uniqueness of cyclic projective planes or planar cyclic difference sets of prime power order is a long-standing unresolved conjecture. Hall [19] has proved the uniqueness for orders 2, 3, 4, 5, 7, 9, 11, 13, 16, 25, 27, and 32. Bruck [5] verified it for orders 49, 64, and 81. In our view, the known evidence for the uniqueness of cyclic projective planes is quite flimsy. In the hope that some

counter-examples might be found, we extend the verification for larger orders. It is shown that for $n \in \{17, 19, 23, 29, 121, 169, 256, 1024\}$, the cyclic projective planes of order n are unique. Unfortunately, no counter-example occurs.

1.3. Classical Examples of Relative Difference Sets

In this section, we present some classical examples of relative difference sets. They are from the automorphism groups of some divisible designs. The next example is due to Bose [3].

Example 13. *Consider a divisible design constructed as follows. Let the point set $\mathcal{P}$ consist of all non-zero elements in $\mathbb{F}_q^2$, where q is a prime power. The block set $\mathcal{B}$ consists of all the cosets of one-dimensional subspaces of $\mathbb{F}_q^2$ excluding all one-dimensional subspaces. We shall show $(\mathcal{P}, \mathcal{B})$ is a symmetric $(q+1, q-1, q, 1)$ -divisible design. Here, we also treat p_1, p_2 as elements in the finite field $\mathbb{F}_{q^2}$. Two distinct points $p_1, p_2 \in \mathcal{P}$ are contained in a common block*

$$\{kp_1 + (1-k)p_2 : k \in \mathbb{F}_q\}$$

if and only if $p_2^{-1}p_1 \notin \mathbb{F}_q^$, where $\mathbb{F}_q^*$ is the multiplicative group of $\mathbb{F}_q$. Then the cosets of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^2}^*$ are the point classes of the divisible design. Let α , a primitive element of $\mathbb{F}_{q^2}$, also denote the automorphism of the divisible design defined by*

$k^\alpha = \alpha k$, $k \in \mathbb{F}_q$. Now we show that $G = \langle \alpha \rangle$ is a Singer group of the design.

Given a point $p \in \mathcal{P}$, the orbit of p under G is

$$O_p = \{p^g : g \in G\} = \{gp : g \in G\}.$$

It is easy to see that $O_p = \mathcal{P}$ since α is primitive in $\mathbb{F}_{q^2}$. Thus G is point regular.

Similarly, the orbit of a block $B \in \mathcal{B}$ is

$$O_B = \{B^g : g \in G\} = \{\{gp : p \in B\} : g \in G\}.$$

To show $O_B = \mathcal{B}$, we first show the injectivity. In other words, for any two distinct elements $\alpha^{d_1}, \alpha^{d_2} \in G$, we show that $B^{\alpha^{d_1}} \neq B^{\alpha^{d_2}}$. Let

$$B = \mathbb{F}_q + \beta = \{k + \beta : k \in \mathbb{F}_q\}, \quad \beta \notin \mathbb{F}_q.$$

Then

$$B^{\alpha^{d_1}} = \alpha^{d_1} \mathbb{F}_q + \alpha^{d_1} \beta, \quad B^{\alpha^{d_2}} = \alpha^{d_2} \mathbb{F}_q + \alpha^{d_2} \beta.$$

If $B^{\alpha^{d_1}} = B^{\alpha^{d_2}}$, then

$$B^{\alpha^{d_1-d_2}} = \alpha^{d_1-d_2} \mathbb{F}_q + \alpha^{d_1-d_2} \beta = B.$$

So $\alpha^{d_1-d_2} \in \mathbb{F}_q$, and

$$\alpha^{d_1}\beta - \alpha^{d_2}\beta \in \alpha^{d_1}\mathbb{F}_q = \alpha^{d_2}\mathbb{F}_q.$$

This implies that

$$(\alpha^{d_1-d_2} - 1)\beta \in \mathbb{F}_q.$$

However, since $\alpha^{d_1-d_2} - 1 \in \mathbb{F}_q$ and $\beta \notin \mathbb{F}_q$, we have

$$(\alpha^{d_1-d_2} - 1)\beta \notin \mathbb{F}_q$$

unless $\alpha^{d_1-d_2} - 1 = 0$. So $\alpha^{d_1} = \alpha^{d_2}$. The injectivity is shown. Furthermore, the size of G is $q^2 - 1$ which is equal to the size of block set. This implies that $O_B = \mathcal{B}$. Hence G is also block regular. Therefore G is a Singer group of the divisible design $(\mathcal{P}, \mathcal{B})$. By Theorem 7, we establish that in the cyclic group $G = \langle \alpha \rangle$, there is a $(q+1, q-1, q, 1)$ -relative difference set R relative to $N = \langle \alpha^{q+1} \rangle$. Namely, it is

$$R = \left\{ \alpha^d : p^{\alpha^d} \in B \right\},$$

for any fixed $p \in \mathcal{P}$ and $B \in \mathcal{B}$.

The following is an example of a divisible design whose automorphisms can be represented by elements in affine general linear groups.

Example 14. *We construct a divisible design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$. The point set $\mathcal{P}$ consists of the column vectors in $V = \mathbb{F}_q^2$, where q is a prime power. Write*

$$\begin{pmatrix} c \\ 1 \end{pmatrix}^\perp = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in V : ac + b = 0, a, b \in \mathbb{F}_q \right\}, c \in \mathbb{F}_q.$$

Then let the block set $\mathcal{B}$ be

$$\left\{ \begin{pmatrix} c \\ 1 \end{pmatrix}^\perp + w : c \in \mathbb{F}_q, w \in V \right\}.$$

It is not hard to show that $\mathcal{D}$ is a $(q, q, q, 1)$ -divisible design. For this divisible design $\mathcal{D}$, its automorphisms can be represented by elements of affine general linear groups. An element in the affine general linear group $AGL(2, q)$ is a pair (A, T) where A is 2 by 2 invertible matrix over $\mathbb{F}_q$, and T is a column vector of length 2 over $\mathbb{F}_q$. Write

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, T = \begin{pmatrix} t_1 \\ t_2 \end{pmatrix}.$$

Define an element (A, T) in $AGL(2, q)$ to act on the point set by

$$p^{(A, T)} = Ap + T, p \in \mathcal{P}.$$

Since A is invertible, (A, T) induces to a permutation of all points in $\mathcal{P}$. However, for a block $B \in \mathcal{B}$, if we define

$$B^{(A,T)} = \{Ap + T : p \in B\}, \quad B \in \mathcal{B},$$

the set $\{Ap + T : p \in B\}$ is not necessarily a block again. Suppose

$$B = \begin{pmatrix} c \\ 1 \end{pmatrix}^\perp + w, \quad c \in \mathbb{F}_q, w \in V.$$

Then

$$B^{(A,T)} = \left((A^{-1})^T \begin{pmatrix} c \\ 1 \end{pmatrix} \right)^\perp + Aw + T.$$

Let $A = (a_{ij})$, $i, j = 1, 2$. Then it is easy to see that $B^{(A,T)}$ is again a block if and only if $a_{12} = 0$. Therefore, (A, T) induces an automorphism of $\mathcal{D}$ if and only if $a_{12} = 0$. Furthermore, it can be verified that the following group G is a Singer group of this divisible design:

$$G = \left\{ \left(\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \begin{pmatrix} a \\ b \end{pmatrix} \right) : a, b \in \mathbb{F}_q \right\}.$$

By calculating the order of the elements in G , it is concluded that G is elementary abelian if q is odd and that G is isomorphic to a direct product of cyclic groups of order 4 if q is even. Hence $(q, q, q, 1)$ -relative difference sets exist in these two types of abelian groups.

We shall call the divisible designs constructed in the above way the **classical** divisible designs. We will extend this example to a construction of new relative difference sets. Our construction is inspired by considering the same classical divisible designs but represented in a different way, and their automorphisms are represented by elements in a group consisting of 2-tuples. The goal is to find point and block regular subgroups of the full automorphism group of the classical divisible design. A large class of such subgroups is found, most of them are non-abelian. The construction is discussed in detail in Chapter 2.

The problems in this dissertation illustrate the interplay of (divisible) designs and (relative) difference sets. In the study of the cyclic projective planes, we translate the problems from designs into the language of difference sets. Conversely, the construction of new relative difference sets illustrates that the information from divisible designs is also useful in the theory of relative difference sets. In particular, as a by-product, an example of Singer groups found from the classical divisible designs reveals that the developments of relative difference sets constructed by

Davis [7] are isomorphic to the classical divisible designs in some cases. Moreover, some results are obtained on the classification of the multipliers of $(16, 4, 16, 4)$ -relative difference sets constructed by Davis, which are also automorphisms of the corresponding divisible designs, hopefully to be generalized.

The role of computational search is crucial in our study. It helps in finding interesting examples as well as proving theorems. To name a few, in the investigation of the uniqueness of cyclic projective planes, we apply extensive computer search after reducing the search space considerably by some theoretical results. Moreover, the idea of the construction of relative difference sets is inspired by the search for all the regular automorphism groups of a small divisible design.

CHAPTER 2

Constructions of (p^a, p^b, p^a, p^{a-b}) -Relative Difference Sets

2.1. Introduction

In this chapter, we introduce our construction of the (p^a, p^b, p^a, p^{a-b}) -relative difference set (RDS). An (m, n, k, λ) -RDS is called **semiregular** if $k = m\lambda$. Let p stand for a prime, and q for a prime power if not particularly specified.

RDSs are closely connected to many other parts of combinatorics. They are equivalent to divisible designs with certain Singer groups. In particular, some type of projective planes can be constructed by RDSs. Furthermore, RDSs can produce generalized Hadamard matrices and sequences with good autocorrelation properties, see Pott's survey [35].

In Pott's survey, the existence problem of (p^a, p^b, p^a, p^{a-b}) -RDSs is said to be one of the most interesting problems about RDSs. Many constructions and nonexistence results are obtained in abelian cases for these semiregular RDSs, see [29],[30],[37]. Generally speaking, much less is known about RDSs in non-abelian groups than abelian ones. The strategies for the constructions in non-abelian groups are limited. To name a few, we can apply the tools in abelian groups in

some non-abelian cases, but usually it brings strict limitations, see the constructions from Davis [7]. Another strategy is to study a particular group, see the discussion on RDSs in dihedral groups by Schmidt [27] and Garciano, Hiramane, Yokonuma [15]. In order to have more information on possible groups, we can also investigate groups of particular order, see the study on the RDSs in non-abelian groups of order p^4 by Elvira [14]. A unifying construction of (relative) difference sets, called "building set method", was introduced by Davis, Jedweb [10]. However, this construction applies to very few non-abelian cases. To resolve the existence problems of RDSs, besides obtaining bounds, people are eager to find new constructions of RDSs in more non-abelian groups. We shall give a new construction of $(p^k, p^k, p^k, 1)$ -RDSs in some infinite families of both abelian and non-abelian groups. Thus by some projection technic, we obtain (p^a, p^b, p^a, p^{a-b}) -RDSs in many types of groups. Most non-abelian cases from this construction are not covered by previous constructions. The structures of these groups admitting a $(p^k, p^k, p^k, 1)$ -RDS are all explicitly described in terms of generators and relations. A classification is given of some cases for the functions that generates the isomorphic groups in our constructions. In particular, we discuss the problem that whether an extra special group contains an RDS. For an illustration, we list some small cases of groups containing an RDS covered by our constructions.

2.2. A Construction of (p^a, p^b, p^a, p^{a-b}) -Relative Difference Sets

In this section, we present our construction of (p^a, p^b, p^a, p^{a-b}) -RDSs. Firstly, we introduce some preliminary definitions and results.

Definition 15. *A function $f(x)$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ is called **additive** if*

$$f(x + y) = f(x) + f(y).$$

Definition 16. *A polynomial $f(x)$ over $\mathbb{F}_q$ is called a **permutation polynomial** if the associated polynomial function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$.*

Definition 17. *Let p be a prime. A **p -polynomial over $\mathbb{F}_{p^n}$** is defined as*

$$\sum_{i=0}^{n-1} a_i x^{p^i},$$

where $a_i \in \mathbb{F}_{p^n}$.

Indeed, all additive functions over $\mathbb{F}_{p^n}$ can be classified by p -polynomials. It is easy to prove the following result by comparing the number of additive functions over $\mathbb{F}_{p^n}$ and that of p -polynomials.

Lemma 18. *Let p be a prime. A function $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ is additive if and only if it is a p -polynomial over $\mathbb{F}_{p^n}$.*

Note that a p -polynomial $f(x)$ over a finite field also satisfies $f(x - y) = f(x) - f(y)$, because $a = -a$ in $\mathbb{F}_{2^k}$ and the p -polynomial $f(x)$ satisfies $f(-x) = -f(x)$ when $p > 2$.

Either by [28], or simply deducing from the properties of p -polynomials, we have the following proposition.

Lemma 19. *A p -polynomial $f(x)$ over $\mathbb{F}_q$ is a permutation polynomial if and only if $f(x)$ has no non-zero root in $\mathbb{F}_q$.*

By [40], all the additive permutation functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ can be described explicitly.

Proposition 20. *All permutation additive functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ can be written as*

$$f(x) = \sum_{i=0}^{n-1} \left(\alpha_0 + \alpha^{p^i} \alpha_1 + \alpha^{2p^i} \alpha_2 + \cdots + \alpha^{(n-1)p^i} \alpha_{n-1} \right) x^{p^i},$$

where α is a fixed primitive element in $\mathbb{F}_{p^n}$, $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ is any basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. There are exactly $(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$ different additive permutation functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$.

For convenience of proof, we define the classical $(p^k, p^k, p^k, 1)$ -divisible design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ as follows.

Take the point set $\mathcal{P}$ to be

$$\{(v, w) : v, w \in \mathbb{F}_{p^k}\}.$$

The block set $\mathcal{B}$ is

$$\{(v, 1)^\perp + t : v \in \mathbb{F}_{p^k}, t \in \mathcal{P}\},$$

where $(v, 1)^\perp = \{(a, b) : av + b = 0\}$.

Now we introduce a group which will be very useful afterwards. Let the trace function be $Tr : \mathbb{F}_{p^k} \rightarrow \mathbb{F}_{p^l}$, where l divides k . Consider the set

$$K = \{\langle x, c \rangle : x \in \mathbb{F}_{p^k}, c \in \mathbb{F}_{p^l}\}.$$

Let $f(x)$ be an additive function. Define a binary operation on K as

$$\begin{aligned} (2.1) \quad & \langle x_1, c_1 \rangle * \langle x_2, c_2 \rangle \\ &= \langle x_1 + x_2, Tr(sx_1f(x_2)) + c_1 + c_2 \rangle, \end{aligned}$$

where s is a fixed nonzero element in $\mathbb{F}_{p^k}$. We shall show that K is a group of order p^{k+l} under this operation. Firstly, by definition, K is closed under this binary operation. Secondly, the associativity is satisfied since

$$\begin{aligned}
& (\langle x_1, z_1 \rangle * \langle x_2, z_2 \rangle) * \langle x_3, z_3 \rangle \\
&= \langle x_1 + x_2 + x_3, \text{Tr}(s(x_1 + x_2)f(x_3) + sx_1f(x_2)) + z_1 + z_2 + z_3 \rangle \\
&= \langle x_1 + x_2 + x_3, \text{Tr}(sx_1(f(x_2) + f(x_3)) + sx_2f(x_3)) + z_1 + z_2 + z_3 \rangle \\
&= \langle x_1, z_1 \rangle * (\langle x_2, z_2 \rangle * \langle x_3, z_3 \rangle).
\end{aligned}$$

Moreover, the identity $\langle 0, 0 \rangle \in K$, and the inverse of any element $\langle x, z \rangle \in K$ is $\langle -x, \text{Tr}(sxf(x)) - z \rangle$, which is still in K . And clearly, the number of the group elements is p^{k+l} . Hence K is indeed a group of order p^{k+l} under such operation. Note that K is abelian if $f(x)$ is an identity function or zero function. Now we give the main result.

Theorem 21. *Let p be a prime, and k be a positive integer. Let*

$$G = \{ \langle x, c \rangle : x, c \in \mathbb{F}_{p^k} \},$$

The operation in G is defined by

$$\langle x_1, c_1 \rangle * \langle x_2, c_2 \rangle = \langle x_1 + x_2, x_1 f(x_2) + c_1 + c_2 \rangle,$$

where $f(x)$ is an additive permutation function from $\mathbb{F}_{p^k}$ to $\mathbb{F}_{p^k}$. Then G is a group of order p^{2k} and the set $R = \{\langle x, 0 \rangle : x \in \mathbb{F}_{p^k}\}$ is a $(p^k, p^k, p^k, 1)$ -RDS in G relative to $N = \{\langle 0, c \rangle : c \in \mathbb{F}_{p^k}\}$. Moreover, all the developments of these RDSs are isomorphic to the classical $(p^k, p^k, p^k, 1)$ -divisible design.

Proof. Firstly, as we have shown, G is a group of order p^{2k} , since $f(x)$ is additive. Note that the trace function in the operation (2.1) becomes identity function in this case. Secondly, we show that R is an RDS in G relative to N . We consider the difference of two distinct elements of R .

$$\begin{aligned} (2.2) \quad & \langle x, 0 \rangle * \langle y, 0 \rangle^{-1} \\ &= \langle x - y, -(x - y)f(y) \rangle. \end{aligned}$$

Partition the set

$$S = \{(x, y) : x, y \in \mathbb{F}_{p^k}, x \neq y\}$$

into $p^k - 1$ subsets of size p^k , so that

$$S_a = \{(a + d, d) : d \in \mathbb{F}_{p^k}\}, \quad a \in \mathbb{F}_{p^k} \setminus \{0\}.$$

For each element $(x, y) = (a + d, d)$ in S_a , the result in (2.2) is

$$(2.3) \quad \langle a, -af(d) \rangle.$$

Since $a \neq 0$ and $f(x)$ is a permutation function, we have $\mathbb{F}_{p^k} = \{-af(d) : d \in \mathbb{F}_{p^k}\}$.

Furthermore, since a can be any nonzero element in $\mathbb{F}_{p^k}$, all the differences of elements of R cover the elements in $G \setminus N$ exactly one time. Now define the group action of G on the point set and block set of the classical $(p^k, p^k, p^k, 1)$ -divisible design (in the representation defined before) as follows.

$$(a, b)^{\langle x, c \rangle} = (a + f(x), ax + b + c);$$

$$((v, 1)^\perp + (a, b))^{\langle x, c \rangle} = (v - x, 1)^\perp + (a, b)^{\langle x, c \rangle}.$$

we can verify that $(a, b)^{\langle x_1, c_1 \rangle * \langle x_2, c_2 \rangle} = ((a, b)^{\langle x_2, c_2 \rangle})^{\langle x_1, c_1 \rangle}$, thus it is indeed a group action on the point set. Then it is easy to see that it is also a group action on the block set. The group action of an element $\sigma = \langle x, c \rangle \in G$ on the point and block sets induces an automorphism of the divisible design because 1) it induces

a bijection of all points and blocks; 2) if two points p_1, p_2 are in a block b , then $p_1^\sigma, p_2^\sigma \in b^\sigma$, since $b^\sigma = \{p^\sigma : p \in b\}$. The orbits of the point $(0, 0)$ and the block $(0, 1)^\perp$ are respectively

$$(0, 0)^G = \{(f(x), c) : x, y \in \mathbb{F}_{p^k}\};$$

$$((0, 1)^\perp)^G = \{(-x, 1)^\perp + (f(x), c) : x, c \in \mathbb{F}_{p^k}\}.$$

Since $f(x)$ is a permutation function, it is easy to see that $\mathcal{P} = (0, 0)^G$ and $\mathcal{B} = ((0, 1)^\perp)^G$. Hence G is a point and block regular automorphism group, thus a Singer group of the divisible design. Therefore, the development of R forms the classical $(p^k, p^k, p^k, 1)$ -divisible design. $\square$

We shall give the projection technic without proof in order to produce RDSs with new parameters.

Proposition 22. *Let G and G' be two groups, and let N and N' be two normal subgroups of G and G' respectively. Suppose R is an RDS in G relative to N . If there is an epimorphism $\tau : G \rightarrow G'$, and τ_N , the mapping τ restricted on N , is also an epimorphism from N to N' , then $\tau(R) = \{\tau(r) : r \in R\}$ is an RDS in G' relative to N' .*

The Theorem 21 together with the Proposition 22 imply that we can obtain (p^a, p^b, p^a, p^{a-b}) -RDS in both abelian and non-abelian groups if an epimorphism stated as in Proposition 22 exists.

Here are some examples illustrating Proposition 22.

Example 23. Let R be a $(p^k, p^k, p^k, 1)$ -RDS in G relative to N , constructed from Theorem 21. Let $G' = \{\langle x, c \rangle : x \in \mathbb{F}_{p^k}, c \in \mathbb{F}_{p^l}\}$ where l divides k , and $N' = \{\langle 0, c \rangle : c \in \mathbb{F}_{p^l}\}$. The operation in G' is defined by

$$\langle x_1, c_1 \rangle * \langle x_2, c_2 \rangle = \left\langle x_1 + x_2, \text{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^l}}(x_1 f(x_2)) + c_1 + c_2 \right\rangle.$$

Then the projection

$$\tau : \langle x, c \rangle \mapsto \left\langle x, \text{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^l}}(c) \right\rangle$$

is an epimorphism from G to G' , and τ_N is an epimorphism from N to N' . Hence

$$\tau(R) = \{\langle x, 0 \rangle : x \in \mathbb{F}_{p^k}\}$$

is a (p^k, p^l, p^k, p^{k-l}) -RDS in G' relative to N .

Example 24. Let R, G, N be the same in Example 23. Let

$$G' = \{\langle x, c, d \rangle : x \in \mathbb{F}_{p^k}, c \in \mathbb{F}_{p^{m_1}}, d \in \mathbb{F}_{p^{m_2}}\},$$

where m_1, m_2 divide k , and $m_1 + m_2 \leq k$. Treat $\mathbb{F}_{p^k}$ as a vector space of dimension k over $\mathbb{F}_p$, denoted by W . The operation in G' is defined by

$$\begin{aligned} & \langle x_1, c_1, d_1 \rangle * \langle x_2, c_2, d_2 \rangle \\ &= \left\langle x_1 + x_2, \text{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_1}}} (x_1 f(x_2)) + c_1 + c_2, \text{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_2}}} (s x_1 f(x_2)) + d_1 + d_2 \right\rangle, \end{aligned}$$

where s is a nonidentity element in $\mathbb{F}_{q^k}$.

Let

$$N' = \{ \langle 0, c, d \rangle : c \in \mathbb{F}_{p^{m_1}}, d \in \mathbb{F}_{p^{m_2}} \}.$$

Then it is not hard to see that

$$\tau : \langle x, c \rangle \longmapsto \left\langle x, \text{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_1}}} (c), \text{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_2}}} (sc) \right\rangle$$

is an epimorphism from G to G' . In order to make τ_N an epimorphism from N to N' , we need $\tau(N) = N'$. This is equivalent to say that, given any $y \in \mathbb{F}_{p^{m_1}}$, $z \in \mathbb{F}_{p^{m_2}}$, there exists some solution $c \in \mathbb{F}_{p^k}$ satisfying the following equation system

$$\begin{cases} \text{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_1}}} (c) = y, \\ \text{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_2}}} (sc) = z. \end{cases}$$

The set of all the solutions of c in the equation $Tr_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_1}}}(c) = y$ is one of the coset of the $(k - m_1)$ -subspace $V_1 = \left\{x : Tr_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_1}}}(x) = 0\right\}$, and the set of all the solutions of c in the equation $Tr_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_2}}}(sc) = y$ is one of the coset of the $(k - m_2)$ -subspace $V_2 = \left\{x : Tr_{\mathbb{F}_{p^k}/\mathbb{F}_{p^{m_2}}}(sx) = 0\right\}$. Choose s such that $V_1 + V_2 = W$, i.e. V_1 and V_2 span W . Then the intersections of the cosets of V_1 and V_2 have the same size as $V_1 \cap V_2$, which is not empty. and the equation system always has some solution c for any y, z . Hence $\tau(N) = N'$. In this case, the $(p^k, p^{m_1+m_2}, p^k, p^{k-m_1-m_2})$ -RDS is obtained. Note that $m_1 + m_2$ does not necessarily divide k .

Example 25. Let R be a (p^a, p^a, p^a, p^a) -RDS in G relative to N . Let $G = G'$, and N' be a normal p^{a-b} -subgroup of N . Define the epimorphism from G to G'/N' by $\tau : g \longmapsto gN'$, then $\tau(R) = \{\tau(r) : r \in R\}$ is an (p^a, p^b, p^a, p^{a-b}) -RDS in G'/N' . Note that b can be any positive integer smaller than a .

In the construction from Theorem 21, it is free to choose any permutation p -polynomial $f(x)$, and the values k, p are arbitrary too. Now the main question is what types of groups are covered by the construction in Theorem 21, especially for the non-abelian cases. Concerning with the structure of G , we firstly consider the order of the group elements. Let m be a positive integer. We compute

$$\langle x, c \rangle^m = \left\langle mx, \frac{m(m-1)}{2}xf(x) + mc \right\rangle.$$

Hence, when $p = 2$, we have $\langle x, c \rangle^4 = \langle 0, 0 \rangle$ for any x , and for $x \neq 0$, $\langle x, c \rangle^2 = \langle 0, xf(x) \rangle \neq \langle 0, 0 \rangle$. Therefore in this case the exponent of G is 4. When $p \neq 2$, the exponent is always p , since $p \mid \frac{p(p-1)}{2}$.

Secondly, it is straightforward to check that $N = \{ \langle 0, c \rangle : c \in \mathbb{F}_{p^k} \}$ is contained in the center of G . Furthermore, note that $h^{-1}gh = gn$ for some $n \in N$ for all $g, h \in G$.

Now it is ready to describe the group structure explicitly. Let $f(x)$ be an additive permutation polynomial over $\mathbb{F}_{p^k}$. Let $\mathbb{F}_{p^k}^* = \langle \alpha \rangle$. Define

$$L(i, j) = \alpha^i f(\alpha^j) - \alpha^j f(\alpha^i).$$

Let $\text{Coeff}(x)$ stand for a vector of coefficients of a polynomial of α over $\mathbb{F}_p$ by which we represent the element x . More precisely, if $x = a_0 + a_1\alpha + \dots + a_{k-1}\alpha^{k-1}$, then $\text{Coeff}(x) = (a_0, \dots, a_{k-1})$. Write $\mathbf{a} = (a_0, \dots, a_{k-1})$ and $\mathbf{z} = (z_0, \dots, z_{k-1})$. Define

$$\mathbf{z}^{\mathbf{a}} = z_0^{a_0} \dots z_{k-1}^{a_{k-1}}.$$

Case 1 Let p be an odd prime. Define the generators $x_i = \langle \alpha^i, 0 \rangle$, $z_l = \langle 0, \alpha^l \rangle$, $i, l = 0, \dots, k-1$. Then the structure of G in Theorem 21 is

$$(2.4) \quad \langle x_0, \dots, x_{k-1}, z_0, \dots, z_{k-1} | x_i^p = z_l^p = 1, x_i z_l = z_l x_i, z_l z_m = z_m z_l, \\ x_i x_j = x_j x_i \mathbf{z}^{\text{Coeff}(L(i,j))}, i, j, l, m = 0, \dots, k-1 \rangle.$$

Case 2 Let $p = 2$. Let x_i, z_l , $i, l = 1, \dots, k-1$ be the same as in Case 1. Then the structure of G is

$$(2.5) \quad \langle x_0, \dots, x_{k-1}, z_0, \dots, z_{k-1} | x_i^p = \mathbf{z}^{\text{Coeff}(\alpha^i f(\alpha^i))}, z_l^p = 1, \\ x_i z_l = z_l x_i, z_l z_m = z_m z_l, x_i x_j = x_j x_i \mathbf{z}^{\text{Coeff}(L(i,j))}, \\ i, j, l, m = 0, \dots, k-1 \rangle.$$

Write the RDSs in Theorem 21 in form of generators, then

$$R = \left\{ x_0^{e_0} x_1^{e_1} \dots x_{k-1}^{e_{k-1}} \mathbf{z}^{\text{Coeff}\left(-\sum_{i=0}^{k-1} \frac{e_i(e_i-1)}{2} \alpha^i f(\alpha^i)\right)} : 1 \leq e_i \leq p \right\}.$$

Let R be a $(q, q, q, 1)$ -RDS in G relative to N . Let the point set be G , and the block set is $\{Rg : g \in G\} \cup \{Ng : g \in G\}$, then this is an affine plane of order q , which corresponds a Desarguesian projective plane of order q .

Quite often, the groups generated by different functions are isomorphic to each other. Since we are concerned with the question whether the RDSs are equivalent to each other in isomorphic groups, it is natural to ask whether we can identify the isomorphic groups just by analyzing the functions in the constructions. We shall discuss this in the next section.

2.3. Classification of Groups and RDSs in Extra Special Groups

In this section, we discuss more about the groups involved in our constructions of RDSs. One problem is that which functions generate the isomorphic groups in our construction. It is enough discuss the $(p^k, p^k, p^k, 1)$ -RDSs cases, since by projection, we can obtain the groups in other cases.

Firstly, we discuss the case when $k = 2$. Let $\mathbb{F}_{p^2} = \langle \alpha \rangle$. For this case, we can classify all the isomorphic groups generated by different additive permutation functions simply by checking the value of $\alpha f(1) - f(\alpha)$.

If p is an odd prime, by Formula (2.4), the structure of G is

$$\begin{aligned} \langle x_0, x_1, z_0, z_1 | x_i^p = z_j^p = 1, x_i z_j = z_j x_i, z_0 z_1 = z_0 z_1, \\ x_0 x_1 = x_1 x_0 \mathbf{z}^{\text{Coeff}(\alpha f(1) - f(\alpha))}, i, j = 0, 1 \rangle. \end{aligned}$$

If $\alpha f(1) - f(\alpha) = 0$, then G is elementary abelian. If $\alpha f(1) - f(\alpha) \neq 0$, then $\mathbf{z}^{\text{Coeff}(\alpha f(1) - f(\alpha))}$ can be z_0, z_1 or $z_0 z_1$. By substitution if necessary, the structure of G in all three cases can be written as

$$\begin{aligned} \langle x_0, x_1, z_0, z_1 | x_i^p = z_j^p = 1, x_i z_j = z_j x_i, z_0 z_1 = z_0 z_1, \\ x_0 x_1 = x_1 x_0 z_0, i, j = 0, 1 \rangle. \end{aligned}$$

If $p = 2$, by Formula (2.5), the group G is

$$\begin{aligned} \langle x_0, x_1, z_0, z_1 | x_i^2 = \mathbf{z}^{\text{Coeff}(\alpha^i f(\alpha^i))}, z_j^2 = 1, x_i z_j = z_j x_i, \\ z_0 z_1 = z_1 z_0, x_0 x_1 = x_1 x_0 \mathbf{z}^{\text{Coeff}(\alpha f(1) - f(\alpha))}, i, j = 0, 1 \rangle. \end{aligned}$$

If $\alpha f(1) - f(\alpha) = 0$, then G is abelian. Moreover, $\alpha f(\alpha)$ and $f(1)$ are non-zero, since $f(x)$ is a permutation polynomial and $f(0) = 0$. And because $\alpha f(1) = f(\alpha)$,

$f(1) = (a+1)f(\alpha) \neq \alpha f(\alpha)$. So the structure of the abelian group G is

$$\langle x_0, x_1, z_0, z_1 | x_0^2 = z_0, x_1^2 = z_1, z_0^2 = z_1^2 = 1 \rangle,$$

and hence $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_4$. If $\alpha f(1) - f(\alpha) \neq 0$, then G is non-abelian. Since $\alpha f(1) \neq f(\alpha)$, $f(1) \neq f(\alpha)(1+\alpha)$. Furthermore, we have $f(1) \neq f(\alpha)$ and $f(1) \neq f(0)$, therefore the value of $f(1)$ has to be $\alpha f(\alpha)$. Similarly, $\alpha f(1) - f(a)$ is not equal to $\alpha f(1)$, $f(\alpha)$ and 0, so $\alpha f(1) - f(\alpha)$ has to be $f(1)$ or $\alpha f(\alpha)$. Hence in this case the structure of G is

$$\langle x_0, x_1, z_0, z_1 | x_0^2 = x_1^2 = z_0, x_i z_j = z_j x_i, z_0 z_1 = z_1 z_0,$$

$$x_0 x_1 = x_1 x_0 z_0, i, j = 0, 1 \rangle.$$

If $k > 2$, in general there are much more non-isomorphic groups from the constructions. It seems much harder to find a simple criteria to classify all the functions that generate isomorphic groups. Later, we shall give a computational search for all the groups from the constructions for some cases when $k > 2$.

Furthermore, it is interesting if we can determine whether the groups of one type contain an RDS. Our constructions of RDS is helpful for such a question.

A p -group G is called **extra special** if its center Z is cyclic of order p , and the quotient G/Z is a nontrivial elementary abelian p -group. Every extra special p -group has order p^{1+2n} for some positive integer n , see [36].

Definition 26. *Let H and K be two groups. A **central product** of H and K is constructed from two subgroups $H_1 \leq Z(H)$, $K_1 \leq Z(K)$, and a group isomorphism $\sigma : H_1 \rightarrow K_1$. The central product is the quotient of the direct product $H \times K$ by the normal subgroup*

$$N = \{(h, k) : h \in H_1, k \in K_1, \sigma(h)k = 1\}.$$

The extra special p -group can be well classified. A central product of two extra special p -groups is extra special, and by [36], every extra special group can be written as a central product of extra special groups of order p^3 . Since all groups of order p^3 are known, all extra special groups can be described explicitly. There are two types of non-abelian groups of order p^3 , and they can be written as follows (for both $p = 2$ and odd prime p).

$$M_1 = \langle a, b, c \mid a^p = b^p = 1, c^2 = 1, ac = ca, bc = cb, ab = bac \rangle,$$

$$M_2 = \langle a, b, c \mid a^p = b^p = c, c^2 = 1, ac = ca, bc = cb, ab = bac \rangle.$$

Note that the exponent of M_1 is p if p is odd. When $p = 2$, the exponent of M_1 is $p^2 = 4$ since there are some elements having order 4. For instance, the order of ab is 4 in this case.

The following result tells which type of extra special groups of order p^3 containing RDSs from our constructions.

Proposition 27. *There are (p^2, p, p^2, p) -RDSs in the group M_1 if p is an odd prime, and in M_2 if $p = 2$.*

Proof. For odd prime p , by Theorem 21 and Example 23, there are RDSs in the following groups:

$$G = \left\langle x_0, x_1, z \mid x_i^p = z^p = 1, x_i z = z x_i, x_0 x_1 = x_1 x_0 z^{Tr_{\mathbb{F}_{p^2}/\mathbb{F}_p}(f(\alpha) - \alpha f(1))}, i = 0, 1 \right\rangle,$$

where α is a primitive element in $\mathbb{F}_{p^2}$, and $f(x)$ is an additive permutation function over $\mathbb{F}_{p^2}$. Let $f(x) = sx^p$, which is an additive permutation polynomial over $\mathbb{F}_{p^2}$.

Then

$$f(\alpha) - \alpha f(1) = \alpha^p - \alpha \neq 0.$$

Since s is arbitrary in $\mathbb{F}_{p^2}$, there exists s such that $Tr_{\mathbb{F}_{p^2}/\mathbb{F}_p}(f(\alpha) - \alpha f(1)) \neq 0$, and hence in this case $G \cong M_1$. So there are (p^2, p, p^2, p) -RDSs in M_1 when p is an odd prime. For the case $p = 2$, by a quick computational verification of our

construction for all additive permutation functions, there are RDSs only in group M_2 . To get a construction of an RDS in M_2 , we can choose $f(x) = x^2$. $\square$

It is straightforward to get the following.

Proposition 28. *The groups G in Example 23 for $(p^{2n}, p, p^{2n}, p^{2n-1})$ -RDSs are extra special if and only if $Z(G)$, the center of G , is exactly $N = \{\langle 0, c \rangle : c \in \mathbb{F}_p\}$.*

Proof. It is enough to show that the quotient group G/N is elementary abelian. To see this, consider the p th power of the quotient group elements.

$$(\langle x, c \rangle * N)^p = \left\langle px, \text{Tr}_{\mathbb{F}_{p^{2n}}/\mathbb{F}_p} \left(\frac{p(p-1)}{2} x f(x) \right) + pc \right\rangle * N = N.$$

Thus every element in G/N has order p . Furthermore, it is obvious that G/N is abelian, hence G/N is elementary abelian. $\square$

In our construction, it is not easy to determine whether a $(p^{2n}, p, p^{2n}, p^{2n-1})$ -RDS lies in a group whose center is exactly the forbidden subgroup N . Thus it is nontrivial to show the existence of RDSs in extra special groups in general cases. However, in a similar case as that of extra special groups, we are able to show the existence of RDSs. Let q be an odd prime. We consider the group G of order p^{3n} where p is an odd prime, with both $G/Z(G)$ and $Z(G)$ being elementary abelian. Then it can be shown that there is a $(p^{2n}, p^n, p^{2n}, p^n)$ -RDS in such a group.

Proposition 29. *Let p^n be an odd prime power. If the function $f(x) = sx^{p^n}$ where $s^{p^n} = -s$, then the center of the group*

$$G = \{ \langle x, z \rangle : x \in \mathbb{F}_{p^{2n}}, z \in \mathbb{F}_{p^n} \},$$

is

$$N = \{ \langle 0, z \rangle : z \in \mathbb{F}_{p^n} \}.$$

Proof. Firstly we show that $s \in \mathbb{F}_{p^{2n}}$ such that $s^{p^n} = -s$ always exists. Let $\mathbb{F}_{p^{2n}} = \langle \gamma \rangle$. Then $\gamma^{\frac{p^{2n}-1}{2}} = -1$. So $\left(\gamma^{\frac{p^n+1}{2}}\right)^{p^n-1} = -1$. Let $s = \gamma^{\frac{p^n+1}{2}}$, then $s^{p^n} = -s$. Now we show that the center of G is indeed N . On one hand, it is straightforward to verify that the elements in N commute with every element in G . On the other hand, in our construction, two elements $\langle x, z_1 \rangle$ and $\langle y, z_2 \rangle$, commute if and only if

$$(2.6) \quad Tr_{\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n}}(xf(y) - yf(x)) = 0.$$

We shall show that if $x \neq 0$, it is always possible to find y such that Condition (2.6) is not satisfied. Let $\alpha = xf(y) - yf(x)$, then $\alpha^{p^n} = -s(x^{p^n}y - y^{p^n}x) = \alpha$. So $\alpha \in \mathbb{F}_{p^n}$, and $Tr_{\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n}}(\alpha) = \alpha + \alpha^{p^n} = 2\alpha$. Thus if q is odd and $\alpha \neq 0$, then $Tr_{\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n}}(\alpha) \neq 0$. If $x \in \mathbb{F}_{p^n} \setminus \{0\}$, then $\alpha = x(y^{p^n} - y) \neq 0$ for $y \notin \mathbb{F}_{p^n}$.

If $x \in \mathbb{F}_{p^{2n}} \setminus \mathbb{F}_{p^n}$, then $\alpha = y(x - x^{p^n}) \neq 0$ for $y \in \mathbb{F}_{p^n} \setminus \{0\}$. Therefore, for any nonzero $x \in \mathbb{F}_{p^{2n}}$, we can always find y such that Condition (2.6) is not satisfied. In other words, none of the elements $\langle x, z \rangle$ ($x \neq 0$) lies in the center of the group. Hence N is exactly the center of G . $\square$

Now we describe our computational search for some small cases of groups admitting RDSs constructed in Example 23. We need to search over all the permutation additive functions in the construction either by Lemma 19 or by Theorem 20. Here, Lemma 19 is utilized for choosing the functions. By Lemma 18, we just need to pick up the permutation p -polynomials $f(x) \in \mathbb{F}_{q^k}[x]$. Then by Lemma 19, in order to test whether a p -polynomial is a permutation, it is enough to test whether there exists a non-zero root of this polynomial. In MAGMA, groups with relatively small order can be identified. In the following table, we list the groups which contain an RDS by our construction for some small parameters. The 'Order' column lists the order of the group the RDS lies in. The 'Field' column indicates the field $f(x)$ is over. The 'Group Type' column lists the index in MAGMA of the groups the RDSs lie in. We also mark the abelian groups and extra special groups by (abelian) and (e.s.) respectively.

Order	(m, n, k, λ) -RDS	Field	Group Type
8	(4, 2, 4, 2)	$\mathbb{F}_{2^2}$	2(abelian), 4(e.s.), 5(abelian)
27	(9, 3, 9, 3)	$\mathbb{F}_{3^2}$	3(e.s.), 5(abelian)
16	(8, 2, 8, 4)	$\mathbb{F}_{2^3}$	10(abelian), 11, 12, 13
81	(27, 3, 27, 9)	$\mathbb{F}_{3^3}$	12, 15(abelian)
125	(125, 5, 125, 25)	$\mathbb{F}_{5^3}$	12, 15(abelian)
32	(16, 2, 16, 8)	$\mathbb{F}_{2^4}$	45, 46, 47, 48, 49(e.s.), 50(e.s.), 51(abelian)
243	(81, 3, 81, 27)	$\mathbb{F}_{3^4}$	62, 65(e.s.), 67(abelian)
64	(16, 4, 16, 4)	$\mathbb{F}_{4^2}$	192(abelian), 193, 198, 199, 200, 202, 206, 207, 210, 214, 215, 217, 219, 223, 224, 230, 232, 237, 239, 242, 244, 245, 262, 264, 267(abelian)
729	(81, 9, 81, 9)	$\mathbb{F}_{9^2}$	425, 440, 453, 469, 498, 501, 504(abelian)

Remark The search for the case of group order 729 is not complete since the number of the corresponding additive permutation functions are too huge. So we just list the groups found after a reasonable time.

Note that in the groups of order 32, the search shows that two types of extra special groups contain RDSs, while in the group of order 8, 27, 243, only one type of extra special groups contain RDSs from our constructions. The remaining questions are the following:

- (1) Given any prime p , and an integer n , is there at least one type of extra special group of order p^{2n+1} contains an RDS?
- (2) If Question 1 is true, in which situation do both types of extra special groups contain an RDS? And in which situation only one type contains one RDS?

CHAPTER 3

Dillon-Davis' Construction of Relative Difference Sets and Automorphism Groups

3.1. Introduction

The full automorphism group of the classical divisible design can be obtained as a subgroup of an affine general linear group. However, in general it is difficult to find the full automorphism groups of designs. For example, concerning with the automorphisms of a divisible design developed by an RDS, we only know that the elements in G lead to $|G|$ automorphisms of the design. However, the full automorphism group often has much larger order than $|G|$.

In this chapter, we shall discuss the automorphism problems related to a construction of infinite families of RDSs. The main idea of the construction comes from Dillon [12], who applied for difference sets. Davis [7] re-modeled it for RDSs. This is why we call it "Dillon-Davis' construction" in the dissertation. Dillon-Davis' construction of RDSs produces infinite families of RDSs in both abelian and non-abelian groups. The developments of these RDSs are divisible designs with large automorphism groups. We shall demonstrate that the developments of

RDSs from Dillon-Davis' construction are isomorphic to the classical designs in some cases through an example of RDSs in subgroups of $AGL(3, q)$.

The information of automorphisms of divisible designs is useful. For example, our main construction of (p^a, p^b, p^a, p^{a-b}) -RDSs is obtained from the point and block regular automorphism groups of the classical designs. Since it is not known whether Dillon-Davis' construction of RDSs produces isomorphic designs in all cases, we also study the automorphisms of the divisible designs developed from those RDSs. Given an RDS R in a group G , if a group automorphism τ of G satisfies $\tau(R) = Rg$ for some $g \in G$, then τ will also lead to an automorphism of the $Dev(R)$. We have observed some symmetries in Dillon-Davis' construction, and found it promising to obtain a large number of automorphisms of designs by studying the group automorphisms. Some efforts are made in this direction in the case of $(16, 4, 16, 4)$ -RDSs obtained from Dillon-Davis' construction. Our discussion on finding design automorphisms might be a good start for finding automorphisms of (divisible) designs which are not classical.

3.2. Dillon-Davis' Construction

J.A. Davis [7] presented a construction of RDSs in both abelian groups and non-abelian groups. For convenience of the reader, we include the construction.

Let E be a vector space of dimension 2 over $\mathbb{F}_{p^n}$, which can be regarded as an elementary abelian group of order p^{2n} . Let

$$H_1, \dots, H_r, \quad r = \frac{p^{2n} - 1}{p^n - 1} = p^n + 1$$

be the hyperplanes (1-dimensional subspaces) of E . It is easy to see that every non-identity element of E is precisely contained in one of these hyperplanes. Using the group ring notation, we have

$$\sum_{i=1}^r H_i = p^n + E.$$

Let G be a group of order p^{3n} having E as a subgroup. Suppose

$$g_1, \dots, g_{r-1}$$

are in distinct cosets of E . Define the mapping ϕ as

$$\phi : H_i \mapsto g_i H_i g_i^{-1}$$

for $i = 1, \dots, r - 1$. Then define the set R as

$$R = \cup_{i=1}^{r-1} g_i H_i.$$

Proposition 30. *If ϕ is a permutation of all the hyperplanes except H_r , then R is an RDS in G relative to H_r . In particular, when E lies in the center of G , then R is an RDS for any choice of the g_i .*

Proof. We apply the group ring language.

$$\begin{aligned} RR^{(-1)} &= \sum_{i < r} \sum_{j < r} g_i H_i H_j g_j^{-1} = p^n \sum_{i < r} g_i H_i g_i^{-1} + \sum_i \sum_{j \neq i} g_i E g_j^{-1} \\ &= p^n \sum_{i < r} g_i H_i g_i^{-1} + p^n (G - E). \end{aligned}$$

Since ϕ is a permutation of hyperplanes except H_r , we have

$$\begin{aligned} RR^{(-1)} &= p^n (p^n + E - H_r) + p^n (G - E) \\ &= p^{2n} + p^n (G - H_r). \end{aligned}$$

Hence R is a $(p^{2n}, p^n, p^{2n}, p^n)$ -RDS in G relative to H_r . In particular, when E is in the center of G , the map ϕ is the identity map, thus also a permutation of the hyperplanes different from H_r . $\square$

3.3. An Example in $AGL(3, q)$

The following lemma is well known. It shows how to produce RDSs with new parameters from the given ones.

Lemma 31. *Let R be an (m, n, k, λ) -RDS in G relative to N . If U is a normal subgroup of order u of G which is contained in N , then there exists an $(m, n/u, k, \lambda u)$ -RDS in G/U relative to N/U . In particular, G/N contains an $(m, k, \lambda n)$ -difference set.*

Proof. We have

$$RR^{(-1)} = n + \lambda(G \setminus N).$$

Apply the map

$$\sigma : g \longmapsto gU$$

to the group ring equation, then

$$\sigma(R)\sigma(R^{(-1)}) = nU + \lambda u((G/U) \setminus (N/U)).$$

Since R is an RDS relative to N , we have

$$r_1U = r_2U,$$

when $r_1 \neq r_2$. Otherwise, $r_1r_2^{-1} \in U \subset N$, a contradiction. Therefore,

$$\sigma(R) = \{rU : r \in R\}$$

is an $(m, n/u, k, \lambda u)$ -RDS in G/U relative to N/U . $\square$

Recall that by the Example 14 in Section 1.3, the $(q, q, q, 1)$ -RDSs exist for all prime power q . Then according to Lemma 31, we derive the existence of (p^a, p^b, p^a, p^{a-b}) -RDSs for any $a, b \in \mathbb{Z}$ such that $a > b$ in some abelian groups.

Now consider a larger design, the classical (q^2, q, q^2, q) -divisible design. It can be constructed as follows. Take the point set as

$$\{(v_1, v_2, v_3) : v_1, v_2, v_3 \in \mathbb{F}_q\},$$

and the block set as

$$\{(v_1, v_2, 1)^\perp + t : v_1, v_2 \in \mathbb{F}_q, t \in V(3, q)\},$$

where $V(3, q)$ stands for the 3-dimensional vector space over $\mathbb{F}_q$, and $(v_1, v_2, 1)^\perp$ is the orthogonal space of the vector $(v_1, v_2, 1)$ in $V(3, q)$. Incidence is given by set-theoretic containment. Denote this design by $\mathcal{D}$.

Now we consider the automorphisms of $\mathcal{D}$. Denote an element in the affine general linear group $AGL(3, q)$ by $\langle A, T \rangle$ where $A = (a_{ij})$ is a 3 by 3 matrix over $\mathbb{F}_q$, T is a 3 by 1 matrix over $\mathbb{F}_q$. The operation in $AGL(3, q)$ is defined by

$$\langle A_1, T_1 \rangle * \langle A_2, T_2 \rangle = \langle A_2 A_1, A_2 T_1 + T_2 \rangle.$$

As in Example 14, we can deduce that an element in $AGL(3, q)$ leads to an automorphism of $\mathcal{D}$ if and only if

$$a_{13} = a_{23} = 0.$$

Consider the elements in $AGL(3, q)$ of the following form:

$$\alpha_{a,b,c} = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & a & 1 \end{pmatrix}, \begin{pmatrix} a \\ b \\ c \end{pmatrix} \right\rangle, a, b, c \in \mathbb{F}_q.$$

Then it is easy to verify that

$$G = \{\alpha_{a,b,c} : a, b, c \in \mathbb{F}_q\}$$

is an abelian group of order q^3 which acts regularly on the point set and block set of $\mathcal{D}$. Thus G is a Singer group. Take the block $(0, 0, 1)^\perp$ and the point $(0, 0, 0)$, then the set R of the group elements that map $(0, 0, 0)$ to the points in $(0, 0, 1)^\perp$ is

$$R = \{\alpha_{a,b,0} : a, b \in \mathbb{F}_q\}.$$

Hence R is a (q^2, q, q^2, q) -RDS relative to the normal subgroup

$$N = \{\alpha_{0,0,c} : c \in \mathbb{F}_q\},$$

which is elementary abelian.

We now discuss the structure of G . Suppose $q = p^k$. When $p = 2, 3$, $G \cong \mathbb{Z}_p^k \times \mathbb{Z}_{p^2}^k$; when $p > 3$, G is elementary abelian. To determine the group structure, first consider the order of the group elements. Let k be a positive integer. We compute

$$\begin{aligned} \alpha_{a,b,c}^k &= \langle A, T \rangle^k = \langle A^k, (A^{k-1} + A^{k-2} + \cdots + I)T \rangle \\ &= \left\langle \begin{pmatrix} 1 & 0 & 0 \\ ka & 1 & 0 \\ kb + \frac{k(k-1)}{2}a^2 & ka & 1 \end{pmatrix}, \begin{pmatrix} ka \\ \frac{k(k-1)}{2}a^2 + kb \\ k(k-1)ab + \sum_{m=1}^{k-1} \frac{m(m-1)}{2}a^2 + kc \end{pmatrix} \right\rangle. \end{aligned}$$

When $q = 2^k$, the order of $\alpha_{a,b,c}$ is 4 if and only if $a \neq 0$, thus in this case the exponent of G is 4. Suppose $G = \mathbb{Z}_4^{m_1} \times \mathbb{Z}_2^{m_2}$, where $2m_1 + m_2 = k$. Counting the number of elements of order 4, we obtain the equality

$$(2^k - 1)2^{2k} = (2^{m_1} - 1)2^{m_2+m_1}.$$

Since the even factors of both sides of the equation must be equal, we also have

$2k = m_1 + m_2$. Hence $m_1 = m_2 = k$. A similar proof works for the case $q = 3^k$. For

any prime $p > 3$, we always have $\alpha_{a,b,c}^p = 1$, since $p \mid \sum_{m=1}^{p-1} \frac{m(m-1)}{2}$, when $p > 3$.

Let $q = p^n$. By Lemma 31, we establish that $(p^{2n}, p^{n-d}, p^{2n}, p^{n+d})$ -RDSs exist in some abelian groups.

One reason to extend the Example 14 is to find RDSs with new parameters or in some new groups, especially for non-abelian groups. Unfortunately, this example just produces RDSs with same parameters, and in abelian groups. Furthermore, we find that these RDSs also can be constructed by Dillon-Davis' construction.

Let

$$G = \{\alpha_{a,b,c} : a, b, c \in \mathbb{F}_q\}.$$

Then

$$E = \{\alpha_{0,a,b} : a, b \in \mathbb{F}_q\}$$

is an elementary abelian group in G . The hyperplanes in E are

$$H_0 = \{\alpha_{0,0,c} : c \in \mathbb{F}_q\},$$

$$H_a = \{\alpha_{0,-b,ba} : b \in \mathbb{F}_q\}, \quad a \in \mathbb{F}_q.$$

The following q elements are from distinct cosets of E in G .

$$g_a = \alpha_{-a,0,0}, \quad a \in \mathbb{F}_q.$$

Then by the Dillon-Davis' construction of RDSs, we deduce that $R = \cup_{a \in \mathbb{F}_q} H_a g_a$ is an RDS in G relative to H_0 , which is the following set:

$$R = \{\alpha_{-a,b,0} : a, b \in \mathbb{F}_q\} = \{\alpha_{a,b,0} : a, b \in \mathbb{F}_q\}.$$

Therefore we obtain the following result:

Theorem 32. *Let $q = p^k$. In $G \cong \mathbb{Z}_p^k \times \mathbb{Z}_{p^2}^k$ ($p = 2, 3$) or $G \cong \mathbb{Z}_p^{3k}$ ($p > 3$), among the RDSs obtained from Dillon-Davis' construction, there are at least q^3 RDSs whose developments are isomorphic to the classical (q^2, q, q^2, q) -divisible design.*

Proof. The above example shows that at least one RDS from Dillon-Davis' construction, $R = \cup_{a \in \mathbb{F}_q} H_a g_a$ in G produces the classical (q^2, q, q^2, q) -divisible design with Singer group G . Moreover, the translates $Rg = \cup_{a \in \mathbb{F}_q} H_a g_a g$ satisfy that the elements in

$$\{g_a g : a \in \mathbb{F}_q\}$$

are still in distinct cosets of E for any $g \in G$. Thus all the translates Rg ($g \in G$) are also from Dillon-Davis' construction. Therefore at least $|G| = q^3$ RDSs from Dillon-Davis' construction have their developments isomorphic to the classical (q^2, q, q^2, q) -divisible design. $\square$

In Dillon-Davis' construction of RDSs, the choice of g_i is only required to be from different cosets of E , and the number of choices is larger than $|G|$. All the RDSs from Dillon-Davis' construction can be partitioned into several translate equivalence classes, and the RDSs in one equivalence class have isomorphic developments. But it is not clear whether there are some group automorphisms of G that map from one translate equivalence class to another.

Note that for $p = 2, 3$, the above example does not include the elementary abelian groups. Hence we also examine the following case.

Let $G = \mathbb{Z}_2^6, E \cong \mathbb{Z}_2^4$. Suppose $G = \langle g_1, g_2, \dots, g_6 \rangle$, and $E = \langle g_1, \dots, g_4 \rangle$. Let $H_i (i = 0, 1, \dots, 4)$ be all the hyperplanes of E , which are listed as follows:

$$H_0 = \langle g_1, g_2 \rangle, H_1 = \langle g_3, g_4 \rangle, H_2 = \langle g_1g_3, g_2g_4 \rangle,$$

$$H_3 = \langle g_1g_4, g_2g_3g_4 \rangle, H_4 = \langle g_1g_3g_4, g_2g_3 \rangle.$$

Let the RDS be

$$R = H_1 \cup H_2g_5 \cup H_3g_6 \cup H_4g_5g_6.$$

The computation of all the automorphisms of $Dev(R)$ shows that the order of the automorphism group of $Dev(R)$ is the same as that of the classical $(16, 4, 16, 4)$ -divisible design.

We have tried all the possible different choices of coset representatives for the RDSs from Dillon-Davis' construction for some small cases, and find that the order of automorphism groups of their developments does not change. It seems that the developments of RDSs from Dillon-Davis' construction are all isomorphic to the classical divisible designs. If this is true, then immediately all the automorphisms of the development of these RDSs are obtained, since all automorphisms of the classical designs are known. However, as far as the isomorphism problem is not resolved completely, it is still interesting to discuss the automorphisms of the development of the RDSs from Dillon-Davis' construction directly. In the next section, we shall discuss the automorphisms for a special case.

3.4. Automorphisms of $(16, 4, 16, 4)$ -Divisible Designs

Let us consider Dillon-Davis' construction for the $(16, 4, 16, 4)$ -RDSs. Let

$$G = \mathbb{Z}_2^6, \quad E \cong \mathbb{Z}_2^4,$$

and E be a subgroup of G . Suppose H_0, H_1, H_2, H_3, H_4 are subgroups of E such that

$$H_0, H_1, H_2, H_3, H_4 \cong \mathbb{Z}_2^2,$$

and each two of them intersect trivially. If $G = \cup_{i=1}^4 E g_i$, then

$$R = \cup_{i=1}^4 H_i g_i$$

is a $(16, 4, 16, 4)$ -RDS in G relative to H_0 .

As mentioned before, there is a simple criterion to check when a group automorphism $\sigma \in \text{Aut}(G)$ leads to a design automorphism of $\text{Dev}(R)$:

Lemma 33. *Let $\sigma \in \text{Aut}(G)$, and let R be an RDS in G . Then $\sigma \in \text{Aut}(\text{Dev}(R))$ if and only if $\sigma(R) = Rg$ for some $g \in G$.*

Proof. If $\sigma(R) = Rg$, then the bijection of points σ also leads to a bijection of blocks. Conversely, if σ leads to a bijection of blocks, $\sigma(R)$ will be some other block, i.e., $\sigma(R) = Rg$ from some $g \in G$. $\square$

Now we divide the group automorphisms into two cases for study: the automorphisms fixing E , and those not fixing E .

3.4.1. Automorphisms Fixing E

First, consider the automorphisms fixing E .

Lemma 34. *Let E be a group. Let H_1, H_2 be two subgroups of E . If $H_1 g_1 = H_2 g_2$, then $H_1 = H_2$ and $g_1 g_2^{-1} \in H_1$.*

Proof. Since $H_1g_1 = H_2g_2$, we have $g_2g_1^{-1} \in H_1$, so $g_1g_2^{-1} = (g_2g_1^{-1})^{-1} \in H_1$, hence $H_1g_1g_2^{-1} = H_1 = H_2$. $\square$

Lemma 35. *If $\sigma(R) = Rg$ for some $g \in G$, and $\sigma(E) = E$, then $\sigma(H_0) = H_0$, and $\sigma(H_i) = H_{\rho(i)}$, $\sigma(g_i)g^{-1}g_{\rho(i)}^{-1} \in \sigma(H_i)$, $i = 1, 2, 3, 4$, where $\rho \in \text{Sym}(\{1, 2, 3, 4\})$.*

Proof. We have $\sigma(R) = \cup_{i=1}^4 \sigma(H_i)\sigma(g_i) = Rg = \cup_{i=1}^4 H_i g_i g$. Since $\sigma(E) = E$, then $\sigma(H_i) \subset E$. Moreover, since $G = Gg = \cup_{i=1}^4 E g_i g$, the four elements in the following set are in the four cosets of E in G respectively.

$$\{H_i g_i g : i = 1, 2, 3, 4\}.$$

Similarly, the elements in

$$\{\sigma(H_i)\sigma(g_i) : i = 1, 2, 3, 4\}$$

are also in the cosets of E respectively.

Then $\cup_{i=1}^4 \sigma(H_i)\sigma(g_i) = \cup_{i=1}^4 H_i g_i g$ implies

$$\sigma(H_i)\sigma(g_i) = H_{\rho(i)}g_{\rho(i)}g$$

for some $\rho \in \text{Sym}(\{1, 2, 3, 4\})$. According to Lemma 34, we have $\sigma(H_i) = H_{\rho(i)}$, and $\sigma(g_i)g^{-1}g_{\rho(i)}^{-1} \in \sigma(H_i)$, for $i = 1, 2, 3, 4$. Then the image of H_0 must be H_0 itself since there is no other choice. Therefore $\sigma(H_0) = H_0$. $\square$

For convenience, in order to study the group automorphisms fixing E , we represent the subgroups H_i ($i = 0, \dots, 4$) as follows.

$$\begin{aligned} H_0 &= \{1, a_0, a_1, a_2\}; \\ H_1 &= \{1, b_0, b_1, b_2\}; \\ H_2 &= \{1, a_0b_0, a_1b_1, a_2b_2\}; \\ H_3 &= \{1, a_0b_1, a_1b_2, a_2b_0\}; \\ H_4 &= \{1, a_0b_2, a_1b_0, a_2b_1\}. \end{aligned}$$

Here, $a_i^2 = b_j^2 = 1$ for any i, j , and $a_0a_1 = a_2, b_0b_1 = b_2$.

We use an array of 2-tuples representing the subscripts of the corresponding non-identity elements in H_2, H_3, H_4 above.

$$\begin{pmatrix} (0, 0) & (1, 1) & (2, 2) \\ (0, 1) & (1, 2) & (2, 0) \\ (0, 2) & (1, 0) & (2, 1) \end{pmatrix}$$

We first study the case that σ is the stabilizer of one H_i ($i = 1, 2, 3, 4$). W.L.O.G., assume $\sigma(H_1) = H_1$. Then an automorphism $\sigma \in \text{Aut}(G)$ induces permutations of $\{a_0, a_1, a_2\}$ and $\{b_0, b_1, b_2\}$. Denote $\sigma_{(\tau, \gamma)}(a_i b_j) = a_{\tau(i)} b_{\gamma(j)}$, $\sigma_{(\tau, \gamma)}(a_i) = a_{\tau(i)}$, and $\sigma_{(\tau, \gamma)}(b_j) = b_{\gamma(j)}$, where $\tau, \gamma \in \text{Sym}(\{0, 1, 2\})$. By Lemma 35, we know that σ leads to a permutation of H_i ($i = 1, 2, 3, 4$). Then we have the following lemma:

Lemma 36. *Let $\sigma \in \text{Aut}(G)$, such that $\sigma(H_0) = H_0$, $\sigma(H_1) = H_1$. Then if $\sigma \in \text{Aut}(\text{Dev}(R))$, we have that σ lies in one of the following three types. The types are classified by the image of H_2 , each type covers 6 automorphisms.*

- 1) $\sigma_{(\tau, \tau\gamma_0)} \Rightarrow H_i \mapsto H_i, i = 0, 1, 2, 3, 4;$
 - 2) $\sigma_{(\tau, \tau\gamma_1)} \Rightarrow H_2 \mapsto H_3, H_3 \mapsto H_4, H_4 \mapsto H_2, H_j \mapsto H_j, j = 0, 1;$
 - 3) $\sigma_{(\tau, \tau\gamma_2)} \Rightarrow H_2 \mapsto H_4, H_3 \mapsto H_2, H_4 \mapsto H_3, H_j \mapsto H_j, j = 0, 1;$
- where τ is arbitrary in $\text{Sym}(\{0, 1, 2\})$, and $\gamma_j(i) = i + j \pmod{3}$.

Proof. It is straightforward to verify that every listed automorphism leads to a permutation of H_i , fixing H_0 and H_1 . On the other hand, when the image of H_2 is determined, it is not hard to show that there are at most 6 automorphisms possible. Therefore, all the automorphisms permuting H_i and fixing H_0, H_1 are covered by the three types. $\square$

According to the Lemma 36, there are 6 choices for each of the three types since τ is arbitrary. To determine the total number of the automorphisms, we need to determine the possible images of g_i for each type.

Assume $g_1 = 1$, $g_2g_3 = g_4$. Then in Type 1) from Lemma 36, we have

$$H_1 = H_1g; \quad H_2\sigma(g_2) = H_2g_2g,$$

$$H_3\sigma(g_3) = H_3g_3g, \quad H_4\sigma(g_4) = H_4g_4g.$$

for some $g \in G$.

On one hand, $\sigma(g_2)\sigma(g_3) = g_2gh_2g_3gh_3 = g_4h_2h_3$ for some $h_2 \in H_2$, $h_3 \in H_3$. On the other hand, $\sigma(g_2)\sigma(g_3) = \sigma(g_2g_3) = \sigma(g_4) \in g_4gH_4$. Hence we have $h_2h_3 \in H_4$. There are exactly 4 pairs of (h_2, h_3) such that $h_2h_3 \in H_4$. Moreover, since $g \in H_1$, there are 4 choices for g too. Therefore there are $4 \times 4 = 16$ choices for the images of σ on g_i .

It is similar for Type 2) and 3), and there are also 16 choices for the images of g_i . Hence there are $6 \times 3 \times 16$ group automorphisms leading to design automorphisms in the case of stabilizers of H_1 . The situation is the same for the stabilizers of H_2, H_3 or H_4 by symmetry. To show it, we just need to modify the representations of H_i for each case. The intersection of stabilizers of H_i and H_j ($i \neq j$) are the

automorphisms of Type 1) in Lemma 36, and the size is 6×16 . So we find in total $9 \times 6 \times 16 = 864$ automorphisms of the $Dev(R)$ from group automorphisms.

In the case that $\sigma(E) = E$, it is not necessary to assume that the group automorphisms fix one U_i ($i = 1, 2, 3, 4$). There are cases where the automorphisms do not fix any H_i . Indeed, we can first choose arbitrarily the images of U_1 and U_2 and determine the automorphisms afterwards. There are 6×16 automorphisms when the images of U_1, U_2 are chosen.

Theorem 37. *The number of automorphisms of $Dev(R)$ induced by elements of $Aut(G)$ which fix E is $6 \times 16 \times 4 \times 3 = 1152$.*

Proof. We have dealt with stabilizer cases above. Other cases are verified by hand. □

Remark 38. *It is better if the counting is unified for every case, not only for the stabilizer cases. We hope to find a unified counting method with the purpose of generalization.*

3.4.2. Automorphisms Not Fixing E

Now let us consider the automorphisms not fixing E .

Lemma 39. *Let G be a group, and H_1, H_2 are subgroups of G with $|H_1| = |H_2|$.*

Let $K = H_1 \cap H_2$. Then $|H_1g_1 \cap H_2g_2|$ is 0 or $|K|$ for any $g_1, g_2 \in G$.

Proof. Let $g = g_1g_2^{-1}$. Then $|H_1g_1 \cap H_2g_2| = |H_1g \cap H_2|$. Take any $\alpha, \beta \in H_1$ from the same coset of K , thus $\alpha\beta^{-1} \in K \subset H_2$. Then either $\alpha g, \beta g \in H_2$, or $\alpha g, \beta g \notin H_2$. Otherwise suppose W.L.O.G. $\alpha g \in H_2$, $\beta g \notin H_2$. Then $\alpha g(\beta g)^{-1} = \alpha\beta^{-1} \notin H_2$, a contradiction. Hence

$$|H_1g \cap H_2| = m|K|,$$

where m is the number of cosets of K in H_1 that are contained in H_2g^{-1} . Furthermore, suppose $\alpha_1, \dots, \alpha_n \in H_1g \cap H_2$. Let $\alpha_i = h_i g$ ($i = 1, \dots, n$) where $h_i \in H_1$. Then

$$\alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, \dots, \alpha_n\alpha_1^{-1}$$

are

$$1, h_2h_1^{-1}, \dots, h_nh_1^{-1}.$$

These are n distinct elements in $H_1 \cap H_2 = K$, so $n \leq |K|$. Hence $|H_1g \cap H_2| = 0$ or $|K|$. $\square$

Lemma 40. *Suppose $\sigma(E) \cap E = H_0$, $\sigma(R) = Rg$ and $\cup_{i=1}^4 Eg_i = G$. Let $g_1 = 1$, and $g_2g_3 = g_4$. Then we have $|\sigma(H_i) \cap H_jg_jg| = 1$ for any $i, j \in \{1, 2, 3, 4\}$.*

Proof. Since $\sigma(E) \cap E = U_0$, we have $\sigma(H_i) \cap H_j = \{1\}$ for any $i, j \in \{1, 2, 3, 4\}$. So according to Lemma 39, $|\sigma(H_i) \sigma(g_i) \cap H_j g_j g| = 0$ or 1 for any $i, j \in \{1, 2, 3, 4\}$. On the other hand, $|\sigma(H_i) \sigma(g_i)| = \sum_{j=1}^4 |\sigma(H_i) \sigma(g_i) \cap H_j g_j g| = 4$, hence $|\sigma(H_i) \sigma(g_i) \cap H_j g_j g| = 1$ for any $i, j \in \{1, 2, 3, 4\}$. $\square$

To find automorphisms σ , such that $\sigma(R) = Rg$ and $\sigma(E) \neq E$, we need to determine the images of the generators of the group G . Lemma 40 is helpful to reduce the possibilities of the choices for the images, and thus makes it easier to find such automorphisms. The following is an example of an automorphism σ such that $\sigma(E) \neq E$, which is found by hand.

Example 41. *Suppose the generators of G are $a_0, a_1, b_0, b_1, g_1, g_2$. Then the automorphism*

$$\begin{aligned} \sigma : \quad a_0 &\mapsto a_2, a_1 \mapsto a_0 \\ b_0 &\mapsto g_2, b_1 \mapsto g_1, \\ g_1 &\mapsto b_0, g_2 \mapsto b_2 \end{aligned}$$

satisfies $\sigma(R) = R$.

It seems much more difficult to find such group automorphisms that do not fix E compared with the case of fixing E . Even with Lemma 40, there are many possibilities to check. However, we believe there are a lot more automorphisms in this case.

CHAPTER 4

Uniqueness of Cyclic Projective Planes

4.1. Introduction

A $(v, k, 1)$ -difference set is called a **planar** difference set. Singer [39] stated that “it seems to be true” that any two cyclic planar difference sets of the same order are equivalent. The *prime power conjecture* asserts that the order of any finite projective plane must be a prime power. Combining Singer’s conjecture with the prime power conjecture gives the following.

Conjecture 42. *Every finite cyclic projective plane is desarguesian.*

Conjecture 42 is sometimes attributed to Singer, though, as a matter of fact, Singer did not conjecture that the order of a cyclic projective plane must be a prime power. Anyway, Conjecture 42 is equivalent to the combination of the following statements.

- (i) Every cyclic finite projective plane has prime power order.
- (ii) The cyclic projective planes of prime power order are all isomorphic.

Statement (i) has been verified by Baumert and Gordon [1, 16] for all orders up to $2 \cdot 10^9$. It also has been verified for several infinite classes of orders [2]. On the other hand, the results on (ii) do not go further than order 81 and date back to the work of Hall [19] and Bruck [5]. Assertion (ii) was proved by Hall [19] for orders 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 25, 27, and 32 with the help of a computer.

In our view, the known evidence for Conjecture 42 is quite flimsy. It seems that Bruck [5] was actually searching for counter examples. However, he was not successful, but verified Conjecture 42 for orders 49, 64, and 81. The following statement of Bruck [5] inspired our work.

“It appears to the author that the present results could be extended considerably ... to find what might be called ‘counter examples’.”

Two cases are studied separately: the case of the square order and the prime order, since they require different strategies. More results can be applied in the square order case to reduce the search space, thus we can deal with the situation of much larger order. For the prime order case, should any counter example appear, it would contradict the conjecture that every projective plane of prime order is desarguesian.

We shall show that the first part of Bruck's statement is correct – unfortunately, we have no success with the second part. We will verify (ii) for orders less than 41 and orders 121, 125, 128, 169, 256, 1024.

We will show that this, in particular, implies the uniqueness of a nontrivial difference set in the cyclic group of order 1,049,601, up to equivalence. To our knowledge, this is by far the largest group which contains a difference set, and for which all difference sets in the group have been classified.

4.2. Preliminary Results

We need some preliminary results before the discussion of the two cases.

By Theorem 11, we obtain the following.

Proposition 43. *Let n be a power of a prime p . Every cyclic planar difference set of order n is equivalent to a planar difference set D with $D^{(p)} = D$.*

This proposition tells that we just need examine the combinations of p -orbits for the search of difference sets, for both square orders and nonsquare orders. If any counter example for Conjecture 42 exists, then it necessarily corresponds to a cyclic planar difference set which is not equivalent to a Singer difference set of a desarguesian projective plane. On the other hand, in general, the inequivalence of two difference sets does not imply that the corresponding designs are non-isomorphic.

However, as the following special case of [[25], Theorem 2.1] shows, this implication does hold if one of difference sets in question is a Singer difference set of a desarguesian plane.

Proposition 44. *Let q be a prime power, and let D be a cyclic planar difference set of order q which is not equivalent to a Singer difference set. Then the projective plane generated by D is non-desarguesian.*

4.3. Cyclic Planes of Square Order

4.3.1. The Results of Bruck

The following Propositions 45-49 are contained in [5]. For the convenience of the reader, we include proofs, since our notation differs from [5].

Throughout this section, we use the following notation. Let q be a prime power, and let G be a cyclic group of order $q^4 + q^2 + 1$. We write $m = q^3$, $s = q^2 - q + 1$, and $t = q^2 + q + 1$.

Proposition 45. *Let D be a planar difference set of order q^2 in G , and assume $D^{(m)} = D$. Let U be the subgroup of G of order t . Then $D \cap U$ is a planar difference set in U .*

Proof. For $g \in G$ we write $Dg = \{dg : d \in D\}$. Let $\mathcal{L} := \{Dg : g \in G, (Dg)^{(m)} = Dg\}$. Note that $U = \{g \in G : g^m = g\}$ and $\mathcal{L} = \{Du : u \in U\}$. For $u \in U$, we

write $\mathcal{L}_u = \{L \in \mathcal{L} : u \in L\}$. Let $w \in U$ and $M \in \mathcal{L} \setminus \mathcal{L}_w$ be arbitrary. It is straightforward to verify that the map $\mathcal{L}_w \rightarrow M \cap U$ sending $L \in \mathcal{L}_w$ to the unique point in $L \cap M$ is a well defined bijection. Using this fact repeatedly, we see that there is a positive integer x such that $|\mathcal{L}_u| = x$ for all $u \in U$ and $|L \cap U| = x$ for all $L \in \mathcal{L}$. Now fix some $u \in U$. Since the lines in $\mathcal{L}_u$ cover each point in $U \setminus \{u\}$ exactly once, we get $q^2 + q = x(x - 1)$ and thus $x = q + 1$. Since $D \in \mathcal{L}$ by assumption, we infer $|D \cap U| = q + 1$. Hence $D \cap U$ is a planar difference set in U . $\square$

Proposition 46. *Write $G = \langle \sigma \rangle \langle \tau \rangle$ where σ has order s and τ has order t .*

Let D be a planar difference set in G satisfying $D^{(m)} = D$. Then there is a function

$$f_D : \{1, \dots, s - 1\} \rightarrow \{0, \dots, t - 1\}$$

such that

$$(4.1) \quad D = \overline{D} + \sum_{x=1}^{s-1} \sigma^x \tau^{f_D(x)}$$

where $\overline{D} = D \cap \langle \tau \rangle$.

Proof. Recall that $\overline{D}$ is a planar difference set in $\langle \tau \rangle$ by Proposition 45. Since $\overline{D} D^{(-1)}$ covers all elements of $\langle \tau \rangle$, the elements of $D \setminus \overline{D}$ must all belong to different

cosets $\neq \langle \tau \rangle$ of $\langle \tau \rangle$ in G . Since there are exactly $s-1$ such cosets and $|D \setminus \overline{D}| = s-1$, the elements of $D \setminus \overline{D}$ represent each coset $\neq \langle \tau \rangle$ of $\langle \tau \rangle$ in G exactly once. This implies the assertion. $\square$

Throughout the rest of Section 4.3, we use the notation introduced in Proposition 46. For a positive integer r and an integer y , we write

$$[y]_r = \min\{z \in \mathbb{N} : z \equiv y \pmod{r}\}.$$

Proposition 47. *Assume $D^{(k)} = D$ for some integer k with $(k, st) = 1$. Then*

$$f_D([kx]_s) \equiv kf_D(x) \pmod{t}$$

for all $x \in \mathbb{Z}$, $x \neq 0$. In particular, if $D^{(p)} = D$, then $f_D([-x]_s) \equiv f_D(x) \pmod{t}$

for all $x \neq 0$.

Proof. By (4.1) we have

$$\bar{D}^{(k)} + \sum_{x=1}^{s-1} \sigma^{kx} \tau^{kf_D(x)} = \bar{D} + \sum_{x=1}^{s-1} \sigma^x \tau^{f_D(x)} = \bar{D} + \sum_{x=1}^{s-1} \sigma^{kx} \tau^{f_D([kx]_s)}.$$

This implies

$$\sum_{x=1}^{s-1} \sigma^{kx} \tau^{kf_D(x)} = \sum_{x=1}^{s-1} \sigma^{kx} \tau^{f_D([kx]_s)}$$

and thus $f_D([kx]_s) \equiv kf_D(x) \pmod{t}$ for all $x \neq 0$. Recall $m = q^3$. If $D^{(p)} = D$, then $D^{(m)} = D$, and thus $f_D([-x]_s) \equiv f_D([mx]_s) \equiv mf_D(x) \equiv f_D(x) \pmod{t}$. $\square$

Proposition 48. *Define $E \subset \{0, \dots, t-1\}$ by $D \cap \langle \tau \rangle = \sum_{d \in E} \tau^d$. The set D given by (4.1) is a planar difference set if and only if for each $x = 1, \dots, s-1$, the following t numbers are pairwise distinct modulo t :*

$$(4.2) \quad \begin{aligned} & f_D(x) - d, \quad d \in E, \quad d - f_D(x), \quad d \in E, \\ & f_D([x+y]_s) - f_D(y), \quad y = 1, \dots, s-1, \quad y \not\equiv -x \pmod{s}, \end{aligned}$$

Proof.

$$\begin{aligned} DD^{(-1)} &= \bar{D} \bar{D}^{(-1)} + \bar{D} \sum_{x=1}^{s-1} \sigma^{-x} \tau^{-f_D(x)} + \bar{D}^{(-1)} \sum_{x=1}^{s-1} \sigma^x \tau^{f_D(x)} + \sum_{x,y=1}^{s-1} \sigma^{x-y} \tau^{f_D(x)-f_D(y)} \\ &= q + \langle \tau \rangle + \sum_{x=1}^{s-1} \sum_{d \in E} \sigma^{-x} \tau^{d-f_D(x)} + \sum_{x=1}^{s-1} \sum_{d \in E} \sigma^x \tau^{f_D(x)-d} \\ &\quad + s-1 + \sum_{x=1}^{s-1} \sigma^x \sum_{\substack{y=1 \\ y \not\equiv -x \pmod{s}}}^{s-1} \tau^{f_D([x+y]_s)-f_D(y)} \\ &= q^2 + \langle \tau \rangle + \sum_{x=1}^{s-1} \sigma^x \left(\sum_{d \in E} \tau^{d-f_D(x)} + \sum_{d \in E} \tau^{f_D(x)-d} + \sum_{\substack{y=1 \\ y \not\equiv -x \pmod{s}}}^{s-1} \tau^{f_D([x+y]_s)-f_D(y)} \right) \end{aligned}$$

Condition (4.2) holds if and only if the term in the parenthesis equals $\langle \tau \rangle$ for all $x \neq 0$. This implies the assertion. $\square$

Proposition 49. *For $S \subset \langle \tau \rangle$, define*

$$K(S) := \{k \in \{0, \dots, t-1\} : \tau^{2k} \neq d_1 d_2 \text{ for all } d_1, d_2 \in S\}.$$

Recall $\bar{D} = D \cap \langle \tau \rangle$. The range of f_D is $K(\bar{D})$. Furthermore, $|K(\bar{D})| = (s-1)/2$, and f_D is a two-to-one map.

Proof. Let $x \in \{1, \dots, s-1\}$ be arbitrary. Then

$$\tau^{f_D(x)} d_1^{-1} \neq d_2 \tau^{-f_D(x)} \text{ for all } d_1, d_2 \in \bar{D}$$

by Proposition 48. Hence the range of f_D is a subset of $K(\bar{D})$. Let $x, y \in \{1, \dots, s-1\}$ with $x \not\equiv \pm y \pmod{s}$ be arbitrary. Define $a, b \in \{0, \dots, s-1\}$ by $x \equiv a+b \pmod{s}$ and $y \equiv a-b \pmod{s}$. Then $a, b \not\equiv 0 \pmod{s}$ and $a \not\equiv \pm b \pmod{s}$. Note that $f_D([-b]_s) \equiv f_D(b) \pmod{t}$ by Proposition 47. Hence

$$f_D([a+b]_s) - f_D(b) \not\equiv f_D([a-b]_s) - f_D(b) \pmod{t}$$

by Proposition 48. Since $[a + b]_s = x$ and $[a - b]_s = y$, this implies $f_D(x) \neq f_D(y) \pmod{t}$. Since $f_D(x) \equiv f_D([-x]_s) \pmod{t}$, this shows that f_D is a two-to-one mapping. Hence the range of f_D has exactly $(s - 1)/2$ elements. It remains to show $|K(\bar{D})| = (s - 1)/2$. Assume that $d_1 d_2 = d_3 d_4$ with $d_i \in \bar{D}$ for $i = 1, 2, 3, 4$. Then $d_1 d_3^{-1} = d_4 d_2^{-1}$. Since $\bar{D}$ is a planar difference set, this implies $d_1 = d_4$ and $d_3 = d_2$ or $d_1 = d_3$ and $d_4 = d_2$, i.e., $\{d_1, d_2\} = \{d_3, d_4\}$. Hence $|K(\bar{D})|$ is the t minus the number of unordered pairs of elements from $\bar{D}$, i.e., $t - (q + 1)(q + 2)/2 = (s - 1)/2$. $\square$

4.3.2. Cyclic Planes of Orders 121, 169, 256, and 1024

In this section, we prove some general auxiliary results on cyclic projective planes of square order, and describe the implementation of complete searches for cyclic projective planes of orders 121, 169, 256, and 1024. Our searches are based on the results of Section 4.3.1 and the following result of Hall [18].

Proposition 50. *Every cyclic projective plane of order at most 16 and of order 32 is desarguesian.*

Throughout this section, we use the notation introduced in Section 4.3.1. We write $q = p^a$ where p is a prime. Recall that $G = \langle \sigma \rangle \langle \tau \rangle$ denotes a cyclic group of

order $q^4 + q^2 + 1$, and σ , respectively τ , is an element of G of order $s = q^2 - q + 1$, respectively $t = q^2 + q + 1$.

Lemma 51. *Let $q = p^a$ where p is a prime and $q \leq 16$ or $q = 32$. Let D_q be an arbitrary planar difference set of order q in $\langle \tau \rangle$ satisfying $D_q^{(p)} = D_q$. Any cyclic planar difference set of order q^2 is equivalent to a difference set D satisfying*

$$(4.3) \quad D^{(p)} = D \text{ and } D \cap \langle \tau \rangle = D_q.$$

Proof. Let F be a cyclic planar difference set of order q^2 . Proposition 43 shows that F is equivalent to a difference set F_1 with $F_1^{(p)} = F_1$. Proposition 44, Proposition 45, and Proposition 50 imply that $F_1 \cap \langle \tau \rangle$ and D_q are equivalent difference sets. Hence there are $g \in \langle \tau \rangle$ and an integer r with $(r, t) = 1$ such that $(F_1 \cap \langle \tau \rangle)^{(r)}g = D_q$. Since $F_1^{(p)} = F_1$ and $D_q^{(p)} = D_q$, we have $g = 1$. Hence $D = F_1^{(r)}$ satisfies (4.3). $\square$

From now on, let D be a cyclic planar difference set of order q^2 in G satisfying (4.3), let f_D be the corresponding function defined in Proposition 46, and let $K(\bar{D})$ be defined as in Proposition 49.

Let r be any positive integer. We define an r -cycle as an orbit of multiplication with $p \bmod r$ on $\{0, \dots, r-1\}$, i.e., a subset of $\{0, \dots, r-1\}$ of the form $\{[xp^i]_r : i \in \mathbb{N}\}$ for some $x \in \{0, \dots, r-1\}$.

Since D satisfies (4.3), we infer that $K(\bar{D})$ is a union of t -cycles. A t -cycle contained in $K(\bar{D})$ is called a $K(\bar{D})$ -cycle.

Lemma 52. *Let O be any s -cycle. Then $f_D(O)$ is a $K(\bar{D})$ -cycle, and*

$$O \rightarrow f_D(O), x \mapsto f_D(x)$$

is a two-to-one map. Furthermore, the map F_D from the set of s -cycles $\neq \{0\}$ to the set of $K(\bar{D})$ -cycles induced by f_D is a bijection.

Proof. Since $D^{(p)} = D$, Proposition 47 shows that $f_D(O)$ is a $K(\bar{D})$ -cycle for every s -cycle O . By Proposition 49, the map F_D is surjective. Let $x, y \in \{0, \dots, s-1\}$ with $f_D(x) = f_D(y)$. By the proof of Proposition 49, this implies $x \equiv -y \pmod{s}$. Since $q^3 \equiv -1 \pmod{s}$, the elements x and y are contained in the same s -cycle. This shows that F_D is injective. Since f_D is a two-to-one map by Proposition 49, we infer that $O \rightarrow f_D(O), x \mapsto f_D(x)$ is also a two-to-one map for each s -cycle O . □

Lemma 53. *If $q \equiv 2 \pmod{3}$, then there is an s -cycle O containing exactly two elements, and we have $f_D(x) = 0$ for $x \in O$.*

Proof. Since $q \equiv 2 \pmod{3}$, we have $s \equiv 0 \pmod{3}$, and $O = \{s/3, 2s/3\}$ is an s -cycle. Since $O \rightarrow f_D(O), x \mapsto f_D(x)$ is a two-to-one map, $f_D(O)$ is a $K(\bar{D})$ -cycle containing only one element. Hence $f_D(x) = 0$ for $x \in O$. $\square$

Let $\mathbb{Z}_s^*$ denote the multiplicative group of integers mod s . Note that $\mathbb{Z}_s^*$ acts by multiplication mod s on the set $\{1, \dots, s-1\}$, and this induces an action of $\mathbb{Z}_s^*$ on the set of s -cycles.

Lemma 54. *Let $M = M_1 \cup \dots \cup M_c$ be the set of s -cycles, where $M_1, \dots, M_c$ are the orbits of the $\mathbb{Z}_s^*$ action on M . For $i = 1, \dots, c$, let $O_i \in M_i$ and $x_i \in O_i$ be arbitrary. Let O be any $K(\bar{D})$ -cycle, and let $y \in O$ be arbitrary.*

Let E be an arbitrary cyclic planar difference set of order q^2 . Then there is $j \in \{1, \dots, c\}$ with $|O_j| = 2|O|$ such that E is equivalent to a difference set D satisfying (4.3) and $f_D(x_j) = y$.

Proof. Let D be any cyclic planar difference set of order q^2 satisfying (4.3). It suffices to show that there are $j \in \{1, \dots, c\}$ and positive integer r coprime to st with $f_{D(r)}(x_j) = y$. Since O is contained in $K(\bar{D})$, and $K(\bar{D})$ is the range of f_D , there is $x \in \{1, \dots, s-1\}$ with $f_D(x) = y$. Let $s(x)$ denote the s -cycle containing x .

Then $s(x) \rightarrow O, z \mapsto f(z)$ is a two-to-one map by Lemma 52. Hence $|s(x)| = 2|O|$.

Furthermore, by the definition of the x_i , there are $j \in \{1, \dots, c\}$ and an integer r with $(r, s) = 1$, $r \equiv 1 \pmod{t}$, and $rx \equiv x_j \pmod{s}$. Note $|O_j| = |s(x)| = 2|O|$.

Moreover,

$$D^{(r)} = D_q + \sum_{z=1}^{s-1} \sigma^{rz} \tau^{f_D(z)} = D_q + \sum_{z=1}^{s-1} \sigma^z \tau^{f_D([r_1 z]_s)}$$

where r_1 is an integer with $rr_1 \equiv 1 \pmod{s}$. This implies $f_{D^{(r)}}(x_j) = f_D([r_1 x_j]_s) = f_D(x) = y$. $\square$

Proposition 55. *Assume that s is a prime, and let D_q be an arbitrary planar difference set of order q in $\langle \tau \rangle$ with $D_q^{(p)} = D_q$. Let $y \in K(D_q)$ be arbitrary. Then every cyclic planar difference set of order q^2 is equivalent to a difference set D satisfying (4.3) and $f_D(1) = y$. Furthermore, any two distinct difference sets D satisfying (4.3) and $f_D(1) = y$ are inequivalent.*

Proof. Note that we have $c = 1$ in Lemma 54 since s is a prime. Thus, choosing $x_j = 1$ in Lemma 54 shows that every cyclic planar difference set of order q^2 is equivalent to a difference set D satisfying (4.3) and $f_D(1) = y$. Now let D and D' be any two distinct difference sets satisfying (4.3) and $f_D(1) = f_{D'}(1) = y$. Assume that D and D' are equivalent. Then there are $g \in G$ and $r \in \mathbb{Z}$ with $(r, st) = 1$

and

$$(4.4) \quad D' = gD^{(r)}.$$

Since $\langle \tau \rangle$ is the only coset of $\langle \tau \rangle$ which contains more than one element of D , respectively D' , this implies $g \in \langle \tau \rangle$. Hence (4.4) implies $D_q = gD_q^{(r)}$. By a result of [17], we have $r \equiv p^j \pmod{t}$ for some $j \in \mathbb{N}$. Since $D_q^{(p)} = D_q$, we get $D_q = gD_q$ and thus $g = 1$. Hence $D' = D^{(r)}$. Let $r_1 \in \{1, \dots, s-1\}$ with $rr_1 \equiv 1 \pmod{s}$. By (4.1) and since $D' = D^{(r)}$, we have $f_{D'}(1) \equiv rf_D(r_1) \equiv p^j f_D(r_1) \pmod{t}$. In view of Proposition 47 and $f_D(1) = f_{D'}(1) = y$, this implies $f_D([p^j r_1]_s) = f_D(1)$. From Propositions 47 and 49, we conclude $\pm p^j r_1 \equiv 1 \pmod{s}$ and thus $r \equiv \pm p^j \pmod{s}$. Recall $r \equiv p^j \pmod{t}$, $q^3 \equiv -1 \pmod{s}$, and $q^3 \equiv 1 \pmod{t}$. We infer $r \equiv p^e \pmod{st}$ for some positive integer e . But this implies $D' = D$, a contradiction. $\square$

Proposition 55 is very useful since it shows that, in the case where D_q is unique up to equivalence and s is a prime, the number of nonisomorphic cyclic projective planes of order q^2 coincides with the number of functions f satisfying Proposition 48 with $D \cap \langle \tau \rangle = D_q$, Proposition 47 for $k = p^j$, $j \in \mathbb{N}$, and $f_D(1) = y$. Thus, in this case, all cyclic projective planes of order q^2 are desarguesian if and only if a function f_D satisfying these conditions is unique.

The following gives a similar result for the case where $s/3$ is a prime.

Proposition 56. *Assume that $s = 3r$ where $r > 3$ is a prime, and let D_q be an arbitrary planar difference set of order q in $\langle \tau \rangle$ with $D_q^{(p)} = D_q$. Let $A \subset \{1, \dots, s-1\}$ with $|A| = r-1$ such that*

$$A \cup \{[(r+1)a]_s : a \in A\} = \{x \in \{1, \dots, s-1\} : (x, s) = 1\} = T.$$

Let $y \in K(D_q)$ be arbitrary nonzero.

Every cyclic planar difference set of order q^2 is equivalent to a difference set D satisfying (4.3) and one of the following conditions.

- (i) $f_D(1) = y$,
- (ii) $f_D(3) = y$ and $f_D(a) = \min\{f_D(x) : x \in T\}$ for some $a \in A$.

Furthermore, any two distinct difference sets D satisfying (4.3) and one of the conditions (i) or (ii) are inequivalent.

Proof. Note that $c = 3$. We have that M_1 contains s -cycles consisting of numbers coprime to s , M_2 contains s -cycles consisting of numbers divisible by 3, and M_3 only contains s -cycle $O = \{r, 2r\}$. By Lemma 53, $f_D(x) = 0$ for all $x \in O$. Hence the preimage of y of f_D is either in s -cycles from M_1 or M_2 . By Lemma 54, every cyclic planar difference set of order q^2 is equivalent to a difference set D satisfying

(4.3) and $f_D(1) = y$ if the preimage of y is in M_1 or $f_D(3) = y$ if the preimage of y is in M_2 . Furthermore, the complement of A in T is $\overline{A} = \{[-x]_s : x \in A\}$, and $f_D(x) = f_D([x]_s)$, hence

$$\{f_D(x) : x \in A\} = \{f_D(x) : x \in \overline{A}\} = \{f_D(x) : x \in T\}.$$

Therefore $f_D(a) = \min\{f_D(x) : x \in T\}$ for some $a \in A$. The proof that any two distinct difference sets D satisfying (4.3) and Condition (i) is exactly the same as the proof of Theorem 55 so omitted. For the cases that two distinct difference sets D, D' satisfying (4.3) and Condition (ii), assume

$$D' = gD^{(r')}.$$

Similarly as in Theorem 55, we obtain that $D' = D^{(r')}$, and $r' \equiv \pm p^j \pmod{r}$. Besides, $r' \equiv p^j \pmod{t}$, and $r' \equiv \pm p^j \pmod{3}$. Hence we infer $r' \equiv p^e \pmod{3rt}$ for some positive integer e . This implies $D' = D$, a contradiction. $\square$

Before describing our algorithm, we introduce some notation. By D_q we denote an arbitrary planar difference set of order q in $\langle \tau \rangle$ with $D_q^{(p)} = D_q$, and define $E \subset \{0, \dots, t-1\}$ by $D_q \cap \langle \tau \rangle = \sum_{d \in E} \tau^d$. We consider the following modification of the condition in Proposition 48.

Let M be a subset of $\{1, \dots, s-1\}$, and let $f : \{1, \dots, s-1\} \rightarrow \{0, \dots, t-1\}$ be a function. For $x \in \{1, \dots, s-1\}$ we define a multiset M_x by

$$M_x = \begin{cases} \bigcup_{d \in E} \{[f(x) - d]_t, [d - f(x)]_t\}, & \text{if } x \in M, \\ \emptyset, & \text{if } x \notin M. \end{cases}$$

We say that the *condition $C(M)$ is satisfied for f* if, for every $x = 1, \dots, s-1$, the multiset

$$M_x \cup \{[f(x+y) - f(y)]_s : y \in M, x+y \in M\}$$

does not contain any element with multiplicity ≥ 2 .

For $y \in K(D_q)$, let $K(y)$ denote the $K(D_q)$ -cycle containing y . For $a \in \{1, \dots, s-1\}$, let $s(a)$ denote the s -cycle containing a .

The correctness of the following algorithm follows from the results of Section 4.3.1 and Lemma 53.

Algorithm 57.

Input: $q = p^a$ where p is a prime, a planar difference set D_q of order q in $\langle \tau \rangle$ with $D_q^{(p)} = D_q$, an s -cycle S with $|S| > 2$, and a k -cycle K with $|K| = |S|/2$

Output: A set $\mathcal{S}$ such that every cyclic planar difference set D of order q^2 with $D \cap \langle \tau \rangle = D_q$ and $f_D(S) = K$ is equivalent to an element of $\mathcal{S}$

Initialization:

1. $\mathcal{S} := \emptyset; M := \emptyset$.
2. Let $\{S_1, \dots, S_b\}$ be the set of all s -cycles, and choose the numbering such that $S_1 = S$ and $S_b = \min\{|S_i| : i = 1, \dots, b\}$. For $i = 1, \dots, b$, choose $s_i \in S_i$ arbitrarily.
3. If $q \not\equiv 2 \pmod{3}$, set $c := b$. If $q \equiv 2 \pmod{3}$, set $c := b - 1$, $f(x) := 0$ for $x \in S_b$ and $M := M \cup S_b$.
4. Choose $y \in K$ arbitrarily, set $f([p^i s_1]_s) := [p^i y]_t$, $i = 0, \dots, |S| - 1$, and $M := M \cup S$.
5. Set $R := K(D_q) \setminus (K \cup \{0\})$, and $L := 2$.

Main Step:

- (i) If $L = c + 1$, then add $D_q \cup \bigcup_{i=1}^{s-1} \sigma^x \tau^{f(x)}$ to $\mathcal{S}$, set $L := L - 1$,
 $R := R \cup K(f(s_L))$, $M := M \setminus S_L$.
- (ii) Repeat until $L = 1$ or $f(s_L) < \max(R)$:
Set $f(s_L) := -1$, $L := L - 1$, $R := R \cup K(f(s_L))$, $M := M \setminus S_L$.
- (iii) If $L = 1$, then terminate and output $\mathcal{S}$.
- (iv) Set $y := \min\{r \in R : r > f(s_L)\}$ and $f([p^i s_L]_s) := [p^i y]_t$ for $i = 0, \dots, |S_L| - 1$.

- (v) Set $M' := M \cup S_L$. If $C(M')$ holds for f , then set $M := M'$, $R := R \setminus K(y)$,
 $L := L + 1$.
- (vi) Go to step (i).

We now describe the application of Algorithm 57 to the cases $q = 11, 13, 16$, and 32. The difference set $D_q \subset \langle \tau \rangle$ will be specified by giving the set $E \subset \{0, \dots, t-1\}$ with $D_q = \sum_{d \in E} \tau^d$. The functions $f : \{1, \dots, s-1\} \rightarrow K(D_q)$ computed by Algorithm 57 are given in the form $f(1) \cdots f(s-1)$ (values separated by spaces).

- (1) $q = 11$. We choose $E = \{1, 11, 16, 40, 41, 43, 52, 60, 74, 78, 121, 128\}$. Since $s = 3 \cdot 37$, we can apply Proposition 56. We take $y = 4$ and choose A such that $4 \in A$ and thus $41 = [4(1 + s/3)]_s \notin A$. The application of Algorithm 57 shows that there is no cyclic planar difference set D of order 11^2 satisfying (4.3) and $f_D(1) = y$. Moreover, there is a unique D satisfying (4.3), $f_D(3) = 4$, and $f_D(4) = \min\{f_D(x) : x \in \{1, \dots, s-1\}, (x, s) = 1\}$. According to Proposition 56, this shows that there is exactly one cyclic planar difference set of order 11^2 , up to equivalence. The following are the values of the unique function f_D for which (4.3) holds, and which satisfies $f_D(3) = 4$, and $f_D(4) = \min\{f_D(x) : x \in \{1, \dots, s-1\}, (x, s) = 1\}$.

13 17 4 5 71 105 32 25 30 110 10 64 115 77 29 12 88 120 83 62 39 54 9
 123 36 119 129 100 7 85 99 68 44 86 37 89 0 35 51 73 15 23 49 55 91 132
 112 48 122 79 70 8 130 53 116 116 53 130 8 70 79 122 48 112 132 91 55 49
 23 15 73 51 35 0 89 37 86 44 68 99 85 7 100 129 119 36 123 9 54 39 62 83
 120 88 12 29 77 115 64 10 110 30 25 32 105 71 5 4 17 13

(2) $q = 13$. Let $E = \{0, 2, 3, 10, 26, 39, 43, 61, 109, 121, 130, 136, 141, 155\}$.

Since $s = 157$ is a prime, we can apply Proposition 55. We take $y = 8$. The application of Algorithm 57 shows that there is exactly one cyclic planar difference set D of order 13^2 satisfying (4.3) and $f_D(1) = y$. According to Proposition 55, this shows that there is exactly one cyclic planar difference set of order 13^2 , up to equivalence. The following are the values of the unique function f_D for which (4.3) holds, and which satisfies $f_D(1) = 8$.

8 84 15 83 19 35 25 53 38 11 57 71 104 9 134 87 96 55 42 46 20 154
 137 105 117 177 143 172 48 102 58 129 149 60 63 156 29 95 12 128 77 107
 27 67 171 36 120 119 17 40 33 164 140 49 30 139 160 103 145 100 173 86
 75 150 64 142 180 22 168 24 144 59 16 88 110 45 166 89 89 166 45 110 88
 16 59 144 24 168 22 180 142 64 150 75 86 173 100 145 103 160 139 30 49
 140 164 33 40 17 119 120 36 171 67 27 107 77 128 12 95 29 156 63 60 149
 129 58 102 48 172 143 177 117 105 137 154 20 46 42 55 96 87 134 9 104
 71 57 11 38 53 25 35 19 83 15 84 8

(3) $q = 16$. Let

$$E = \{39, 78, 156, 91, 182, 17, 34, 68, 136, 272, 271, 269, 265, 257, 241, 209, 145\}.$$

Since $s = 241$ is a prime, we can apply Proposition 55. We take $y = 3$. The application of Algorithm 57 shows that there is exactly one cyclic planar difference set D of order 16^2 satisfying (4.3) and $f_D(1) = y$. According to Proposition 55, this shows that there is exactly one cyclic planar difference set of order 16^2 , up to equivalence. The following are the values of the unique function f_D for which (4.3) holds, and which satisfies $f_D(1) = 3$.

3 6 50 12 198 100 185 24 238 123 20 200 157 97 222 48 187 203 188
 246 163 40 167 127 63 41 42 194 98 171 262 96 55 101 71 133 116 103 22
 219 231 53 158 80 242 61 245 254 197 126 29 82 161 84 109 115 244 196
 186 69 149 251 5 192 47 110 147 202 86 142 176 266 212 232 183 206 105
 44 114 165 57 189 228 106 88 43 210 160 139 211 93 122 191 217 151 235
 259 121 79 252 11 58 172 164 131 49 21 168 220 218 94 230 111 215 10
 119 229 99 25 138 138 25 99 229 119 10 215 111 230 94 218 220 168 21 49
 131 164 172 58 11 252 79 121 259 235 151 217 191 122 93 211 139 160 210
 43 88 106 228 189 57 165 114 44 105 206 183 232 212 266 176 142 86 202
 147 110 47 192 5 251 149 69 186 196 244 115 109 84 161 82 29 126 197
 254 245 61 242 80 158 53 231 219 22 103 116 133 71 101 55 96 262 171 98

194 42 41 63 127 167 40 163 246 188 203 187 48 222 97 157 200 20 123
 238 24 185 100 198 12 50 6 3

(4) $q = 32$. Let

$E = \{1, 2, 4, 8, 16, 32, 55, 64, 110, 128, 139, 220, 256, 278, 299, 339, 349, 440, 453, 512, 529, 556, 598, 678, 698, 703, 755, 793, 880, 906, 925, 991, 1024\}$. Since $s = 3 \cdot 331$, we can apply Proposition 56. We take $y = 297$ and choose A such that $113 \in A$ and thus $775 = [113(1 + s/3)]_s \notin A$. The application of Algorithm 57 shows that there is no cyclic planar difference set D of order 32^2 satisfying (4.3) and $f_D(1) = y$. Moreover, there is a unique D satisfying (4.3), $f_D(3) = 297$, and $f_D(113) = \min\{f_D(x) : x \in \{1, \dots, s-1\}, (x, s) = 1\}$. According to Proposition 56, this shows that there is exactly one cyclic planar difference set of order 32^2 , up to equivalence. The following are representatives of the values of the unique function f_D for which (4.3) holds, and which satisfies $f_D(3) = 297$, and $f_D(113) = \min\{f_D(x) : x \in \{1, \dots, s-1\}, (x, s) = 1\}$. The remaining

values of f_D can be determined by Proposition 47.

x	1	3	5	7	9	11	13	15	17	19	21	23
$f(x)$	168	297	594	1012	161	251	675	832	1030	823	659	984

x	25	27	29	37	41	43	45	49	51	53	55	57
$f(x)$	432	1020	871	370	497	318	597	601	843	50	67	966

x	67	69	71	73	75	83	87	103	149	331		
$f(x)$	746	369	587	820	869	499	540	408	493	0		

These results lead to the following.

Theorem 58. *Let q be a prime power such that $q \leq 16$ or $q = 32$. Then every cyclic projective plane of order q^2 is desarguesian.*

Proof. For $q \leq 9$, this was shown by Bruck [5]. The cases $q = 11, 13, 16, 32$ have been dealt with above. □

Remark 59. *Using Algorithm 57, we have independently verified all results of Bruck [5].*

Corollary 60. *The cyclic group of order $v = 1,049,601$ contains a unique nontrivial difference set, up to equivalence.*

Proof. It is straightforward to check that, up to taking complements, we have $k \in \{1025, 460800, 461825\}$ if a (v, k, λ) difference set exists (see [2] for the definitions). Note that $v = q^2 + q + 1$ where $q = 1024$. Theorem 58 and Proposition 44 imply that there is a unique (v, k, λ) difference with $k = 1025$ cyclic group of order v . The Mann Test (see [2]) shows that there is no (v, k, λ) difference with $k \in \{460800, 461825\}$ in this group. $\square$

4.4. Cyclic Planes of Nonsquare Order

In this section, we use a depth first search algorithm together with homomorphic images to search for cyclic planes of order less than 41 and of orders 125 and 128. We first introduce some notation.

Let D be a subset of a cyclic group. We say that the condition $\Gamma(D)$ holds if $d_1 d_2^{-1} \neq d_3 d_4^{-1}$ for all $d_1, \dots, d_4 \in D$ with $d_1 \neq d_2$.

Algorithm 61 (Depth first search for cyclic planes).

Input: $q = p^a$ where p is prime.

Output: A set $\mathcal{S}$ such that every cyclic planar difference set of order q is equivalent to an element of $\mathcal{S}$

Initialization:

1. Let G be a cyclic group of order $q^2 + q + 1$, and let $O_1, \dots, O_t$ be the orbits of $x \mapsto x^p$ on G .
2. Set $\mathcal{S} := \emptyset$, $D := \emptyset$, $L := 1$, and $f(x) := 0$, $x = 1, \dots, t$.

Main Step:

- (i) If $|D| = q + 1$, then set $\mathcal{S} := \mathcal{S} \cup \{D\}$, $L := L - 1$, $D := D \setminus O_{f(L)}$.
- (ii) Repeat until $L = 0$ or $f(L) < t$:

$f(L) := 0$, $L := L - 1$. If $L > 0$, then set $D := D \setminus O_{f(L)}$.
- (iii) If $L = 0$, then output $\mathcal{S}$ and terminate the execution of the algorithm.
- (iv) Set $y := f(L) + 1$. If $f(L) > 0$, then set $E := (D \setminus O_{f(L)}) \cup O_y$. If $f(L) = 0$, then set $E := D \cup O_y$.
- (v) Set $f(L) := f(L) + 1$.
- (vi) If $\Gamma(E)$ holds, then set $D := E$, $L := L + 1$.
- (vii) Go to step (i).

The correctness of Algorithm 61 can be proved using the definition of a planar difference set and Proposition 43. For $q \leq 19$ and $q = 128$, a straightforward implementation of Algorithm 61 on a PC is sufficient to find all planar difference sets of order q up to equivalence. All difference sets found are equivalent to Singer difference sets. Thus all cyclic projective planes of order at most 19 and of order 128 are desarguesian.

For $q = 23, 29, 31, 37, 125$, we can use the results below to speed up Algorithm 61.

We first introduce some notation. Let $q = p^a$ where p is a prime, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v . Let u be a divisor of v and $x \in \{0, \dots, u - 1\}$. We set

$$\mathcal{O}(x, q, u) = \{\{g^{yp^t} : t \in \mathbb{N}\} : y \in \mathbb{Z}, y \equiv x \pmod{u}\}.$$

The elements of $\mathcal{O}(x, q, u)$ will be called *orbits* since they are orbits of the map $z \mapsto z^p$ on G .

Lemma 62. *Let $q = 23$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v . Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(q)}$ which contains $\{g, g^{23}, g^{489}\}$, two further orbits in $\mathcal{O}(1, 23, 7)$ and five orbits in $\mathcal{O}(3, 23, 7)$.*

Proof. By Result 43 we can assume $D = D^{(23)}$. Let U be the subgroup of G of order 79. Let $\rho : G \rightarrow G/U$ be the natural epimorphism, and write $\rho(D) = \sum_{i=0}^6 a_i h^i$ where $a_i \in \mathbb{Z}$ and h is a generator of G/U . As $D^{(23)} = D$, we have $\rho(D)^{(2)} = \rho(D)$, and thus $a_1 = a_2 = a_4$ and $a_3 = a_6 = a_5$. Since $|D| = 24$, we have $\sum a_i = 24$. Comparing the coefficient of the identity element in (??), we get $\sum a_i^2 = 23 + 79 = 102$. The only solutions to these conditions are $a_0 = 0$, $a_1 =$

$a_2 = a_4 = 3$, $a_3 = a_6 = a_5 = 5$ and $a_0 = 0$, $a_1 = a_2 = a_4 = 5$, $a_3 = a_6 = a_5 = 3$. Replacing D by $D^{(3)}$, if necessary, we can assume $a_0 = 0$, $a_1 = a_2 = a_4 = 3$, and $a_3 = a_6 = a_5 = 5$. Note that every orbit in $\mathcal{O}(1, 23, 7)$ contained in D contributes exactly 1 to a_1 , a_2 , and a_4 . Similarly, every orbit in $\mathcal{O}(3, 23, 7)$ contained in D contributes exactly 1 to a_3 , a_6 , and a_5 . Thus D consists of three orbit in $\mathcal{O}(1, 23, 7)$ and five orbit in $\mathcal{O}(3, 23, 7)$. At least one element of $\mathcal{O}(1, 23, 7)$ contained in D , say O , contains a group element g^x with $(x, 533) = 1$. Thus there is an integer y with $y \equiv 1 \pmod{7}$ and $(y, 533) = 1$ such that $g^y \in O$. Let t be an integer with $t \equiv 1 \pmod{7}$ and $ty \equiv 1 \pmod{79}$. Replacing D by $D^{(t)}$, if necessary, we can assume $g^{ty} = g \in D$. Since $D = D^{(23)}$, this implies $\{g, g^{23}, g^{489}\} \subset D$. $\square$

Lemma 63. *Let $q = 29$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v . Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(q)}$ which contains $\{g^2, g^{58}, g^{811}\}$, one further orbit in $\mathcal{O}(2, 29, 13)$, three orbits in $\mathcal{O}(0, 29, 13)$, three orbits in $\mathcal{O}(4, 29, 13)$, and four orbits in $\mathcal{O}(7, 29, 13)$. Let $q = 29$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v . Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(q)}$ which contains $\{g^2, g^{58}, g^{811}\}$, one further orbit in $\mathcal{O}(2, 29, 13)$, three orbits in $\mathcal{O}(0, 29, 13)$, three orbits in $\mathcal{O}(4, 29, 13)$, and four orbits in $\mathcal{O}(7, 29, 13)$.*

Proof. By Proposition 43 we can assume $D = D^{(29)}$. Let U be the subgroup of G of order 67. Let $\rho : G \rightarrow G/U$ be the natural epimorphism, and write $\rho(D) = \sum_{i=0}^{12} a_i h^i$ where $a_i \in \mathbb{Z}$ and h is a generator of G/U . As $D^{(29)} = D$, we have $\rho(D)^{(3)} = \rho(D)$, and thus $a_1 = a_3 = a_9$, $a_2 = a_6 = a_5$, $a_4 = a_{12} = a_{10}$, and $a_7 = a_8 = a_{11}$. Since $|D| = 30$, we have $\sum a_i = 30$. Comparing the coefficient of the identity element in (??), we get $\sum a_i^2 = 29 + 67 = 96$. There are exactly 30 solutions $(a_0, \dots, a_{12})$ to these conditions, and the only solutions which satisfy (??) are given in the following table (the values of the other a_i 's can be deduced from the equations above).

a_0	a_1	a_2	a_4	a_7
3	0	2	3	4
3	4	0	2	3
3	3	4	0	2
3	2	3	4	0

Replacing D by $D^{(2)}$, $D^{(4)}$, or $D^{(8)}$, if necessary, we can assume $a_0 = 3$, $a_1 = 0$, $a_2 = 2$, $a_4 = 3$, and $a_7 = 4$. Note that, for $x \in \{0, 1, 2, 4, 7\}$ every orbit in $\mathcal{O}(x, 29, 13)$ contained in D contributes exactly 1 to a_x . This implies that D contains three orbits in $\mathcal{O}(0, 29, 13)$, two orbits in $\mathcal{O}(2, 29, 13)$, three orbits in $\mathcal{O}(4, 29, 13)$, and four orbits in $\mathcal{O}(7, 29, 13)$. At least one orbit in $\mathcal{O}(2, 29, 13)$

contained in D , say O , contains an element g^x with $(x, 871) = 1$. Thus there is an integer y with $y \equiv 2 \pmod{13}$ and $(y, 871) = 1$ such that $g^y \in O$. Let t be an integer with $t \equiv 1 \pmod{13}$ and $ty \equiv 2 \pmod{67}$. Replacing D by $D^{(t)}$, if necessary, we can assume $g^{ty} = g^2 \in D$. Since $D = D^{(29)}$, this implies $\{g^2, g^{58}, g^{811}\} \subset D$. $\square$

The following three lemmas can be proved by similar arguments, and we skip their proof.

Lemma 64. *Let $q = 31$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v . Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(q)}$ which contains $\{g^{331}, g^{662}\}$, four orbits in $\mathcal{O}(0, 31, 3)$ different from $\{1\}$, four orbits in $\mathcal{O}(1, 31, 3)$ different from $\{g^{331}\}$, and two orbits in $\mathcal{O}(2, 31, 3)$ different from $\{g^{662}\}$.*

Lemma 65. *Let $q = 37$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v . Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(q)}$ which contains $\{g^{469}, g^{938}\}$ and satisfies one of the following conditions.*

- (i) *For $x \in \{4, 6, 17, 18, 25, 27, 30, 41\}$, the difference set D contains $N(x)$ orbits in $\mathcal{O}(x, 37, 67)$ where $N(x)$ is given in the following table.*

x	4	6	15	17	18	25	27	30	41
$f(x)$	2	1	2	2	1	1	1	1	1

- (ii) *The difference set D contains one orbit in $\mathcal{O}(0, 37, 67)$ different from $\{0\}$, $\{g^{469}\}$, and $\{g^{938}\}$ and exactly one orbit from $\mathcal{O}(x, 37, 67)$ for each $x \in \{2, 3, 5, 8, 12, 18, 27, 30, 32, 34, 41\}$.*

Lemma 66. *Let $q = 125$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v . Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(5)}$ which contains exactly two orbits from $\mathcal{O}(1, 125, 829)$.*

Using Lemmas 62-66 to reduce the number of choices for the orbits in Algorithm 61 dramatically narrows the search space. For instance, a complete search for cyclic projective planes of order 37 using Lemma 65 takes less than three seconds on a PC. Straightforward implementations show that all cyclic planar difference sets of orders 23, 29, 31, 37, and 125 are equivalent to Singer difference sets. Summarizing the results of this section, we have the following.

Theorem 67. *Every cyclic projective plane of order at most 37 and of order 125 or 128 is desarguesian.*

References

- [1] L.D. Baumert, D.M. Gordon: On the existence of cyclic difference sets with small parameters. In: High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun. 41 (2004), 61-68.
- [2] T. Beth, D. Jungnickel, H. Lenz: Design theory (2nd ed.), Cambridge Univer. Press (1999).
- [3] R.C. Bose: An affine analogue of Singer's theorem. J. Indian Math. Soc. 6, (1942), 1-15.
- [4] R.H. Bruck, H.J. Ryser: The nonexistence of certain finite projective planes, Canadian J. Math. 1 (1949), 88-93
- [5] R.H. Bruck: Quadratic Extensions of Cyclic Planes. Proc. Sympos. appl. Math. 10 (1960), 15-44.
- [6] Y.Q. Chen, D.K. Ray-Chaudhuri, Q.Xiang: Constructions of partial difference sets and relative difference sets using Galois rings II. J. Combin. Theory Ser. A 76 (1996), 179-196.
- [7] J.A. Davis: Construction of relative difference sets in p-groups. Disc. Math. 103 (1992), 7-15.
- [8] J.A. Davis, S.K. Sehgal: Using the simplex code to construct relative difference sets in 2-groups. Des. Codes Cryptogr. 11(1997), 267-277.
- [9] J.A. Davis, J. Jedwab, M. Mowbray: New families of relative difference sets. Des. Codes Cryptogr. 13 (1998), 131-146.

- [10] J.A. Davis, J. Jedwab: A unifying construction for difference sets, *J. Combin. Theory Ser. A* 80 (1997), 13-78.
- [11] P. Dembowski: Finite geometries. Repr. of the 1968 ed. Springer (1997).
- [12] J.F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, *J. Combin. Theory Ser. A* 40 (1985), 9-21.
- [13] E. Ellers, H. Karzel: Endliche Inzidenzgruppen. *Abh. Math. Semin. Univ. Hamb.* 27 (1964), 250-264.
- [14] D.T. Elvira: On Semi-regular relative difference sets in non-abelian groups of order p^4 . *Kyushu J. Math.* 56 (2002), 419-431.
- [15] A.D. Garciano, Y.Hiramine, T.Yokonuma: On relative difference sets in dihedral groups. *Des. Codes Cryptogr.* 29 (2006), 51-63.
- [16] D.M. Gordon: The prime power conjecture is true for $n < 2,000,000$. *J. Comb.* 1 (1994), 101-107.
- [17] B. Gordon, W.H. Mills, L.R. Welch: Some new difference sets. *Canad. J. Math.* 14 (1962) 614-625.
- [18] M. Hall: Cyclic projective planes. *Duke Math. J.* 14 (1947), 1079-1090.
- [19] M. Hall: A survey of difference sets. *Proc. Am. Math. Soc.* 7 (1957), 975-986.
- [20] M. Hall, H.J. Ryser: Cyclic incidence matrices. *Canad. J. Math.* 3 (1951), 495-502.
- [21] Y. Huang, B. Schmidt: Uniqueness of some cyclic projective planes. *Des. Codes Cryptogr.* 50 (2009), 253-266.
- [22] M. Harada, C. Lam, V.D. Tonchev: sSymmetric $(4, 4)$ -nets and generalized Hadamard matrices over groups of order 4. *Des. Codes Cryptogr.* 34 (2005), 71-87.
- [23] J.W.P. Hirschfeld: Projective geometries over finite fields. 2nd ed. Oxford Mathematical Monographs. Clarendon Press (1998).

- [24] D. Jungnickel: On automorphism groups of divisible designs. *Canad. J. Math.* 34 (1982) 257-297.
- [25] D. Jungnickel: The isomorphism problem for abelian projective planes. *Appl. Algebra Eng. Commun. Comput.* 19, (2008) 195–200.
- [26] C.W.H. Lam: The search for a finite projective plane of order 10. *Amer. Math. Monthly* 98 no. 4, (1991), 305–318.
- [27] K.H. Leung, B. Schmidt: Asymptotic nonexistence of difference sets in dihedral groups. *J. Combin. Theory Ser. A* 99 (2002), 261-280.
- [28] R. Lidl, H. Niederreiter, P.M. Chon: *Finite fields*. Cambridge Univer. Press (1997).
- [29] S.L. Ma, B. Schmidt: On (p^a, p, p^a, p^{a-1}) -relative difference sets. *Des. Codes Cryptogr.* 6(1995), 57-72.
- [30] S.L. Ma, B. Schmidt: Relative (p^a, p^b, p^a, p^{a-b}) -difference sets: A unified Exponent Bound and a Local Ring Construction. *Finite Fields appli.* 6 (2000), 1-22.
- [31] R.L. McFarland: A family of difference sets in non-cyclic groups. *J. Combin. Theory Ser. A* 15 (1973), 1-10.
- [32] R.L. McFarland, B.F. Rice: Translates and multipliers of abelian difference sets. *Proc. Amer. Math. Soc.* 68 (1978), 375-379.
- [33] R.L. McFarland: On multipliers of abelian difference sets. Ph. D. dissertation. Ohio State Univer. (1970).
- [34] M.F. Newman: On a class of nilpotent groups, *Proc. London Math. Soc. Third Series* 10 (1960), 365–375
- [35] A. Pott: A survey on relative difference sets, in *Groups, Difference Sets and the Monster*. EDs. K.T. Arasu et al. De Gruyter, Berlin, (1996), 195-233.
- [36] D.J.S. Robinson: *A course in the theory of groups*. 2nd Ed. Springer (1996).
- [37] B. Schmidt: On (p^a, p^b, p^a, p^{a-b}) -relative difference sets. *J. Alg. Combin.* 6 (1997), 279–297.

- [38] B. Schmidt: *Characters and Cyclotomic Fields in Finite Geometry*, Springer (2002).
- [39] J. Singer: A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* 43 (1938), 377-385.
- [40] K. Zhou: A remark on linear permutation polynomials, *Finite Fields appli.* 14 (2008), 532-536.
- [41] <http://www.uwyo.edu/moorhouse/pub/planes/>