

2015

Partial geometric designs and difference families

Kathleen Elizabeth Nowak
Iowa State University

Follow this and additional works at: <https://lib.dr.iastate.edu/etd>

 Part of the [Mathematics Commons](#)

Recommended Citation

Nowak, Kathleen Elizabeth, "Partial geometric designs and difference families" (2015). *Graduate Theses and Dissertations*. 14519.
<https://lib.dr.iastate.edu/etd/14519>

This Dissertation is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

Partial geometric designs and difference families

by

Kathleen Elizabeth Nowak

A dissertation submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of
DOCTOR OF PHILOSOPHY

Major: Mathematics

Program of Study Committee:

Sung Yell Song, Major Professor

Clifford Bergman

Steve Butler

Leslie Hogben

Zhijun Wu

Iowa State University

Ames, Iowa

2015

Copyright © Kathleen Elizabeth Nowak, 2015. All rights reserved.

DEDICATION

To my parents, Lawrence and Heidi, and to my siblings, Chelsea and William, my very first
math students and partners in crime

TABLE OF CONTENTS

LIST OF TABLES	vi
LIST OF FIGURES	vii
ACKNOWLEDGEMENTS	viii
ABSTRACT	ix
CHAPTER 1. GENERAL INTRODUCTION	1
1.1 Designs	1
1.2 Difference families	4
1.2.1 Terminology	4
1.2.2 Group rings	6
1.3 Connection between difference families and designs	8
1.4 Dissertation organization	8
CHAPTER 2. PARTIAL GEOMETRIC DIFFERENCE FAMILIES	10
Abstract	10
2.1 Introduction	10
2.2 Preliminaries	11
2.2.1 Block designs	11
2.2.2 Difference sets and difference families	12
2.2.3 Partial geometric difference family	13
2.3 Difference families, partial geometric designs, and directed strongly regular graphs	14
2.4 Some feasibility conditions on parameters	17
2.5 Some families in finite fields	19
2.6 Some families in cyclic groups	20

2.7	Some families in \mathbb{Z}_v with $v = 2^u$	22
2.8	Some families in \mathbb{Z}_v with v an odd prime power	25
2.9	Concluding remarks	26
2.9.1	Partial geometric difference families and the obtained directed strongly regular graphs	27
2.9.2	Overlap with partial difference sets, almost difference sets, and almost difference families	28
CHAPTER 3. PARTIAL GEOMETRIC DESIGNS WITH PRESCRIBED		
	AUTOMORPHISMS	33
	Abstract	33
3.1	Introduction	33
3.2	Preliminaries	35
3.3	Partial geometric designs with specified automorphisms	39
3.4	Partial geometric difference family constructions	46
3.5	Concluding remarks	52
CHAPTER 4. LINKS BETWEEN ORTHOGONAL ARRAYS, ASSOCIA-		
	TION SCHEMES AND PARTIAL GEOMETRIC DESIGNS	54
	Abstract	54
4.1	Introduction	54
4.2	Preliminaries	56
4.2.1	Designs	56
4.2.2	Association schemes and their Bose-Mesner algebras	57
4.3	Strongly regular graphs with either $k = \mu$ or $\lambda = \mu$	58
4.4	Wreath product of a scheme by a one-class association scheme	60
4.5	Certain three-class self-dual association schemes of order $3m^2$	62
4.6	The association schemes from codes and orthogonal arrays	66
4.6.1	From Hamming schemes	66
4.6.2	From orthogonal arrays of strength two	69

4.7	Directed strongly regular graphs	76
4.8	Concluding remarks	78
CHAPTER 5. SUMMARY AND DISCUSSION		80
5.1	General discussion	80
5.2	Recommendations for future research	80
BIBLIOGRAPHY		82

LIST OF TABLES

Table 2.1	Parameters of DSRGs obtained from PGDFs	28
Table 3.1	Parameters of partial geometric designs obtained from PGDFs	53
Table 4.1	Parameters of DSRGs obtained from partial geometric designs	77

LIST OF FIGURES

Figure 1.1 Fano's Plane 2

ACKNOWLEDGEMENTS

First and foremost, I would like to thank professor Sung-Yell Song for his guidance, patience, and encouragement. He believed in me and pushed me to my limits as a mathematician. I am proud to have been your student, Dr. Song. Next, I would like to thank my committee members for their support and oversight on this work: Drs. Cliff Bergman, Steve Butler, Leslie Hogben, and Zhijun Wu. I would also like to thank my family for their love and encouragement. It has been a long road but I am finally here. Thank you for always believing in me. I would also like to thank all my friends in the math department. You were my first collaborators and partners on this crazy journey. Finally, I would like to thank Juan Marcos Brandi. You were my family for the last five years, standing beside me through the good times and the bad.

ABSTRACT

We examine the designs produced by different types of difference families. Difference families have long been known to produce designs with well behaved automorphism groups. These designs provide the elegant solutions desired for applications. In this work, we explore the following question: Does every (named) design have a difference family analogue? We answer this question in the affirmative for partial geometric designs.

CHAPTER 1. GENERAL INTRODUCTION

In this chapter, we start by introducing our main objects of study, designs and difference families. We provide the necessary background and a brief history of each. Next, we reveal how these concepts are connected and we present the question which motivates this work. Finally, we close with a summary of the thesis organization.

1.1 Designs

Combinatorial design theory asks questions about whether it is possible to arrange elements of a finite set into subsets so that certain “balance” properties are satisfied. Designs were formally introduced in the 1920s to answer questions about the design and analysis of statistical experiments [53]. Since then many different types have been introduced, each motivated by a particular application.

Definition 1. *A block design is a pair (P, \mathcal{B}) where*

1. *P is a finite set of elements called points, and*
2. *\mathcal{B} is a family of nonempty subsets of P called blocks.*

If two blocks are identical, they are said to be repeated blocks. A design is said to be *simple* if it does not contain repeated blocks. A point-block pair (x, B) is called a *flag* if $x \in B$; otherwise, it is called an *antiflag*. Designs provide a way of capturing certain combinatorial and algebraic properties. The first level of order imposed on a design is almost always the following.

Definition 2. *A tactical configuration (also called a 1-design) with parameters (v, b, k, r) is a design (P, \mathcal{B}) with $|P| = v$ and $|\mathcal{B}| = b$ such that each block consists of k points and each point*

belongs to r blocks.

The t -designs, tied to the design of efficient statistical experiments, are probably the most studied type of design. They were introduced by Fischer and Yates in the 1930s [53].

Definition 3. Let v , k , and λ be positive integers such that $v > k \geq 2$. A t -design with parameters (v, k, λ) is a tactical configuration (P, \mathcal{B}) where $|\{B \in \mathcal{B} \mid X \subset B\}| = \lambda$ for each t -subset $X \subset P$.

The 2-designs, often called balanced incomplete block designs, are most widely used in application.

Example 4. The following is a 2-design with parameters $(7, 3, 1)$.

$$P = \{1, 2, 3, 4, 5, 6, 7\}$$

$$\mathcal{B} = \{123, 246, 145, 167, 246, 257, 347, 356\}$$

This 2-design has a famous diagrammatic representation which is known as the Fano plane.

More generally, a 2-design with parameters $(v, 3, 1)$ is called a Steiner triple system.

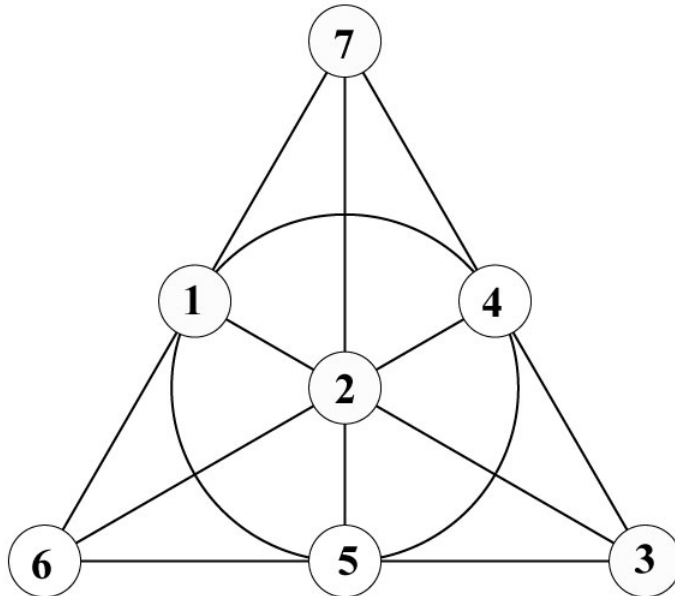


Figure 1.1 Fano's Plane

Below we list some of the other more widely studied designs.

Definition 5. A design (P, \mathcal{B}) is called a projective plane if

1. any two distinct points are contained in exactly one block,
2. any two blocks intersect in exactly one point, and
3. there exists a quadrangle, that is, four points no three of which are contained in a common block.

Definition 6. A design (P, \mathcal{B}) is called an affine plane if

1. any two distinct points are contained in exactly one block,
2. given any point p and any block B with $p \notin B$, there is precisely one block H with $p \in H$ that does not intersect B , and
3. there is a triangle, that is, three points which are not contained in a common block.

Definition 7. A divisible design with parameters $(v, b, k, r; m, \lambda_1, \lambda_2)$ is a triple (P, \mathcal{B}, G) where (P, \mathcal{B}) is a tactical configuration and G is a partition of P into m groups such that for any pair of distinct points $p_1, p_2 \in P$

$$|\{B \in \mathcal{B} \mid p_1, p_2 \in B\}| = \begin{cases} \lambda_1, & \text{if } p_1 \text{ and } p_2 \text{ belong to the same group} \\ \lambda_2, & \text{otherwise.} \end{cases}$$

Definition 8. A partial geometry with parameters $(v, b, k, r; \tau)$ is a tactical configuration (P, \mathcal{B}) such that

1. Any two points are contained together in at most one block, and
2. for any point block pair (p, B) , if $p \notin B$, then there exist τ blocks which contain p and intersect with B .

Definition 9. A partial geometric design with parameters $(v, b, k, r; \alpha, \beta)$ is a tactical configuration (P, \mathcal{B}) with parameters (v, b, k, r) which satisfies the property:

For every point $x \in P$ and every block $B \in \mathcal{B}$, the number of flags (y, C) such that $y \in B$ and $x \in C$, is β if $x \in B$, and is α if $x \notin B$.

It is often convenient to represent a design with an incidence matrix.

Definition 10. Let (P, \mathcal{B}) be a design with $|P| = v$ and $|\mathcal{B}| = b$. The incidence matrix of (P, \mathcal{B}) is the $v \times b$ $\{0, 1\}$ -matrix N defined by the rule

$$N_{i,j} = \begin{cases} 1, & \text{if } p_i \in B_j \\ 0, & \text{otherwise.} \end{cases}$$

Designs arise in a multitude of settings so a notion of equivalence is necessary.

Definition 11. Suppose that (P, \mathcal{B}) and (Y, \mathcal{A}) are two designs with $|P| = |Y|$. (P, \mathcal{B}) and (Y, \mathcal{A}) are isomorphic if there exists a bijection $\pi : P \rightarrow Y$ such that

$$[\pi(B) : B \in \mathcal{B}] = \mathcal{A}.$$

In other words, if we rename every point $x \in P$ by $\pi(x)$, then the collection of blocks \mathcal{B} is transformed into \mathcal{A} . The bijection π is called an isomorphism.

In particular, an isomorphism from a design to itself is called an automorphism. Isomorphisms between designs can be described in terms of incidence matrices as follows.

Theorem 12. Suppose that M and N are both $v \times b$ incidence matrices of designs. Then two designs are isomorphic if and only if there exists a permutation α of $\{1, 2, \dots, v\}$ and a permutation β of $\{1, 2, \dots, b\}$ such that

$$M_{i,j} = N_{\alpha(i),\beta(j)}$$

Since designs are formulated to possess certain combinatorial properties, many of the fundamental questions are existence questions. Specifically, designs with certain prescribed automorphisms generally provide the elegant solutions sought in application.

1.2 Difference families

1.2.1 Terminology

A difference set is a subset of a group which generates a difference table with certain regularity properties. Let G be a finite group. For a given subset $S \subset G$, we define the multiset

$\Delta(S)$ by

$$\Delta(S) := [xy^{-1} : x, y \in S].$$

Next for any element $z \in G$, we define $\delta_S(z) := |\{(x, y) \in S \times S : xy^{-1} = z\}|$. That is, $\delta_S(z)$ is the multiplicity of z in $\Delta(S)$. With these definitions, a difference set is described as follows.

Definition 13. *Let G be a finite group of order v . A k -subset S of G is called a (v, k, λ) -difference set if $\delta_S(z) = \lambda$ for each non-identity element $z \in G$.*

Difference sets were introduced by Singer in 1930 [50]. They can be used to produce binary sequences with two-level autocorrelation as well as two weight codes [2]. These sets were then generalized to difference families by R. M. Wilson in the 1960s [58] and have recently been applied in the study of multiple-access communication [56]. For a family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of subsets of G , we define the multiset $\Delta(\mathcal{S})$ by

$$\Delta(\mathcal{S}) := [xy^{-1} : x, y \in S_i \text{ for some } i \in \{1, 2, \dots, n\}] = \bigsqcup_{i=1}^n \Delta(S_i)$$

where the union \bigsqcup is a concatenation of multisets. Next, for a non-identity element $z \in G$, we define $\delta_j(z) := |\{(x, y) \in S_j \times S_j : xy^{-1} = z\}|$ to be the multiplicity of z in $\Delta(S_j)$ and $\delta(z) := \sum_{j=1}^n \delta_j(z)$ to be the multiplicity of z in $\Delta(\mathcal{S})$. With this notation, a difference family is defined as follows.

Definition 14. *Let G be a finite group of order v . A family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of distinct k -subsets of G is called a (v, k, n, λ) -difference family if $\delta(z) = \lambda$ for each non-identity element $z \in G$.*

Over the last few decades, many variations of this definition have been studied. In all cases, a partition of a group is specified and we look for sets (families) whose difference table includes every subset of the partition with constant multiplicity. Some of the more widely studied variations are as follows.

Definition 15. *A k -element subset S of a group G of order v is called a (v, k, λ, t) -almost difference set if $\delta_S(x)$ takes on the value λ altogether t times and $\lambda + 1$ altogether $v - t - 1$ as x ranges over $G \setminus \{e\}$.*

Almost difference sets are used to obtain binary sequences with three-level autocorrelation [2]. Almost difference families have also been studied [26].

Definition 16. A k -element subset S of a group G is called a (v, k, λ, μ) -partial difference set if for each non-identity element $x \in G$

$$\delta_S(x) = \begin{cases} \lambda, & \text{if } x \in S \\ \mu, & \text{otherwise.} \end{cases}$$

Partial difference sets are used to produce strongly regular Cayley graphs and two-weight codes [40].

Definition 17. Let G be a group of order v and let $N \leq G$ be subgroup of order m . A k -element subset $S \subset G$ is called a $(v, m, k, \lambda_1, \lambda_2)$ -divisible difference set if for each non-identity element $x \in G$

$$\delta_S(x) = \begin{cases} \lambda_1, & \text{if } x \in N \\ \lambda_2, & \text{otherwise.} \end{cases}$$

In particular, if $\lambda_1 = 0$ and $\lambda_2 = \lambda$, then S is called a (v, m, k, λ) -relative difference set. Divisible difference families have also been studied. These families give rise to optical orthogonal codes which are used in frequency-hopping spread-spectrum communication [17].

1.2.2 Group rings

Difference sets are characterized by the multiplicities of certain group elements coming as differences taken within a set. Therefore, an efficient tool for working with differences within a group is required.

Let G be a group and let \mathbb{Z} denote the ring of integers. Then we define the group ring $\mathbb{Z}[G]$ to be the ring of formal sums

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g X^g \mid a_g \in \mathbb{Z} \right\}$$

where X is an indeterminate variable. The ring $\mathbb{Z}[G]$ has the operation of addition given by

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

and the operation of multiplication defined by

$$\left(\sum_{g \in G} a_g X^g \right) \left(\sum_{g \in G} b_g X^g \right) = \sum_{h \in G} \left(\sum_{g \in G} a_g b_{g^{-1}h} \right) X^h.$$

The zero and unit of $\mathbb{Z}[G]$ are $\sum_{g \in G} 0X^g := \underline{0}$ and $X^e := \underline{1}$ respectively where e denotes the identity of G . If S is a subset of G , we will identify S with the group ring element $S(X) = \sum_{s \in S} X^s$. This sum is sometimes referred to as a *simple quantity*. Additionally, we define $S(X^{-1}) = \sum_{s \in S^{-1}} X^s$ where $S^{-1} = \{s^{-1} \mid s \in S\}$. With this new terminology, we are able to provide a more succinct characterization of the different types of difference sets.

Proposition 18. *Let G be a group of order v and let S be a k -subset of G . Then S is a (v, k, λ) -difference set in G if and only if in $\mathbb{Z}[G]$,*

$$S(X)S(X^{-1}) = k \cdot \underline{1} + \lambda(G(X) - \underline{1}).$$

Proposition 19. *Let G be a group of order v and let S be a k -subset of G . Then S is an (v, k, λ, t) -almost difference set in G if and only if there exists a t -subset D of $G \setminus \{0\}$ such that*

$$S(X)S(X^{-1}) = k \cdot \underline{1} + \lambda D(X) + (\lambda + 1)(G(X) - D(X) - \underline{1})$$

in $\mathbb{Z}[G]$.

Proposition 20. *Let G be a group of order v and let S be a k -subset of G . Then S is a (v, k, λ, μ) -partial difference set in G if and only if in $\mathbb{Z}[G]$,*

$$S(X)S(X^{-1}) = \begin{cases} k \cdot \underline{1} + \lambda(S(X) - \underline{1}) + \mu(G(X) - S(X)), & \text{if } e \in S \\ k \cdot \underline{1} + \lambda S(X) + \mu(G(X) - S(X) - \underline{1}), & \text{if } e \notin S. \end{cases}$$

Proposition 21. *Let G be a group of order v , N a subgroup of G of order m , and S a k -subset of G . Then S is a $(v, m, k, \lambda_1, \lambda_2)$ -divisible difference set in G relative to N if and only if in $\mathbb{Z}[G]$,*

$$S(X)S(X^{-1}) = k \cdot \underline{1} + \lambda_1(N(X) - \underline{1}) + \lambda_2(G(X) - N(X)).$$

1.3 Connection between difference families and designs

In this section we establish the connection between difference families and designs.

Let G be a group of order v and let S be a subset of G . For any element $g \in G$, we define the *translate* of S by g as $Sg := \{xg : x \in S\}$. We then define $Dev(S) := [Sg : g \in G]$ to be the collection of all v translates of S . The set S is called the *base set* and $Dev(S)$ is called the *development*. Similarly, we define the development of a family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of distinct k -element subsets of G to be the vn -multiset

$$Dev(\mathcal{S}) := \bigsqcup_{i=1}^n [S_i g : g \in G].$$

Then $(G, Dev(S))$ and $(G, Dev(\mathcal{S}))$ are designs. Constructing designs in this way is referred to as the method of difference sets (families).

Now the key here lies in the choice for the base set. In particular, taking \mathcal{S} to be a certain type of difference family produces a design with a well behaved automorphism group. When \mathcal{S} is a classical difference family, $(G, Dev(\mathcal{S}))$ is a 2-design with an automorphism group which acts transitively on both the point set and the block set. When \mathcal{S} is a divisible difference family, $(G, Dev(\mathcal{S}))$ is a divisible design admitting a group of automorphisms which acts regularly on the point set and semi-regularly on the block set. Designs with well structured automorphism groups are of interest since these designs provide the elegant solutions desired for applications. This connection begs the following question: Do all (named) designs have a difference family analogue and if so what sort of structure can be gleaned from the automorphism group of a particular design? This is the question we set out to investigate in this work. In particular, we will focus on partial geometric designs.

1.4 Dissertation organization

This dissertation is organized in the format of a dissertation containing journal papers. In the general introduction, the research problem is posed and pertinent background information is presented.

Chapter 2 contains the paper “Partial geometric difference families” accepted by the *Journal of Combinatorial Designs*. In the paper we introduce the notion of a partial geometric

difference family, a difference family analogue for the partial geometric design. We show that partial geometric difference families give rise to partial geometric designs admitting a group of automorphisms which acts regularly on the point set and semi-regularly on the block set. Next, we investigate necessary conditions for such a difference family. Finally, we construct infinite families of partial geometric difference families in the setting of Galois fields and cyclic groups.

Chapter 3 contains the paper “Partial geometric designs with prescribed automorphisms” submitted to *Designs, Codes, and Cryptography*. In this paper we generalize the well-known Kramer-Mesner theorem for 2-designs to partial geometric designs. This result provides a method that can be used to determine the existence or nonexistence of partial geometric designs having specified automorphisms. Additionally, we also provide more constructions of partial geometric difference families.

Chapter 4 contains the paper “Links between orthogonal arrays, association schemes, and partial geometric designs” submitted to *Designs, Codes, and Cryptography*. In this paper we investigate three-class association schemes as a possible source of partial geometric designs. We find that the desired association schemes come from certain orthogonal arrays of strength two and linear codes. As a consequence we are able to find an infinite family of partial geometric designs.

Chapter 5 contains concluding remarks and recommendations for future research.

CHAPTER 2. PARTIAL GEOMETRIC DIFFERENCE FAMILIES

A paper accepted by the *Journal of Combinatorial Designs*

Kathleen Nowak, Oktay Olmez, and Sung-Yell Song

Abstract

We introduce the notion of a partial geometric difference family as a variation on the classical difference family and a generalization of partial geometric difference sets. We study the relationship between partial geometric difference families and both partial geometric designs and difference families, and show that partial geometric difference families give rise to partial geometric designs. We construct several infinite families of partial geometric difference families using Galois rings and the cyclotomy of Galois fields. From these partial geometric difference families, we generate a list of infinite families of partial geometric designs and directed strongly regular graphs.

2.1 Introduction

Recently, Brouwer and the second and third authors [12] showed how to construct two directed strongly regular graphs from a given partial geometric design (also called a ‘ $1\frac{1}{2}$ -design’): One is defined on the set of flags of the design and the other is defined on the set of antiflags. Additionally, the second author [46] has introduced the notion of a partial geometric difference set, under the name ‘ $1\frac{1}{2}$ -difference set’, as a difference set version of a partial geometric design. Further, he showed that we can obtain partial geometric designs from partial geometric difference sets in precisely the same manner that we obtain symmetric 2-designs from ordinary difference sets. In this paper, we introduce the idea of a partial geometric difference family.

This notion generalizes both the classical difference family and the partial geometric difference set. As we will see in Theorem 57 below, a partial geometric difference family also yields a partial geometric design. Thus, we can obtain directed strongly regular graphs whenever we have partial geometric difference families as well.

The organization of the paper is as follows. In the following section, in order to introduce partial geometric difference families, our main objects of study, we recall some notation and basic terminology from block designs and difference sets. In Section 3.2, we discuss how partial geometric difference families relate to difference families, partial geometric designs, and directed strongly regular graphs. In Section 3.4, we investigate some necessary conditions to have a partial geometric difference family. In Sections 3.5 through 2.8, we construct infinite families of partial geometric difference families in Galois fields and cyclic groups by using cyclotomic classes of Galois fields and certain subsets or multiplicative subgroups of Galois rings. Finally, in Section 2.9, we summarize our constructions, highlighting the parameters of the resulting directed strongly regular graphs. We then close the section with a discussion of how partial geometric difference families align with other difference set variations, namely partial difference sets, almost difference sets, and almost difference families.

2.2 Preliminaries

2.2.1 Block designs

A (*block*) *design* is a pair (P, \mathcal{B}) consisting of a finite set P of points, and a finite collection (possibly multiset) \mathcal{B} of nonempty subsets of P called blocks.¹ A point-block pair (x, B) is called a *flag* if $x \in B$ and is otherwise called an *antiflag*. Let v, b, k and r be positive integers such that $v > k > 2$. A (v, b, k, r) -*tactical configuration*² is a design (P, \mathcal{B}) with $|P| = v$ and $|\mathcal{B}| = b$ such that each block consists of k points and each point belongs to r blocks. A *partial geometric design*³ with parameters $(v, b, k, r; \alpha, \beta)$ is a (v, b, k, r) -tactical configuration (P, \mathcal{B}) satisfying the ‘partial geometric’ property:

¹If two blocks in a design are identical as sets, they are said to be *repeated blocks*. A design is said to be a *simple design* if it does not contain repeated blocks.

²A tactical configuration is sometimes called a 1-design.

³Bose, Shrikhande and Singhi [8] called it a partial geometric design and Neumaier [43] called it a $1\frac{1}{2}$ -design.

For every point $x \in P$ and every block $B \in \mathcal{B}$, the number of flags (y, C) such that $y \in B$ and $C \ni x$, is β if $x \in B$, and is α if $x \notin B$.

Examples of partial geometric designs include 2-designs, transversal designs, and partial geometries.

2.2.2 Difference sets and difference families

Let G be a finite group. Given any subset $S \subset G$, we define the multiset $\Delta(S)$ by

$$\Delta(S) := [xy^{-1} : x, y \in S].$$

Notice that we denote a multiset by using $[]$. If all elements of a multiset have multiplicity one, then the multiset is a set. The order of the elements in a multiset is irrelevant, as with a set. For example, $[1, 2, 3] = \{1, 2, 3\} \neq [1, 2, 2, 3] = [1, 2, 3, 2]$. Moreover, this definition naturally extends to a family of subsets. Given a family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of subsets of G , we define the multiset $\Delta(\mathcal{S})$ by

$$\Delta(\mathcal{S}) := [xy^{-1} : x, y \in S_i \text{ for some } i \in \{1, 2, \dots, n\}] = \bigsqcup_{i=1}^n \Delta(S_i)$$

where the union \bigsqcup is a concatenation of multisets.

Next, we introduce notation for the multiplicity of an element participating in one of the aforementioned multisets. First, for a subset $S \subset G$ and an element $z \in G$, we define

$$\delta_S(z) := |\{(x, y) \in S \times S : z = xy^{-1}\}|.$$

That is, $\delta_S(z)$ is the multiplicity of z in $\Delta(S)$. Similarly, for a family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of subsets of G and an element $z \in G$, we define

$$\delta_j(z) := |\{(x, y) \in S_j \times S_j : z = xy^{-1}\}|$$

to be the multiplicity of z in $\Delta(S_j)$ and

$$\delta(z) := \sum_{j=1}^n \delta_j(z)$$

to be the multiplicity of z in $\Delta(\mathcal{S})$.

Now let G be a finite group of order v and let k and λ be integers such that $v > k > 2$. A (v, k, λ) -*difference set* in G is a k -element subset $S \subset G$ that satisfies the property: $\delta_S(x) = \lambda$ for each non-identity element $x \in G$. Similarly, a family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of distinct k -element subsets of G is called a (v, k, n, λ) -*difference family* in G if every non-identity element of G is contained in the multiset union $\bigsqcup_{j=1}^n \Delta(S_j)$ exactly λ times. Therefore, $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ is a difference family in G if and only if $\delta(x) = \sum_{j=1}^n \delta_j(x) = \lambda$ for each non-identity element x of G .

2.2.3 Partial geometric difference family

We now introduce the notion of a partial geometric difference family. This concept generalizes both the classical difference family and the partial geometric difference sets introduced by Olmez [46].

Definition 22. *Let v, k and n be integers with $v > k > 2$. Let G be a group of order v . A collection $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of distinct k -element subsets of G is called a *partial geometric difference family (PGDF)* in G with parameters $(v, k, n; \alpha, \beta)$ if there exist constants α and β such that, for each $x \in G$ and every $i \in \{1, 2, \dots, n\}$,*

$$\sum_{y \in S_i} \delta(xy^{-1}) = \begin{cases} \alpha & \text{if } x \notin S_i, \\ \beta & \text{if } x \in S_i. \end{cases}$$

In particular, when $n = 1$, the single member S_1 of the partial geometric difference family $\mathcal{S} = \{S_1\}$ is called a *partial geometric difference set* with parameters $(v, k; \alpha, \beta)$ [46].⁴ These families are of interest since they can be used to produce partial geometric designs and directed strongly regular graphs.

For further background information on designs, difference sets and difference families, we refer the readers to excellent books by Beth-Junickel-Lenz [4], Stinson [53] and the *CRC Handbook of Combinatorial Designs* [18] edited by Colbourn and Dinitz, and references found in there. For recent development of the theory as well as reports on different variations of difference sets and difference families, including partial difference sets (which are related to strongly

⁴The definition of the parameter β in [46] is different from ours. The value of β defined by Olmez is $2k - 1$ less than our β .

regular graphs), divisible difference sets, almost difference sets (which have applications in error correcting codes and sequence design), almost difference families and external difference families, especially, in connection with other sciences, we refer the readers to the following resources [2, 13, 16, 19, 22, 23, 24, 25, 26, 28, 33, 39, 41, 45, 57, 56].

2.3 Difference families, partial geometric designs, and directed strongly regular graphs

In this section, we establish ties between partial geometric difference families, partial geometric designs and directed strongly regular graphs.

Theorem 23. *Every (v, k, n, λ) -difference family in a finite group G is a partial geometric difference family with parameters $(v, k, n; k\lambda, (k-1)\lambda + kn)$.*

Proof. Suppose $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ is a (v, k, n, λ) -difference family in G . Then $|S_i| = k$ for all i , and for every non-identity element $x \in G$, $\delta(x) = \lambda$ as we have noted above. Therefore, $\alpha = k\lambda$ and $\beta = (k-1)\lambda + kn$ since $\delta(e) = kn$ for the identity e of G . \square

Let G be a group of order v and let S be a subset of G . For any element $g \in G$, we define the *translate* of S by g as $Sg := \{xg : x \in S\}$. We then define $Dev(S) := [Sg : g \in G]$ to be the collection of all v translates of S . $Dev(S)$ is often called the *development* of S . Similarly, we define the development of a family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of distinct k -element subsets of G to be the vn -multiset

$$Dev(\mathcal{S}) := \bigsqcup_{i=1}^n [S_i g : g \in G].$$

Theorem 24. *Let $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ be a family of distinct k -subsets of a group G of order v . If \mathcal{S} is a partial geometric difference family with parameters $(v, k, n; \alpha, \beta)$, then $(G, Dev(\mathcal{S}))$ is a partial geometric design with parameters $(v, vn, k, kn; \alpha, \beta)$.*

Proof. By construction, $(G, Dev(\mathcal{S}))$ is a tactical configuration with parameters (v, vn, k, kn) . Thus, for any point $x \in G$ and block $B = S_i g \in Dev(\mathcal{S})$, we must show that the set

$$\Phi(x, S_i g) := \{(y, S_j h) : x \in S_j h, y \in S_i g \cap S_j h\}$$

has cardinality β if x belongs to $S_i g$, and α otherwise.

First, consider the case when $B = S_i$. We will show that

$$|\Phi(x, S_i)| = \sum_{z \in S_i} \delta(xz^{-1})$$

by establishing a bijection between $\Phi(x, S_i)$ and the multiset

$$\Delta(x, i) := \bigsqcup_{z \in S_i} \bigsqcup_{j=1}^n [(s_1, s_2) \in S_j \times S_j : s_1 s_2^{-1} = xz^{-1}].$$

First consider $(y, S_j h) \in \Phi(x, S_i)$. Since $x, y \in S_j h$, $x = s_1 h$ and $y = s_2 h$ for some $s_1, s_2 \in S_j$. Also, as $y \in S_i$, we have that $s_1 s_2^{-1} = (s_1 h)(s_2 h)^{-1} = xy^{-1} \in \{xz^{-1} : z \in S_i\}$.

Now consider an ordered pair $(s_1, s_2) \in \Delta(x, i)$. We have that $s_1, s_2 \in S_j$ for some $1 \leq j \leq n$ and $s_1 s_2^{-1} = xy^{-1}$ for some $y \in S_i$. Thus, $x = s_1 s_2^{-1} y \in S_j(s_2^{-1} y)$ and $y = s_2 s_2^{-1} y \in S_j(s_2^{-1} y)$. Therefore, $(y, S_j(s_2^{-1} y)) \in \Phi(x, S_i)$.

Now, by the bijection just established, we have

$$\begin{aligned} |\Phi(x, S_i)| &= |\Delta(x, i)| \\ &= \sum_{z \in S_i} \left(\sum_{j=1}^n |[(s_1, s_2) \in S_j \times S_j : s_1 s_2^{-1} = xz^{-1}]| \right) \\ &= \sum_{z \in S_i} \delta(xz^{-1}) \\ &= \begin{cases} \beta, & \text{if } x \in S_i \\ \alpha, & \text{if } x \notin S_i \end{cases}. \end{aligned}$$

Finally, to complete the proof, we show that $|\Phi(x, S_i g)| = |\Phi(xg^{-1}, S_i)|$ for any $g \in G$. For any $(x, S_i g) \in G \times \text{Dev}(\mathcal{S})$, if $(y, S_j h) \in \Phi(x, S_i g)$, then $xg^{-1} \in S_j h g^{-1}$, $yg^{-1} \in S_j h g^{-1}$ and $yg^{-1} \in S_i$, so $(yg^{-1}, S_j h g^{-1}) \in \Phi(xg^{-1}, S_i)$. Similarly, if $(y, S_j h) \in \Phi(xg^{-1}, S_i)$, then $x \in S_j h g$, $yg \in S_j h g$ and $yg \in S_i g$; and so, $(yg, S_j h g) \in \Phi(x, S_i g)$. \square

Theorem 25. *The partial geometric designs admitting a group of automorphisms which acts regularly on the point set and semi-regularly on the block set are precisely those arising from partial geometric difference families.*

Proof. Let G be a finite group and $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ be a partial geometric difference family of G with parameters $(v, k, n; \alpha, \beta)$. By Theorem 57, $(G, Dev(\mathcal{S}))$ is a partial geometric design with parameters $(v, vn, k, kn; \alpha, \beta)$. Now let $\hat{G} = \{\tau_g : g \in G\}$ be the set of right regular representations of G . Then \hat{G} is a group of automorphisms which acts regularly on the point set G . Furthermore, for any non-identity element $h \in G$ and $S_i g \in Dev(\mathcal{S})$, $\tau_h(S_i g) = (S_i g)h = S_i(gh) = S_i g'$ for some $g' \neq g$ in G . Thus, for $\tau_h \in \hat{G}$, if h is not the identity of G , τ_h moves every block in $Dev(\mathcal{S})$. Therefore, \hat{G} acts semi-regularly on the block set.

Suppose that $\mathcal{T} = (P, \mathcal{B})$ is a partial geometric design with parameters $(v, b, k, r; \alpha, \beta)$ admitting a group of automorphisms G which acts regularly on P and semi-regularly on \mathcal{B} . Then we can identify P with G and the action of G on P as multiplication by each $g \in G$ on the right; and so, each block of \mathcal{T} can be identified as a k -subset of G . Now let $\mathcal{O} = \{O_j : j \in I\}$ where $I = \{1, 2, \dots, n\}$ for some n , be a complete system of representatives for the block orbits of \mathcal{T} under G . Then since G acts semi-regularly on \mathcal{B} , \mathcal{T} is realized as $(G, Dev(\mathcal{O}))$.

We now claim that \mathcal{O} is a partial geometric difference family in G . For any $x \in G$ and $O_i \in \mathcal{O}$, as in the proof of Theorem 57,

$$\sum_{z \in O_i} \delta(xz^{-1}) = |\{(y, O_j h) \in G \times Dev(\mathcal{O}) : y \in O_i \cap O_j h, x \in O_j h\}|$$

and this number depends on whether x belongs to O_i or not. Thus, \mathcal{O} is a partial geometric difference family in G as $\mathcal{T} = (G, Dev(\mathcal{O}))$ is a partial geometric design. \square

By Brouwer-Olmez-Song's results in [12, Theorem 2.1, Theorem 2.2], from a partial geometric design with parameters $(v, b, k, r; \alpha, \beta)$ we can obtain directed strongly regular graphs⁵ whose parameters $(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda, \mu)$ are given by $(b(v - k), r(v - k), kr - \alpha, kr - \beta, kr - \alpha)$ and $(vr, kr - 1, \beta - 1, \beta - 2, \alpha)$. Thus, we have the following:

Corollary 26. *Let $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ be a family of distinct k -subsets of a group G of order v . Suppose that \mathcal{S} is a partial geometric difference family with parameters $(v, k, n; \alpha, \beta)$ and*

⁵A directed strongly regular graph with parameters $(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda, \mu)$ is, by definition, a directed graph on \mathbf{v} vertices without loops such that (i) every vertex has in-degree and out-degree \mathbf{k} , (ii) every vertex x has \mathbf{t} out-neighbors that are also in-neighbors of x , and (iii) the number of directed paths of length 2 from a vertex x to another vertex y is λ if there is an edge from x to y , and is μ if there is no edge from x to y [27].

$(P, \mathcal{B}) = (G, \text{Dev}(\mathcal{S}))$ is the associated partial geometric design with parameters $(v, vn, k, kn; \alpha, \beta)$.

Then

- (i) the directed graph Γ whose vertex set is $V(\Gamma) = \{(p, B) \in P \times \mathcal{B} : p \notin B\}$ and adjacency is defined by $(p, B) \rightarrow (q, C)$ if and only if $p \in C$, is a directed strongly regular graph with parameters

$$(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda, \mu) = (vn(v - k), kn(v - k), k^2n - \alpha, k^2n - \beta, k^2n - \alpha);$$

- (ii) the directed graph Γ' whose vertex set is $V(\Gamma') = \{(p, B) \in P \times \mathcal{B} : p \in B\}$ and adjacency is defined by $(p, B) \rightarrow (q, C)$ if and only if $(p, B) \neq (q, C)$ and $p \in C$, is a directed strongly regular graph with parameters

$$(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda, \mu) = (vkn, k^2n - 1, \beta - 1, \beta - 2, \alpha).$$

Remark 27. It is observed that the dual of a partial geometric design is a partial geometric design.⁶ In this dualization, α and β are preserved, k and r (as well as v and b) are interchanged (cf. [43]); and thus, we do not obtain new parameter sets for directed strongly regular graphs besides what we have already obtained in the above corollary. However, the complement of a partial geometric design is a partial geometric design, and the corresponding directed strongly regular graphs have different parameters.

We also note that the directed strongly regular graphs, Γ and Γ' , obtained above are complement to each other if $v = 2k$ and $\alpha + \beta = k^2n$.

2.4 Some feasibility conditions on parameters

We have the following necessary conditions for the parameters of a partial geometric difference family.

Theorem 28. Let $\mathcal{S} = \{S_i : i \in I\}$ where $I := \{1, 2, \dots, n\}$, be a partial geometric difference family with parameters $(v, k, n; \alpha, \beta)$ in a finite group G , then

$$(v - k)\alpha + k\beta = k^3n.$$

⁶The dual of a design is obtained by interchanging the roles of points and blocks and reversing the point-block incidence.

Proof. Fix $i \in I$, and consider the following N

$$N = \sum_{j=1}^n |S_j \times S_j^{-1} \times S_i| = \sum_{j=1}^n k^3 = nk^3.$$

This number can be also calculated as

$$N = \sum_{g \in G} \left(\sum_{j=1}^n |\{(x, y, z) \in S_j \times S_j \times S_i, xy^{-1}z = g\}| \right).$$

The sum over all g in G may be broken up as the sum over all g in S_i and the sum over all g in $G \setminus S_i$. Since

$$\sum_{j=1}^n |\{(x, y, z) \in S_j \times S_j \times S_i: xy^{-1}z = g\}| = \sum_{z \in S_i} \delta(gz^{-1}) = \begin{cases} \beta & \text{if } g \in S_i \\ \alpha & \text{if } g \notin S_i \end{cases},$$

we have,

$$N = \sum_{g \in S_i} \beta + \sum_{g \notin S_i} \alpha = k\beta + (v - k)\alpha.$$

Finally, we obtain the desired identity by equating the expressions for N . \square

Theorem 29. *Let $\mathcal{S} = \{S_i: i \in I\}$ where $I = \{1, 2, \dots, n\}$, be a family of subsets of a finite group G . If \mathcal{S} is a partial geometric difference family in G with parameters $(v, k, n; \alpha, \beta)$ then $kn(\beta - k)$ is even.*

Proof. Consider the sum

$$\sum_{i=1}^n \sum_{x \in S_i} (\beta - kn - k + 1).$$

On one hand, since $|S_i| = k$ for all $i \in I$, we have that

$$\sum_{i=1}^n \sum_{x \in S_i} (\beta - kn - k + 1) = \sum_{i=1}^n (\beta - kn - k + 1)k = nk(\beta - k) - nk(nk - 1).$$

Alternatively, since \mathcal{S} is a partial geometric difference family, we have that

$$\sum_{i=1}^n \sum_{x \in S_i} (\beta - kn - k + 1) = \sum_{i=1}^n \sum_{x \in S_i} \left(\sum_{r \in S_i \setminus \{x\}} (\delta(xr^{-1}) - 1) \right).$$

Now let d_1, d_2, \dots, d_s be the non-identity distinct differences in the multiset $\bigsqcup_{i \in I} \Delta(S_i)$ and suppose that the difference d_j occurs m_j times in $\bigsqcup_{i \in I} \Delta(S_i)$. Then, the sum on the right-hand side equals to $\sum_{j=1}^s m_j(m_j - 1)$. This completes the proof since each term $m_j(m_j - 1)$ is even. \square

From this theorem, we see that β must be odd if n and k are odd.

2.5 Some families in finite fields

In this section, we find some partial geometric difference families in the additive abelian groups of Galois fields. Thus all our groups and relevant notation will be written additively⁷.

Theorem 30. *Let p be a prime and consider the field $GF(p^2)$. For a fixed primitive element $\gamma \in GF(p^2)$ define the cyclotomic classes of order $p+1$ with respect to $GF(p^2)$ by*

$$C_i = \gamma^i \langle \gamma^{p+1} \rangle \quad \text{for } i = 0, 1, \dots, p.$$

Let $S_i := C_i \cup \{0\}$ for each $i \in \{0, 1, \dots, p\}$, and let I be any n -element subset of $\{0, 1, \dots, p\}$ for $1 \leq n \leq p+1$. Then $\mathcal{S} := \{S_i : i \in I\}$ is a partial geometric difference family in $(GF(p^2), +)$ with parameters $(p^2, p, n; p(n-1), p(p-1) + pn)$. Furthermore, \mathcal{S} is a difference family if and only if $I = \{0, 1, \dots, p\}$.

Proof. We note that $S_0 \cong GF(p)$ and $S_i = \gamma^i S_0$ is a subgroup of $(GF(p^2), +)$ for every $i \in \{0, 1, \dots, p\}$. Now fix $j \in \{0, 1, \dots, p\}$. Since S_j is a subgroup of $(GF(p^2), +)$, for each $z \in GF(p^2)$ the multiplicity $\delta_j(z)$ of z in $\Delta(S_j)$ is

$$\delta_j(z) = \begin{cases} |S_j| = p, & \text{if } z \in S_j \\ 0, & \text{if } z \notin S_j \end{cases}.$$

We also have that

$$x - S_j = \{x - y : y \in S_j\} = S_j \quad \text{for each } x \in S_j.$$

Claim. If $x \notin S_j$, then $|(x - S_j) \cap C_i| = 1$ for every $i \in \{0, 1, \dots, p\} \setminus \{j\}$.

Proof of Claim. First note that $(x - S_j) \cap S_j = \emptyset$ since otherwise $x = z + y$ for some $z, y \in S_j$ yielding $x \in S_j$, which is absurd.

Now suppose that $x - y, x - z \in C_l$ for some distinct $y, z \in S_j$. Then $(x - y) - (x - z) = z - y \in C_l$ since S_l is a subgroup of $(GF(p^2), +)$. It follows that $l = j$ as $z - y \in C_j \cap C_l$. Thus,

⁷As group G is written additively, we adapt $\delta(z) = \sum_{j \in I} \delta_j(z)$ with $\delta_j(z) := |\{(s, t) \in S_j \times S_j : z = s - t\}|$ and use $\delta(x - y)$ instead of $\delta(xy^{-1})$, etc.

$|(x - S_j) \cap C_i| \leq 1$ for all $i \in \{0, 1, \dots, p\} \setminus \{j\}$.

Finally, since $|x - S_j| = |S_j| = \frac{p^2-1}{p+1} + 1 = p$, it must be the case that $|(x - S_j) \cap C_i| = 1$ for all $i \in \{0, 1, \dots, p\} \setminus \{j\}$ as desired; and so the claim follows.

Now let $I \subseteq \{0, 1, \dots, p\}$ and consider $\mathcal{S} = \{S_i : i \in I\}$. Then the multiset union $\bigsqcup_{j \in I} \Delta(S_j)$ contains every element from the set $\bigcup_{j \in I} C_j$ with multiplicity p . Therefore, for $S_k \in \mathcal{S}$ and $x \in GF(p^2)$, if $x \in S_k$, then $x - S_k = S_k$; and so,

$$\beta = \sum_{y \in S_k} \delta(x - y) = \delta(0) + \sum_{y \in S_k \setminus \{x\}} \delta(x - y) = pn + |C_k| \cdot p = pn + p(p - 1).$$

If $x \notin S_k$, $|(x - S_k) \cap C_i| = 1$ for all $i \in \{0, 1, \dots, p\} \setminus \{k\}$, and so

$$\alpha = \sum_{y \in S_k} \delta(x - y) = (n - 1)p.$$

Hence, \mathcal{S} is a partial geometric difference family in $(GF(p^2), +)$ with parameters

$$(p^2, p, n; p(n - 1), p(p - 1) + pn).$$

Lastly, it is clear that the multiset union $\bigsqcup_{j \in I} \Delta(S_j)$ contains every non-zero element of the group λ times if and only if $I = \{0, 1, \dots, p\}$. In this case, $\lambda = p$. This completes the proof. \square

Example 31. Consider $p = 11$ and let ρ be a primitive element of $GF(11^2)$ with characteristic polynomial $x^2 + 7x + 2$. Then $\mathcal{S} = \{S_0, S_1, S_5\}$ is a $(11^2, 11, 3; 22, 143)$ -partial geometric difference family in $GF(11^2)$ where

$$S_0 = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 0\}, \quad S_1 = \{\rho, 2\rho, 4\rho, 8\rho, 5\rho, 10\rho, 9\rho, 7\rho, 3\rho, 6\rho, 0\} \quad \text{and}$$

$$S_5 = \{10\rho + 3, 9\rho + 6, 7\rho + 1, 3\rho + 2, 6\rho + 4, \rho + 8, 2\rho + 5, 4\rho + 10, 8\rho + 9, 5\rho + 7, 0\}.$$

2.6 Some families in cyclic groups

In this section we find many examples of partial geometric difference families in the cyclic group of order $v = dl$ with $d, l \in \mathbb{N}$, by taking a union of certain cosets.

Theorem 32. Consider $G = \mathbb{Z}_v$ where $v = dl$ for some positive integers d and l . Let $H = \langle d \rangle$ be the unique subgroup of G of order l . Then

$$H + i = \{z + i : z \in H\} = \{x \in \mathbb{Z}_v : x \equiv i \pmod{d}\}$$

for $i = 0, 1, \dots, d-1$ are the cosets of H in G . Let

$$S_j := (H + 2j) \cup H, \quad T_j := (H + (2j - 1)) \cup H, \quad U_j := (H + (2j - 1)) \cup (H + \lfloor d/2 \rfloor)$$

for $j = 1, 2, \dots, \lfloor \frac{d}{2} \rfloor$ where $\lfloor d/2 \rfloor$ is the integer part of $d/2$. Then we have the following partial geometric difference families in \mathbb{Z}_v depending on the parity of d .

- (a) If $d \equiv 1 \pmod{2}$, then both $\mathcal{S} := \{S_1, S_2, \dots, S_{(d-1)/2}\}$ and $\mathcal{T} := \{T_1, T_2, \dots, T_{(d-1)/2}\}$ are partial geometric difference families with parameters $(dl, 2l, (d-1)/2; 2l^2, dl^2)$.
- (b) If $d \equiv 0 \pmod{2}$, then $\mathcal{T} := \{T_1, T_2, \dots, T_{d/2}\}$ is a partial geometric difference family with parameters $(dl, 2l, d/2; 2l^2, (d+2)l^2)$.
- (c) If $d \equiv 0 \pmod{4}$, then $\mathcal{U} := \{U_1, U_2, \dots, U_{d/2}\}$ is a partial geometric difference family in \mathbb{Z}_v with parameters $(dl, 2l, d/2; 2l^2, (d+2)l^2)$.

Proof. We will prove the case for \mathcal{S} in Part (a) by assuming that $d = 2h - 1$. The other cases can be proved in the same manner.

First note that, for each $i = 1, 2, \dots, h-1$, the multiset $\Delta(S_i)$ consists of all elements of H with multiplicity $2l$ and all elements of $H + 2i$ and $H + (d - 2i)$ with multiplicity l . Therefore, the multiset union $\bigsqcup_{i=1}^{h-1} \Delta(S_i)$ consists of all elements of H with multiplicity $2l(h-1)$ and all other elements of \mathbb{Z}_v with multiplicity l .

Let $x \in \mathbb{Z}_v$ and $S_i \in \mathcal{S}$ be given. If $x \in S_i = H \cup (H + 2i)$, then we have

$$\begin{aligned} \beta &= \sum_{y \in S_i} \delta(x - y) \\ &= \begin{cases} \sum_{z \in H} \delta(z) + \sum_{z \in H + (d-2i)} \delta(z) & \text{if } x \in H \\ \sum_{z \in H} \delta(z) + \sum_{z \in (H+2i)} \delta(z) & \text{if } x \in H + 2i \end{cases} \\ &= (2h-1)l^2. \end{aligned}$$

The last equality follows from the above note which asserts that

$$\delta(z) = \begin{cases} 2l(h-1) & \text{if } z \in H \\ l & \text{if } z \in \mathbb{Z}_v \setminus H. \end{cases}$$

If $x \notin S_i$, then $x \in H + j$ for some $j \in \{0, 1, \dots, d-1\} \setminus \{0, 2i\}$; and so

$$\alpha = \sum_{y \in S_i} \delta(x - y) = \sum_{z \in H+j} \delta(z) + \sum_{z \in H+(j-2i)} \delta(z) = 2l^2.$$

Thus, \mathcal{S} is a partial geometric difference family in \mathbb{Z}_v with parameters $(v, 2l, h-1; 2l^2, dl^2)$ as desired. \square

Corollary 33. *Let $v = 4l$ for some positive integer l and let H be the unique subgroup of order l in \mathbb{Z}_v . Then both $\mathcal{T} = \{H \cup (H+1), H \cup (H+3)\}$ and $\mathcal{U} = \{(H+2) \cup (H+1), (H+2) \cup (H+3)\}$ are partial geometric difference families in \mathbb{Z}_v with parameters $(4l, 2l, 2; 2l^2, 6l^2)$.*

2.7 Some families in \mathbb{Z}_v with $v = 2^u$

We find some examples of partial geometric difference families in the Galois rings \mathbb{Z}_v for prime power v . We consider the case when $v = 2^u$ here and the odd prime power case in the following section.

Theorem 34. *Let $v = 2^u$ with $u > 2$ and let S be a subset of \mathbb{Z}_v such that $|S \cap \{i, \frac{v}{2} + i\}| = 1$ for every $i \in \{0, 1, \dots, \frac{v}{2} - 1\}$. If $\delta_S(x) = \frac{v}{4}$ for each $x \in \{m \in \mathbb{Z}_v : m \text{ is even, } m < \frac{v}{4}\}$, where $\delta_S(x)$ is the multiplicity of x in $\Delta(S)$, then $\mathcal{S} = \{S, (\frac{v}{2} - 1)S\}$ is a partial geometric difference family in \mathbb{Z}_v with parameters*

$$(2^u, 2^{u-1}, 2; (2^{u-1} - 1)2^{u-1}, (2^{u-1} + 1)2^{u-1}).$$

Proof. Let a denote $\frac{v}{2} - 1$. Then $a^2 = (2^{u-1} - 1)^2 \equiv 1 \pmod{v}$. Thus, $a(ag) = g$ for all $g \in \mathbb{Z}_v$. Hence, the multiplicity of x in $\Delta(aS)$ is equal to that of ax in $\Delta(S)$, so $\delta(x) = \delta_S(x) + \delta_S(ax)$ for all $x \in \mathbb{Z}_v$. Further, it is clear from the definition of δ_S that $\delta_S(x) = \delta_S(-x)$ for any $x \in \mathbb{Z}_v$.

Now, it is easy to verify that, for $x \in \mathbb{Z}_v$,

$$ax = \begin{cases} -x & \text{if } x \text{ is even;} \\ \frac{v}{2} - x & \text{if } x \text{ is odd.} \end{cases}$$

For $x = \frac{v}{2}$, since $|S \cap \{i, \frac{v}{2} + i\}| = 1$ for every $i \in \{0, 1, \dots, \frac{v}{2} - 1\}$, $\delta(\frac{v}{2}) = \delta_S(\frac{v}{2}) + \delta_S(-\frac{v}{2}) = 0$. For $x \not\equiv 0 \pmod{\frac{v}{2}}$, we prove the following identity which will be useful in calculating $\delta(x)$.

Claim: For any $x \in \mathbb{Z}_v \setminus \{0, \frac{v}{2}\}$,

$$\delta_S(x) + \delta_S\left(\frac{v}{2} - x\right) = \frac{v}{2}.$$

Proof of the claim. Fix $x \in \mathbb{Z}_v \setminus \{0, \frac{v}{2}\}$. For each $s \in S$, we know that there exists a unique $r \in \mathbb{Z}_v$ such that $s - r = x$. (i) If $r \in S$, then $\frac{v}{2} + r \notin S$; and so, there is no element $y \in S$ such that $y - s = \frac{v}{2} - x$ since $y - s = \frac{v}{2} - x$ if and only if $y = \frac{v}{2} + r$. Thus, $\delta_S(\frac{v}{2} - x) \leq |S| - \delta_S(x)$, or equivalently, $\delta_S(x) + \delta_S(\frac{v}{2} - x) \leq |S|$. (ii) On the other hand, if $r \notin S$, then $\frac{v}{2} + r \in S$ and $(\frac{v}{2} + r) - s = \frac{v}{2} - (s - r) = \frac{v}{2} - x$. Thus, $\delta_S(\frac{v}{2} - x) \geq |S| - \delta_S(x)$, or equivalently, $\delta_S(x) + \delta_S(\frac{v}{2} - x) \geq |S|$. Lastly, combining the inequalities obtained in (i) and (ii), we have the identity in the claim.

As an immediate consequence of this claim, we have, for any odd $x \in \mathbb{Z}_v$,

$$\delta(x) = \delta_S(x) + \delta_S(ax) = \delta_S(x) + \delta_S\left(\frac{v}{2} - x\right) = \frac{v}{2}.$$

Now since $\delta_S(x) = \frac{v}{4}$ for any even $x < \frac{v}{4}$, by the above identity, $\delta_S(x) = \frac{v}{4}$ for any even $x < \frac{v}{2}$. Moreover, since $\delta_S(x) = \delta_S(-x)$, we have that $\delta_S(x) = \frac{v}{4}$ for every even $x \in \mathbb{Z}_v \setminus \{0, \frac{v}{2}\}$. Thus, for any even $x \in \mathbb{Z}_v \setminus \{0, \frac{v}{2}\}$,

$$\delta(x) = \delta_S(x) + \delta_S(ax) = \delta_S(x) + \delta_S(-x) = \frac{v}{4} + \frac{v}{4} = \frac{v}{2}.$$

We are now ready to compute α and β . Let $x \in \mathbb{Z}_v$.

$$\beta = \begin{cases} \sum_{y \in S} \delta(x - y) = \delta(0) + \sum_{y \in S \setminus \{x\}} \frac{v}{2} = v + \frac{v}{2} \left(\frac{v}{2} - 1\right) & \text{if } x \in S, \\ \sum_{y \in aS} \delta(x - y) = \delta(0) + \sum_{y \in aS \setminus \{x\}} \frac{v}{2} = v + \frac{v}{2} \left(\frac{v}{2} - 1\right) & \text{if } x \in aS; \end{cases}$$

$$\alpha = \begin{cases} \sum_{y \in S} \delta(x - y) = \sum_{y \in S \setminus \{\frac{v}{2} + x\}} \frac{v}{2} = \frac{v}{2} \left(\frac{v}{2} - 1\right) & \text{if } x \notin S, \\ \sum_{y \in aS} \delta(x - y) = \sum_{y \in aS \setminus \{\frac{v}{2} + x\}} \delta(x - y) = \frac{v}{2} \left(\frac{v}{2} - 1\right) & \text{if } x \notin aS. \end{cases}$$

We note that in the above calculation, we used the facts that $\delta(0) = v$, $\delta(\frac{v}{2}) = 0$ and $\frac{v}{2} + x$ belongs to S and aS when x does not. Therefore, $\{S, aS\}$ is a partial geometric difference family in \mathbb{Z}_v for $v = 2^u$. \square

Example 35. In \mathbb{Z}_8 , $\mathcal{S} = \{\{0, 1, 2, 7\}, \{0, 3, 5, 6\}\}$ is a partial geometric difference family with parameters $(8, 4, 2; 12, 20)$.

Example 36. In \mathbb{Z}_{16} , $\mathcal{S} = \{\{0, 1, 2, 3, 4, 6, 7, 13\}, \{0, 7, 14, 5, 12, 10, 1, 11\}\}$ is a partial geometric difference family with parameters $(16, 8, 2; 56, 72)$.

Theorem 37. Let $v = 2^u$ with $u > 2$ and let $S = \{0, 1, 2, 3\} \subset \mathbb{Z}_v$. Then

$$\mathcal{S} = \{(2l - 1)S : l = 1, 2, \dots, v/4\}$$

is a partial geometric difference family in \mathbb{Z}_v with parameters $(2^u, 4, 2^{u-2}; 12, 2^u + 12)$.

Proof. For the simplicity, let $S_l = (2l - 1)S = \{0, 2l - 1, 4l - 2, 6l - 3\}$ for $l = 0, 1, \dots, v/4$. Then

$$\Delta(S_l) = [0, 0, 0, 0, \pm(2l - 1), \pm(2l - 1), \pm(2l - 1), \pm(4l - 2), \pm(4l - 2), \pm(6l - 3)].$$

Thus, we see that the multiset $\bigsqcup_{l=1}^{v/4} \Delta(S_l)$ contains the elements of \mathbb{Z}_v with the multiplicities as in the following table for every $l \in \{0, 1, \dots, v/4\}$:

x	$\pm(2l - 1)$	$\pm 2(2l - 1)$	$\pm 3(2l - 1)$
$\delta(x)$	3	2	1

That is, $\delta(x) = 4$ for every element x in $\{m \in \mathbb{Z}_v : x \not\equiv 0 \pmod{4}\}$ and $\delta(0) = v$.

We note that for every $l = 1, 2, \dots, v/4$, if we reduce the elements of S_l modulo 4, then the residues are precisely the elements of $S = \{0, 1, 2, 3\}$. It follows that for any S_l and any $x \notin S_l$, the set $x - S_l := \{x - y : y \in S_l\}$ contains exactly one element congruent to 0 modulo 4. Therefore, for any $x \in \mathbb{Z}_v$ and any $S_l \in \mathcal{S}$, we have the following.

If $x \in S_l$, then

$$\beta = \sum_{y \in S_l} \delta(x - y) = v + 12.$$

If $x \notin S_l$, then

$$\alpha = \sum_{y \in S_l} \delta(x - y) = \sum_{y \in S_l, x-y \not\equiv 0 \pmod{4}} 4 = 12.$$

Thus, \mathcal{S} is a $(2^u, 4, 2^{u-2}; 12, 2^u + 12)$ -partial geometric difference family in \mathbb{Z}_v . \square

2.8 Some families in \mathbb{Z}_v with v an odd prime power

The following elementary number theoretic facts will be used in the construction of our next example of partial geometric difference families.

Lemma 38. *Let p be an odd prime and let u be a positive integer.*

(a) *If a is an integer with the property that $p^u \mid a - 1$ but $p^{u+1} \nmid a - 1$, then $p^{u+1} \mid a^p - 1$ but $p^{u+2} \nmid a^p - 1$.*

(b) *The element $p + 1$ has order p^{u-1} modulo p^u .*

Proof. It is easy to verify (a), and we omit the proof.

For (b), if $u = 1$, it is obvious. If we set $a = p + 1$, $a - 1$ is divisible by p but not p^2 . Thus by Part (a), $a^p - 1 = (p + 1)^p - 1$ is divisible by p^2 but not p^3 . But then, by (a) again, we have that $a^{p^2} - 1 = (p + 1)^{p^2} - 1$ is divisible by p^3 but not p^4 . Applying Part (a) recursively, we eventually have that $(p + 1)^{p^{u-1}} - 1$ is divisible by p^u but not p^{u+1} . Since $(p + 1)^{p^{u-1}} \equiv 1 \pmod{p^u}$, we have that the order of $p + 1$ divides p^{u-1} . However, if the order were less than p^{u-1} , it would divide p^{u-2} implying that p^u must divide $(p + 1)^{p^{u-2}} - 1$, which is a contradiction. Thus, the order of $a = p + 1$ is p^{u-1} modulo p^u . \square

Theorem 39. *Let $v = p^u$ for some odd prime p and $u \geq 2$. Let $S = \{0, 1, \dots, p - 1\}$ and let $S_i = (p + 1)^i S$ then $\mathcal{S} = \{S_i : i = 0, 1, \dots, p^{u-1} - 1\}$ is a partial geometric difference family in the ring \mathbb{Z}_v with parameters $(p^u, p, p^{u-1}; p(p - 1), p^u + p(p - 1))$.*

Proof. First note that since $S = \{0, 1, \dots, p - 1\}$, the multiset $\Delta(S)$ contains the elements $\pm 1, \pm 2, \dots, \pm(p - 1)$ with multiplicities $p - 1, p - 2, \dots, 1$, respectively. If we describe this multiset by

$$\begin{aligned} \Delta(S) &= p\underline{0} + (p - 1)\{\underline{\pm 1}\} + \cdots + 2\{\underline{\pm(p - 2)}\} + 1\{\underline{\pm(p - 1)}\} \\ &= \sum_{i=0}^{p-1} (p - i)\{\underline{\pm i}\} \end{aligned}$$

adopting the same notation, we can express the multiset $\sum_{i=0}^{p^{u-1}-1} \Delta(S_i)$ by

$$\begin{aligned}
\sum_{i=0}^{p^{u-1}-1} \Delta(S_i) &= \sum_{i=0}^{p^{u-1}-1} (p+1)^i \Delta(S) \\
&= \sum_{i=0}^{p^{u-1}-1} \sum_{j=1}^{p-1} (p-j)(p+1)^i \{\pm j\} \\
&= p^u \underline{0} + \sum_{j=1}^{p-1} (p-j) \left(\sum_{i=0}^{p^{u-1}-1} \frac{j(p+1)^i}{j(p+1)^i} + \sum_{i=0}^{p^{u-1}-1} \frac{-j(p+1)^i}{-j(p+1)^i} \right).
\end{aligned}$$

Here we note that by Lemma 38, $\{(p+1)^i : i = 0, 1, \dots, p^{u-1}-1\} = \langle p+1 \rangle$ is the multiplicative subgroup generated by $p+1$ in the ring \mathbb{Z}_v . We see that $\langle p+1 \rangle = \{x \in \mathbb{Z}_v : x \equiv 1 \pmod{p}\}$ with $|\langle p+1 \rangle| = p^{u-1}$. We also notice that $j\langle p+1 \rangle = \{x \in \mathbb{Z}_v : x \equiv j \pmod{p}\}$ for all $j = 1, 2, \dots, p-1$. Therefore, $\{\langle p+1 \rangle, 2\langle p+1 \rangle, \dots, (p-1)\langle p+1 \rangle\}$ are the cosets of $\langle p+1 \rangle$ in \mathbb{Z}_v^\times . Further, $-j\langle p+1 \rangle = (p-j)\langle p+1 \rangle$. Thus, the multiset $\sum_{i=0}^{p^{u-1}-1} \Delta(S_i)$ contains all the elements of $\{x \in \mathbb{Z}_v : x \not\equiv 0 \pmod{p}\}$ with multiplicity p .

For the constants α and β for this family, we need the following observation. Recall that $(p+1)^j \equiv 1 \pmod{p}$ for all $j = 0, 1, \dots, p^{u-1}-1$. Thus the complete set of residues modulo p for the set S_j is $S = \{0, 1, \dots, p-1\}$ for all $j = 0, 1, \dots, p^{u-1}-1$. It follows that for any $S_j \in \mathcal{S}$ and $x \notin S_j$, the set $x - S_j$ contains exactly one element congruent to 0 modulo p .

Now let $x \in \mathbb{Z}_v$ and $S_j = (p+1)^j S \in \mathcal{S}$ be given. If $x \in S_j$, then we have

$$\beta = \sum_{y \in S_j} \delta(x-y) = p^u + p(p-1).$$

If $x \notin S_j$, then

$$\sum_{y \in S_j} \delta(x-y) = \sum_{y \in S_j, x-y \not\equiv 0 \pmod{p}} p = p(p-1).$$

Therefore, \mathcal{S} is a $(p^u, p, p^{u-1}; p(p-1), p^u + p(p-1))$ -partial geometric difference family. \square

2.9 Concluding remarks

In this paper, we introduced partial geometric difference families and studied their existence as well as different construction methods. We established a link between these families and

a class of partial geometric designs as well as classical difference families. Concerning the existence of partial geometric difference families, we established some results in cyclic groups and finite fields.

2.9.1 Partial geometric difference families and the obtained directed strongly regular graphs

In Section 5, we showed that there are partial geometric difference families in $(GF(p^2), +)$ with parameters $(v, k, n; \alpha, \beta) = (p^2, p, n; p(n-1), p(p-1) + pn)$ as described in Theorem 30. In Sections 6 – 8, we found partial geometric difference families with the following parameters:

$$\begin{aligned} &(dl, 2l, (d-1)/2; 2l^2, dl^2), \quad \text{for positive integers } d \text{ and } l \text{ with } d \equiv 1 \pmod{2}, \\ &(dl, 2l, d/2; 2l^2, (d+2)l^2), \quad d \equiv 0 \pmod{2} \quad (\text{cf. Theorem 32}); \\ &(2^{u+2}, 2^{u+1}, 2; 2^{u+1}(2^{u+1}-1), 2^{u+1}(2^{u+1}+1)), \quad \text{for } u \geq 1 \text{ (cf. Theorem 34)}; \\ &(2^{u+2}, 4, 2^u; 12, 2^{u+2} + 12), \quad \text{for } u \geq 1 \text{ (cf. Theorem 37)}; \\ &(p^u, p, p^{u-1}; p(p-1), p^u + p(p-1)), \quad \text{for an odd prime } p \text{ (cf. Theorem 39)}. \end{aligned}$$

In Corollary 26, we saw that a directed strongly regular graph can be obtained using the set of antiflags or the set of flags of the partial geometric design associated with a partial geometric difference family with parameters $(v, k, n; \alpha, \beta)$. The parameters $(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda, \mu)$ of the directed strongly regular graphs obtained in this way are respectively given by

$$(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda, \mu) = \begin{cases} (vn(v-k), kn(v-k), k^2n - \alpha, k^2n - \beta, k^2n - \alpha); \\ (vkn, k^2n - 1, \beta - 1, \beta - 2, \alpha). \end{cases}$$

Therefore, from the partial geometric difference families constructed in Sections 5 through 8, we obtain infinite families of directed strongly regular graphs. The parameters of these families are listed in Table 1.⁸ Using our construction method, we were able to confirm some known DSRGs with small parameters, for instance, with $e = 4, l = 2$ we have DSRG(64, 32, 24, 8, 24) and (64, 31, 23, 22, 8); with $u = 2$ or $u = 1$ from the rows corresponding to Theorem 34 or 37, we have DSRG(64, 32, 20, 12, 20) and (64, 31, 19, 18, 12), all of which were constructed by A. Duval [27] employing construction methods T10 and T11 listed in the Brouwer and Hobart's

⁸The last column of Table 1 refers to the theorems on partial geometric difference families which give the corresponding DSRGs.

list of DSRGs with \mathbf{v} up to 110 in [11]. Many of these were also constructed by Olmez and Song [47] in different contexts.

Table 2.1 Parameters of DSRGs obtained from PGDFs

(Here n, l, u, d, e are positive integers, $d \geq 3$ odd, $e > 2$ even, p a prime and q odd prime.)

\mathbf{v}	\mathbf{k}	\mathbf{t}	λ	μ	Note (Th.#)
$p^3(p-1)n$ p^3n	$p^2(p-1)n$ p^2n-1	$p(pn-n+1)$ $pn+p^2-p-1$	$p(p-1)(n-1)$ $pn+p^2-p-2$	$p(pn-n+1)$ $p(n-1)$	30
$\frac{1}{2}d(d-1)(d-2)l^2$ $d(d-1)l^2$	$(d-1)(d-2)l^2$ $2(d-1)l^2-1$	$2(d-2)l^2$ dl^2-1	$(d-2)l^2$ dl^2-2	$2(d-2)l^2$ $2l^2$	32(a)
$\frac{1}{2}e^2(e-2)l^2$ e^2l^2	$e(e-2)l^2$ $2el^2-1$	$2(e-1)l^2$ $(e+2)l^2-1$	$(e-2)l^2$ $(e+2)l^2-2$	$2(e-1)l^2$ $2l^2$	32(b, c)
2^{2u+2} 2^{2u+2}	2^{2u+1} $2^{2u+1}-1$	$2^{2u}+2^u$ $2^{2u}+2^u-1$	$2^{2u}-2^u$ $2^{2u}+2^u-2$	$2^{2u}+2^u$ $2^{2u}-2^u$	34
$2^{2u+4}(2^u-1)$ 2^{2u+4}	$2^{u+4}(2^u-1)$ $2^{u+4}-1$	$2^{u+4}-12$ $2^{u+2}+11$	$3 \cdot 2^{u+2}-12$ $2^{u+2}+10$	$2^{u+4}-12$ 12	37
$q^{2u-1}(q^u-q)$ q^{2u}	$q^u(q^u-q)$ $q^{u+1}-1$	$q^{u+1}-q^2+q$ q^u+q^2-q-1	$(q-1)(q^u-q)$ q^u+q^2-q-2	$q^{u+1}-q^2+q$ q^2-q	39

2.9.2 Overlap with partial difference sets, almost difference sets, and almost difference families

Several other variations on the classical difference set have been introduced. Here we discuss the overlap between partial geometric difference sets (families) and three other widely studied variations, namely, partial difference sets, almost difference sets, and almost difference families. Partial difference sets have meaningful links to other areas of mathematics, such as, partial geometries, strongly regular Cayley graphs, Schur rings and two-weight codes, while almost difference sets have a wide range of applications in many areas of engineering including cryptography, coding theory, and CDMA communications. We briefly recall their definitions before making our comparison.

Let G be a group of order v . A k -element subset D is called a (v, k, λ, μ) -*partial difference set* if the multiplicity function $\delta_D(x)$ takes on the value λ for each non-identity $x \in D$ and takes on the value μ for each non-identity $x \in G \setminus D$. On the other hand, D is called a (v, k, λ, t) -*almost difference set* if the multiplicity function $\delta_D(x)$ takes on the value λ altogether t times and

$\lambda + 1$ altogether $v - t - 1$ times as x ranges over all non-identity elements of G ; in other words, the multiset ΔD contains t non-identity elements of G with multiplicity λ and the remaining non-identity elements with multiplicity $\lambda + 1$.⁹

Observe that a partial difference set with $\lambda = \mu$ is nothing but a (v, k, λ) -difference set. Similarly, any almost difference set with $t = 0$ (or $t = v - 1$) is an (v, k, λ) -difference set. Although partial difference sets and almost difference sets capture two very different ideas, there is overlap in certain cases. Explicitly, any partial difference set with $|\lambda - \mu| = 1$ is an almost difference set. For the abelian case, S. Ma [41] characterized partial difference sets that are also almost difference sets in the following theorem.

Theorem 40. [41] *Let G be an abelian group of order v written additively. Suppose a k -subset D of $G \setminus \{0\}$ is (v, k, λ, μ) partial difference set with $\mu = \lambda + 1$. Then up to complementation, either $(v, k, \lambda, \mu) = (v, (v - 1)/2, (v - 5)/4, (v - 1)/4)$ where $v \equiv 1 \pmod{4}$, or $(v, k, \lambda, \mu) = (243, 22, 1, 2)$.*

Given a group G and a non-empty subset S of G , in the group ring $\mathbb{Z}G$, the element $\underline{S} := \sum_{s \in S} s$ is often called a simple quantity. Let e be the identity element of G . Let \underline{e} denote $\{e\}$, and define $\underline{S}^{-1} := \{s^{-1} \mid s \in S\}$. Next, we recall the following group ring characterization for almost difference sets and partial geometric difference sets in order to see their relation.

Lemma 41. [2] *Let G be an additive abelian group of order v and let S be a k -subset of G . Then S is a (v, k, λ, t) -almost difference set in G if and only if there exists a t -subset D of G such that $\underline{S} \cdot \underline{S}^{-1} = k\underline{e} + \lambda\underline{D} + (\lambda + 1)(\underline{G} - \underline{D})$ in the group ring $\mathbb{Z}G$.*

Lemma 42. [46] *Let G be a group of order v and let S be a k -subset of G . Then S is a partial geometric difference set with parameters $(v, k; \alpha, \beta)$ if and only if in the group ring $\mathbb{Z}G$, $\underline{S} \cdot \underline{S}^{-1} \cdot \underline{S} = n\underline{S} + \alpha\underline{G}$ where $n = \beta - \alpha$.*

⁹Different definitions of an almost difference set were independently developed by J. Davis and C. Ding in the early 1990s. For an additive group G with subgroup H , we call a k -subset $D \subset G$ a $(|G|, |H|, k, \lambda_1, \lambda_2)$ -divisible difference set if the multiplicity function $\delta_D(x)$ defined additively takes on the value λ for each nonzero $x \in H$ and takes on the value μ for each nonzero $x \in G \setminus H$. Davis [20] called a divisible difference set an almost difference set in the case where $|\lambda - \mu| = 1$. The two notions were generalized to the current definition by Ding, Helleseth, and Martinsen [24].

Comparing these two characterizations we have the following:

Lemma 43. *Let S be a (v, k, λ, t) -almost difference set in the group G and let D denote the t -set of elements which appear λ times as differences of S . Then S is a partial geometric difference set if and only if there exist nonnegative integers γ_1 and γ_2 such that $\underline{D \cdot S} = \gamma_1 \underline{S} + \gamma_2 \underline{G}$ in the group ring $\mathbb{Z}G$.*

Proof. Since S is an almost difference set, by Lemma 41,

$$\underline{S \cdot S^{-1}} = k\underline{e} + (\lambda + 1)\underline{G} - \underline{D}$$

in the group ring $\mathbb{Z}G$. Thus,

$$\begin{aligned} \underline{S \cdot S^{-1} \cdot S} &= \{k\underline{e} + (\lambda + 1)\underline{G} - \underline{D}\} \cdot \underline{S} \\ &= k\underline{S} + k(\lambda + 1)\underline{G} - \underline{D \cdot S}. \end{aligned}$$

The result now follows by comparing this equation with that of Lemma 42. \square

As a generalization of almost difference sets, C. Ding and J. Yin studied almost difference families in [26]. Let G be a group of order v . A family $\mathcal{F} = \{D_1, D_2, \dots, D_s\}$ of k -element subsets of G is called an *almost difference family* with parameters (v, k, λ, t) if some t nonzero elements of G occur exactly λ times in $\Delta(\mathcal{F})$ while the remaining $v - 1 - t$ nonzero elements of G each occur exactly $\lambda + 1$ times in $\Delta(\mathcal{F})$.

By the above characterization, we find that in most cases almost difference sets and partial geometric difference sets are not comparable. Similar analysis also shows almost difference families and partial geometric difference families to be incomparable in general.

Similar to almost difference sets, we have the following group ring characterization for partial difference sets.

Lemma 44. [41] *Let S be a k -subset of a group G of order v . Then S is a (v, k, λ, μ) -partial difference set in G if and only if in the group ring $\mathbb{Z}G$,*

$$\underline{S \cdot S^{-1}} = \mu \underline{G} - \underline{S} + \lambda \underline{S} + \gamma \underline{e}$$

where $\gamma = k - \mu$ if $e \notin S$ and $\gamma = k - \lambda$ if $e \in S$.

Combining this characterization with that for partial geometric difference sets, we have:

Lemma 45. *Let S be (v, k, λ, μ) -partial difference set, $\lambda \neq \mu$, in a group G . Then S is a partial geometric difference set if and only if $S = S^{-1}$, $e \notin S$ and $k = \mu$. (In this case, the partial geometric difference set has parameters $(v, \mu; (\lambda - \mu)^2, (\lambda - \mu)^2 + (\lambda - 2)\mu + 1)$.)*

Proof. First since $\lambda \neq \mu$, we have that S is reversible [40]. That is, $S^{-1} = S$. Next, since S is a partial difference set, by Lemma 44, in the group ring $\mathbb{Z}G$,

$$\underline{S} \cdot \underline{S}^{-1} = \mu \underline{G} + (\lambda - \mu) \underline{S} + \gamma \underline{e}$$

where $\gamma = k - \mu$ if $e \notin S$ and $\gamma = k - \lambda$ if $e \in S$. Thus,

$$\begin{aligned} \underline{S} \cdot \underline{S}^{-1} \cdot \underline{S} &= \{\mu \underline{G} + (\lambda - \mu) \underline{S} + \gamma \underline{e}\} \cdot \underline{S} \\ &= \mu k \underline{G} + (\lambda - \mu) \underline{S} \cdot \underline{S} + \gamma \underline{S} \\ &= \mu k \underline{G} + (\lambda - \mu) \{\mu \underline{G} + (\lambda - \mu) \underline{S} + \gamma \underline{e}\} + \gamma \underline{S}. \end{aligned}$$

Comparing this with the equation in Lemma 42, we see that S is a partial geometric difference set exactly when $\gamma = 0$. Now if $e \in S$, then from the necessary condition for partial difference sets, we have

$$\begin{aligned} k(k-1) &= \lambda k + \mu(v-1-k) \\ k^2 - k &= k^2 + \mu(v-1-k) \\ -k &= \mu(v-1-k) \end{aligned}$$

which is a contradiction. Thus, it must be the case that $e \notin S$ and $k = \mu$. In this case, S is a $(v, \mu; (\lambda - \mu)^2, (\lambda - \mu)^2 + (\lambda - 2)\mu + 1)$ -partial geometric difference set. \square

Finally, we would like to mention that this work makes a meaningful contribution by introducing and studying the existence problem of partial geometric difference families, a combinatorial structure related to difference families, partial geometric designs and directed strongly regular graphs. In Section 3.4, we discussed some parametric conditions concerning the existence of a partial geometric difference family. However, we did not make use of these conditions

in this work. In Sections 3.5 through 2.8, we gave many examples, but there are still many other interesting and important examples that have yet to be described. In the last section, we briefly discussed their links to partial and almost difference sets and families. We definitely believe that the current work serves to make abundantly clear that more research on this subject is required as the notion of a partial geometric difference family has been introduced here for the first time.

CHAPTER 3. PARTIAL GEOMETRIC DESIGNS WITH PRESCRIBED AUTOMORPHISMS

A paper submitted to *Designs, Codes, and Cryptography*

Kathleen Nowak and Oktay Olmez

Abstract

We generalize the well-known Kramer-Mesner theorem for $2 - (v, k, \lambda)$ designs to partial geometric designs. We also construct infinite families of partial geometric designs admitting a group of automorphisms which acts regularly on the point set and semi-regularly on the block set.

3.1 Introduction

In recent years, combinatorial designs have garnered a lot of attention. People are drawn not only to the rich mathematical heritage of combinatorial design theory but also to the genuine solutions they provide to problems coming from signal processing, radar, error-correcting codes, optical orthogonal codes, and image processing [1, 17, 59].

Designs with prescribed automorphisms are of interest since these designs provide the elegant solutions desired for applications. For example, binary sequences with ideal autocorrelation functions have applications in signal processing, radar, and audio coding [19, 32, 36]. A binary sequence with two-level(optimal) autocorrelation is equivalent to a 2-design obtained by taking the development of a difference set [34]. This method generates designs with an automorphism group which acts transitively on both the point set and the block set. Further, optical orthogonal codes are used in frequency-hopping spread-spectrum communications, radar,

sonar, collision channels without feedback, and neuromorphic networks ([17], [30], [42], [48], [49]). Optical orthogonal codes can be obtained from relative difference families ([14], [60]). In [13], it was shown that the divisible designs admitting a group of automorphisms acting regularly on the point set and semi-regularly on the block set are precisely those arising from relative difference families.

The study of automorphisms of a design provides links between algebra, geometry, and combinatorial design theory and it deserves special attention. Designs with specified automorphisms can supply valuable information for proving general existence and non-existence results. For instance, a cyclic 5-design with parameters $(13, 6, 4)$ was constructed by considering its specified automorphisms [38]. Another example is the nonexistence of a 3-design with parameters $(112, 12, 1)$ which is fixed by the Frobenius group of order 56 [51]. The existence of this design is known to be closely related to the existence of a projective plane of order 10.

In this paper, we focus on a certain family of designs known as partial geometric designs (also called ‘ $1\frac{1}{2}$ -designs’). Examples of partial geometric designs include 2-designs, transversal designs, and partial geometries. Recently, Brouwer, the second author, and Song, showed how to construct two directed strongly regular graphs from a given partial geometric design [12]. One is defined on the set of flags of the design and the other is defined on the set of antiflags. Here we describe a method that can often be used to determine the existence or nonexistence of a $(v, k; \alpha, \beta)$ -partial geometric design having specified automorphisms. Our technique can be viewed as a generalization of the well-known Kramer-Mesner theorem (This theorem can be found in [37]). We also provide some new constructions of partial geometric difference families. The equivalence between partial geometric difference families and partial geometric designs admitting a group of automorphisms which acts regularly on the point set and semi-regularly on the block set was established in [44].

The organization of the paper is as follows. In the following section, we introduce our central objects of study and recall some notation and basic terminology from combinatorial design theory. In Section 3.3, we discuss our method for constructing partial geometric designs with specified automorphisms and provide some examples. In Section 3.4, we then present new constructions of partial geometric difference families. Finally, in Section 3.5 we summarize

the parameters of the partial geometric designs obtained from the partial geometric difference families prescribed in Section 3.4. We also highlight the parameters of the directed strongly regular graphs which result from these designs.

3.2 Preliminaries

A (*block*) *design* is a pair (P, \mathcal{B}) consisting of a finite set P of points and a finite collection \mathcal{B} of nonempty subsets of P called blocks. A design is said to be a *simple design* if it does not contain repeated blocks. A point-block pair (x, B) is called a *flag* if $x \in B$; otherwise, it is called an *antiflag*. Designs are usually classified by their nice combinatorial and algebraic properties. For instance, a block design where “each block has the same size” and “each point occurs in exactly the same number of blocks” is known as a 1-design. More formally, a block design (P, \mathcal{B}) is called a 1-design with parameters (v, b, k, r) if $|P| = v$ and $|\mathcal{B}| = b$ such that each block consists of k points and each point belongs to r blocks. Further, a 1-design is said to be symmetric if $v = b$. It is often convenient to represent a 1-design with an incidence matrix. A point-block incidence matrix N of a 1-design with parameters (v, b, k, r) is a $v \times b$ $\{0, 1\}$ -matrix such that the entry in row i and column j is 1 if the i -th point is incident to the j -th block. Notice that a 1-design N satisfies the equations:

$$NJ = rJ \quad \text{and} \quad JN = kJ \tag{3.1}$$

where J denotes the all-ones matrix. One can classify 1-designs by studying the eigenvalues of the matrix $C = NN^t$ (N^t denotes the transpose of N). The matrix C is called the concurrence matrix of the design. For example, 2-designs are well-studied examples of 1-designs where C has two distinct singular values [55]. A 2-design with parameters (v, k, λ) is a 1-design with parameters (v, b, k, r) whose incidence matrix N satisfies the equation:

$$NN^t = (r - \lambda)I + \lambda J \tag{3.2}$$

where I denotes the identity matrix. Equation 3.2 combinatorially conveys that every pair of distinct points in a 2-design is contained in exactly λ blocks.

Difference sets are well-studied and provide a powerful tool for constructing symmetric 2-designs. Let G be a finite group of order v written multiplicatively. Let k and λ be integers

such that $v > k > 2$. A (v, k, λ) -difference set in G is a k -element subset $D \subset G$ that satisfies the property: Every non-identity element of G appears in the multiset

$$\Delta(D) := [xy^{-1} : x, y \in D, x \neq y]$$

with multiplicity λ . Difference families were introduced as a generalization of difference sets to provide additional 2-design constructions. A family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of n distinct k -element subsets of G is called a (v, k, n, λ) -*difference family* in G if every non-identity element of G is contained exactly λ times in the multiset union $\Delta(\mathcal{S}) := \bigcup_{j=1}^n \Delta(S_j)$. Notice that a difference set is a difference family with $n = 1$.

Let S be a subset of G . For any element $g \in G$, we define the *translate* of S by g as $Sg := \{xg : x \in S\}$. We then define $Dev(S) := [Sg : g \in G]$ to be the collection of all translates of S . $Dev(S)$ is often called the *development* of S . Similarly, we define the development of a family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of subsets of G to be the vn -multiset

$$Dev(\mathcal{S}) := \bigcup_{i=1}^n [S_i g : g \in G].$$

If \mathcal{S} is a (v, k, n, λ) -difference family in G , then $(G, Dev(\mathcal{S}))$ is a 2-design with parameters (v, k, λ) [53]. Further if $n = 1$ (that is, \mathcal{S} consists of a single set), the design is symmetric. Constructing 2-designs in this way is referred to as the method of difference sets (families).

Let (P, \mathcal{B}) be a design and let σ be a permutation on the point set. For any block $B = \{b_1, b_2, \dots, b_k\}$, define $\sigma(B) = \{\sigma(b_1), \sigma(b_2), \dots, \sigma(b_k)\}$. If $\sigma(\mathcal{B}) := \{\sigma(B) : B \in \mathcal{B}\} = \mathcal{B}$, then σ is called an automorphism of the design. The set of all such permutations forms a group under composition called the full automorphism group of the design. Further, any subgroup of the full automorphism group is referred to as an automorphism group of the design. The method of difference sets (families) generates 2-designs with an automorphism group isomorphic to G .

The Kramer-Mesner theorem provides a method that can often be used to determine the existence or nonexistence of 2-designs having specified automorphisms. For this result, we introduce some notation which is adopted from Stinson [53]. Let \mathcal{S}_v denote the symmetric group on a v -set, say X . For a positive integer $j \leq v$, let $\binom{X}{j}$ denote the set of all $\binom{v}{j}$ j -subsets of X . Suppose that G is a subgroup of \mathcal{S}_v . Let $j \leq v$ be a positive integer, and for $A, B \in \binom{X}{j}$,

define $A \sim_j B$ if $\sigma(A) = B$ for some $\sigma \in G$. It is not hard to see that \sim_j is an equivalence relation on $\binom{X}{j}$. The equivalence classes of this relation are called the j -orbits of X with respect to the group G . The j -orbits comprise a partition of the set $\binom{X}{j}$ and $\sigma(A) = B$ for some $\sigma \in G$ if and only if A and B are in the same orbit of G .

Suppose that $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_s$ are the k -orbits and $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_m$ are the l -orbits ($l \leq k$) of X with respect to the group G . We define an $s \times m$ matrix, denoted $A_{k,l}$, as follows. For each $1 \leq j \leq m$, choose any l -subset $Y_j \in \mathcal{P}_j$. Then for $1 \leq i \leq s$, the i, j entry of $A_{k,l}$, denoted $a_{i,j}$ is defined as follows:

$$a_{i,j} = |\{A \in \mathcal{O}_i \mid Y_j \subseteq A\}|.$$

It can be shown that the definition of $a_{i,j}$ does not depend on the particular orbit representatives Y_j that are chosen, so $A_{k,l}$ is well-defined. With this notation in hand, we now give an important result due to E. S. Kramer and D. M. Mesner.

Theorem 46. (Kramer-Mesner Theorem) *There exists a $2 - (v, k, \lambda)$ design having G as a subgroup of its automorphism group if and only if there exists a solution $z \in \mathbb{Z}^s$ to the matrix equation*

$$zA_{k,2} = \lambda \mathbf{1}_m$$

where z has nonnegative entries and $\mathbf{1}_m$ denotes the $1 \times m$ all-ones vector.

Example 47. [53]

Let $X = \{1, 2, 3, 4, 5, 6\}$, σ be the permutation $(1, 2, 3, 4, 5)(6)$ and let $G = \langle \sigma \rangle$. It is easy to see that there are three 2-orbits of X with respect to G , namely

$$\begin{aligned} \mathcal{P}_1 &= \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{5, 1\}\}, \\ \mathcal{P}_2 &= \{\{1, 3\}, \{2, 4\}, \{3, 5\}, \{4, 1\}, \{5, 2\}\}, \text{ and} \\ \mathcal{P}_3 &= \{\{1, 6\}, \{2, 6\}, \{3, 6\}, \{4, 6\}, \{5, 6\}\}. \end{aligned}$$

Also, there are four 3-orbits:

$$\begin{aligned}\mathcal{O}_1 &= \{\{1, 4, 5\}, \{3, 4, 5\}, \{1, 2, 3\}, \{2, 3, 4\}, \{1, 2, 5\}\}, \\ \mathcal{O}_2 &= \{\{2, 3, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \{2, 4, 5\}, \{1, 2, 4\}\}, \\ \mathcal{O}_3 &= \{\{1, 2, 6\}, \{1, 5, 6\}, \{2, 3, 6\}, \{3, 4, 6\}, \{4, 5, 6\}\}, \text{ and} \\ \mathcal{O}_4 &= \{\{1, 3, 6\}, \{2, 4, 6\}, \{1, 4, 6\}, \{3, 5, 6\}, \{2, 5, 6\}\}.\end{aligned}$$

The matrix $A_{3,2}$ is as follows:

$$A_{3,2} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}.$$

The equation $zA_{3,2} = 2\mathbf{1}_3$ has exactly two nonnegative integral solutions $z = (1, 0, 0, 1)$ and $z = (0, 1, 1, 0)$. Each of these solutions yields a 2-design with parameters $(6, 3, 2)$ having σ as an automorphism.

In this paper, we generalize the Kramer-Mesner theorem to partial geometric designs. A *partial geometric design*¹ with parameters $(v, b, k, r; \alpha, \beta)$ is a 1-design with parameters (v, b, k, r) which satisfies the property:

For every point $x \in P$ and every block $B \in \mathcal{B}$, the number of flags (y, C) such that $y \in B$ and $C \ni x$, is β if $x \in B$, and is α if $x \notin B$.

To avoid trivialities, in this work we restrict our attention to partial geometric designs whose parameters satisfy $\alpha > 0$, $v - 3 \geq k \geq 3$, and $b - 3 \geq r \geq 3$.

The combinatorial characterization for partial geometric designs given above can be reformulated in terms of matrix equations. Namely, (P, \mathcal{B}) is a partial geometric design with parameters $(v, b, k, r; \alpha, \beta)$ if and only if its corresponding incidence matrix N satisfies:

$$NJ = rJ, \quad JN = kJ, \quad NN^tN = (\beta - \alpha)N + \alpha J. \quad (3.3)$$

By considering Eq. (3.2) and Eq. (3.3) we see that a 2-design with parameters (v, k, λ) is a partial geometric design with parameters $\left(v, b = \frac{vr}{k}, k, r = \frac{\lambda(v-1)}{k-1}; \alpha = \lambda k, \beta = r + \lambda(k-1)\right)$.

¹Bose, Shrikhande and Singhi [8] called it a partial geometric design and Neumaier [43] called a $1\frac{1}{2}$ -design.

Also note that a partial geometric design which is not a 2-design has a concurrence matrix C which has three distinct eigenvalues where one of these eigenvalues is 0. Since partial geometric designs are a generalization of 2-designs, many of the construction methods for 2-designs can be modified for partial geometric designs. Additionally, partial geometric difference sets (originally called $1\frac{1}{2}$ -difference sets) were introduced by the second author as a generalization of difference sets [46]. This concept was then extended to partial geometric difference families, a generalization of difference families, by the authors with S. Y. Song [44].

Given a family $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of n distinct k -element subsets of a group G , for each element $z \in G$, we define the multiplicity of z in $\Delta(S_j)$ by

$$\delta_j(z) := |\{(s, t) \in S_j \times S_j : z = st^{-1}\}|.$$

Let $\delta(z)$ denote the sum of $\delta_j(z)$ over all j ; that is,

$$\delta(z) := \sum_{j=1}^n \delta_j(z).$$

Definition 48. Let v, k , and n be positive integers with $v > k > 2$. Let G be a group of order v . A collection $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ of distinct k -element subsets of G is called a *partial geometric difference family (PGDF)* in G with parameters $(v, k, n; \alpha, \beta)$ if there exist constants α and β such that, for each $x \in G$ and every $i \in \{1, 2, \dots, n\}$,

$$\sum_{y \in S_i} \delta(xy^{-1}) = \begin{cases} \alpha & \text{if } x \notin S_i, \\ \beta & \text{if } x \in S_i. \end{cases}$$

In particular, when $n = 1$, the partial geometric difference family $\mathcal{S} = \{S_1\}$ is called a *partial geometric difference set* with parameters $(v, k; \alpha, \beta)$.

One can show that the partial geometric designs admitting a group of automorphisms, which acts regularly on the point set and semi-regularly on the block set, are precisely those arising as the development of a partial geometric difference family [44].

3.3 Partial geometric designs with specified automorphisms

In this section, we give a generalization of the Kramer-Mesner theorem for partial geometric designs. First, for a given vector $z \in \mathbb{Z}^s$, we define the truncation vector \hat{z} and the index

sequence $\text{ind}(z)$ of z . The truncation vector \hat{z} is the vector z punctured on its zero coordinates, and the index sequence $\text{ind}(z)$ is the increasing sequence of nonzero coordinate positions of z . For example, for $z = (7, 0, -2, 0, 0, 12) \in \mathbb{Z}^6$, $\hat{z} = (7, -2, 12)$ and $\text{ind}(z) = (1, 3, 6)$. In what follows, we will denote the set $\{1, 2, 3, \dots, s\}$ by $[s]$.

Next, let v and k be integers with $v > k > 2$. Suppose that G is a subgroup of \mathcal{S}_v and $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_s$ are the k -orbits of G . Let $\mathcal{I} = (i_1, i_2, \dots, i_q)$, $i_j \in [s]$, be an increasing sequence. Next, for each $1 \leq h \leq q$, choose any k -subset $Y_h \in \mathcal{O}_{i_h}$ to be the orbit representative for \mathcal{O}_{i_h} . Then for each $j \in [q]$, we define the $q \times v$ matrix M_j as follows:

$$M_j(u, t) = \sum_{A \in \mathcal{O}_{i_u}, x_t \in A} |A \cap Y_j|.$$

Let M_j and M'_j be the matrices corresponding to the subsets $Y \in \mathcal{O}_{i_j}$ and $Y' \in \mathcal{O}_{i_j}$ respectively. Next we show that M_j and M'_j are same up to a permutation of the columns.

Lemma 49. *Let $\mathcal{I} = (i_1, i_2, \dots, i_q)$, $i_j \in [s]$, be an increasing sequence. Then, for $Y, Y' \in \mathcal{O}_{i_j}$,*

$$M_j = M'_j P$$

where P is a $v \times v$ permutation matrix.

Proof. There exists $\sigma \in G$ such that $\sigma(Y) = Y'$. Let $t \in [v]$ and suppose that $\sigma(x_t) = x_{t'}$. For $u \in [q]$, if $A \in \mathcal{O}_{i_u}$ with $x_t \in A$ and $|A \cap Y| = w$, then $\sigma(A) \in \mathcal{O}_{i_u}$ with $x_{t'} = \sigma(x_t) \in \sigma(A)$ and $|Y' \cap \sigma(A)| = w$. Thus,

$$M_j(u, t) = \sum_{A \in \mathcal{O}_{i_u}, x_t \in A} |A \cap Y| \leq \sum_{A \in \mathcal{O}_{i_u}, x_{t'} \in A} |A \cap Y'| = M'_j(u, t').$$

The inequality in the opposite direction follows by interchanging the roles of Y and Y' and t' and t and replacing σ by σ^{-1} . Thus, the t -th column of M_j is precisely the t' -th column of M'_j . Finally, since σ is a permutation, we have that $M_j = M'_j P$. \square

With this in mind, we then have the following.

Corollary 50. *Let $\mathcal{I} = (i_1, i_2, \dots, i_q)$, $i_j \in [s]$, be an increasing sequence and let $Y, Y' \in \mathcal{O}_{i_j}$. Then, for any $w \in \mathbb{Z}^q$,*

$$(wM_j)_t = \begin{cases} \beta & \text{if } x_t \in Y \\ \alpha & \text{if } x_t \notin Y \end{cases} \quad \text{if and only if} \quad (wM'_j)_t = \begin{cases} \beta & \text{if } x_t \in Y' \\ \alpha & \text{if } x_t \notin Y'. \end{cases}$$

Proof. There exists $\sigma \in G$ such that $\sigma(Y) = Y'$. Suppose that $\sigma(x_t) = x_{t'}$. Then $x_{t'} \in Y'$ if and only if $x_t \in Y$ and from the previous lemma $M_j(:, t) = M'_j(:, t')$, where $M(:, t)$ denotes the t -th column of the matrix M . Thus, $(wM_j)_t = (wM'_j)_{t'}$. The result now follows since σ is a permutation. \square

We now give an analogue of the Kramer-Mesner theorem for partial geometric designs.

Theorem 51. *Let G be a subgroup of \mathcal{S}_v . There exists a partial geometric design with parameters $(v, b, k, r; \alpha, \beta)$ having G as a subgroup of its automorphism group if and only if there exists a solution $z \in \mathbb{Z}^s$ to the matrix equation*

$$zA_{k,1} = r\mathbf{1}_v$$

where z has nonnegative entries and for all $j \in [q]$,

$$(\hat{z}M_j)_t = \begin{cases} \beta & \text{if } x_t \in Y_j \\ \alpha & \text{if } x_t \notin Y_j, \end{cases}$$

where $\mathcal{I} = (i_1, i_2, \dots, i_q) = \text{ind}(z)$.

Proof. First suppose that $z = (z_1, z_2, \dots, z_s)$ is a nonnegative integral solution to $zA_{k,1} = r\mathbf{1}_v$ and for all $j \in [q]$,

$$(\hat{z}M_j)_t = \begin{cases} \beta & \text{if } x_t \in Y_j \\ \alpha & \text{if } x_t \notin Y_j, \end{cases}$$

where $\mathcal{I} = (i_1, i_2, \dots, i_q) = \text{ind}(z)$. Define

$$\mathcal{B} = \bigcup_{i=1}^s z_i \mathcal{O}_i.$$

This notation indicates a multiset union. \mathcal{B} is formed by taking z_i copies of every block in \mathcal{O}_i for $1 \leq i \leq s$. Note that, by construction, every block in \mathcal{B} contains k points. Now for $x_j \in X$, the number of blocks containing x_j is

$$|\{B \in \mathcal{B} \mid x_j \in B\}| = \sum_{i=1}^s z_i |\{B \in \mathcal{O}_i \mid x_j \in B\}| = \sum_{i=1}^s z_i A_{k,1}(i, j) = r.$$

Thus, (X, \mathcal{B}) is a 1-design. Now let $x_i \in X$ and $B \in \mathcal{B}$. Then $B \in \mathcal{O}_{i_j}$ for some $i_j \in \text{ind}(z)$, $\sigma(B) = Y_j$ for some $\sigma \in G$, and $\sigma(x_i) = x_{i'}$.

$$\begin{aligned}
|\{(y, A) \mid x_i \in A, y \in A, y \in B\}| &= \sum_{u=1}^q \hat{z}_u \sum_{A \in \mathcal{O}_{i_u}, x_i \in A} |A \cap B| \\
&= \sum_{u=1}^q \hat{z}_u \sum_{A \in \mathcal{O}_{i_u}, x_{i'} \in A} |A \cap Y_j| \text{ by Lemma 49} \\
&= \sum_{u=1}^q \hat{z}_u M_j(u, i') \\
&= (\hat{z}M_j)_{i'} \\
&= \begin{cases} \beta & \text{if } x_{i'} \in Y_j \\ \alpha & \text{if } x_{i'} \notin Y_j \end{cases} \\
&= \begin{cases} \beta & \text{if } x_i \in B \\ \alpha & \text{if } x_i \notin B \end{cases} \text{ by Corollary 50.}
\end{aligned}$$

Thus, (X, \mathcal{B}) is a partial geometric design with parameters $(v, b, k, r; \alpha, \beta)$. Lastly, note that by construction, (X, \mathcal{B}) has G as a subgroup of its automorphism group.

Conversely, suppose that (X, \mathcal{B}) is the desired partial geometric design. Then necessarily \mathcal{B} must consist of a multiset union of the k -orbits \mathcal{O}_i , $1 \leq i \leq s$. Let z_i denote the number of times each block from \mathcal{O}_i occurs in \mathcal{B} . Then, since (X, \mathcal{B}) is a tactical configuration, $z = (z_1, z_2, \dots, z_s)$ is a nonnegative integral solution to $zA_{k,1} = r\mathbf{1}_v$ and for each $j \in [q]$ where $\text{ind}(z) = (i_1, i_2, \dots, i_q)$,

$$\begin{aligned}
(\hat{z}M_j)_i &= \sum_{u=1}^q \hat{z}_u M_j(u, i) \\
&= \sum_{u=1}^q \hat{z}_u \sum_{A \in \mathcal{O}_{i_u}, x_i \in A} |A \cap Y_j| \\
&= \sum_{B \in \mathcal{B}, x_i \in B} |B \cap Y_j| \\
&= |\{(y, B) \mid y \in B, y \in Y_j, x_i \in B\}| \\
&= \begin{cases} \beta & \text{if } x_i \in Y_j, \\ \alpha & \text{if } x_i \notin Y_j. \end{cases}
\end{aligned}$$

□

Further, note that the partial geometric design in Theorem 51 is simple if and only if the vector $z \in \{0, 1\}^s$.

Example 52. Let $X = [6]$ and let $G = \mathbb{Z}_6$. The 3-orbits X with respect to G are:

$$\begin{aligned}\mathcal{O}_1 &= \{\{1, 2, 3\}, \{3, 4, 5\}, \{1, 5, 6\}, \{2, 3, 4\}, \{4, 5, 6\}, \{1, 2, 6\}\}, \\ \mathcal{O}_2 &= \{\{1, 2, 4\}, \{3, 4, 6\}, \{2, 5, 6\}, \{2, 3, 5\}, \{1, 4, 5\}, \{1, 3, 6\}\}, \\ \mathcal{O}_3 &= \{\{1, 2, 5\}, \{1, 3, 4\}, \{3, 5, 6\}, \{2, 3, 6\}, \{2, 4, 5\}, \{1, 4, 6\}\}, \text{ and} \\ \mathcal{O}_4 &= \{\{1, 3, 5\}, \{2, 4, 6\}\},\end{aligned}$$

$$A_{3,1} = \begin{pmatrix} 3 & 3 & 3 & 3 & 3 & 3 \\ 3 & 3 & 3 & 3 & 3 & 3 \\ 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

and $z = (1, 0, 0, 1)$ is a solution to

$$zA_{k,1} = 4\mathbf{1}_6.$$

Note that $\hat{z} = (1, 1)$ and $\text{ind}(z) = (1, 4)$. Now let $Y_1 = \{1, 2, 3\}$ and $Y_4 = \{1, 3, 5\}$. Then,

$$M_1 = \begin{pmatrix} 6 & 7 & 6 & 3 & 2 & 3 \\ 2 & 1 & 2 & 1 & 2 & 1 \end{pmatrix} \text{ and } M_4 = \begin{pmatrix} 5 & 4 & 5 & 4 & 5 & 4 \\ 3 & 0 & 3 & 0 & 3 & 0 \end{pmatrix}$$

and

$$\hat{z}M_1 = (8, 8, 8, 4, 4, 4) = \begin{cases} 8 & \text{if } x_i \in Y_1 \\ 4 & \text{if } x_i \notin Y_1 \end{cases} \text{ and } \hat{z}M_4 = (8, 4, 8, 4, 8, 4) = \begin{cases} 8 & \text{if } x_i \in Y_4 \\ 4 & \text{if } x_i \notin Y_4 \end{cases}$$

so $(X, \mathcal{O}_1 \cup \mathcal{O}_4)$ is a partial geometric design with parameters $(v, b, k, r; \alpha, \beta) = (6, 8, 3, 4; 4, 8)$.

Example 53. In this example we provide a design with repeated blocks. Let $X = [6]$, $k = 3$ and let $G = \mathbb{Z}_6$. Note that $z = (1, 2, 0, 1)$ is a solution to

$$zA_{k,1} = 10\mathbf{1}_6.$$

Thus, $\hat{z} = (1, 2, 1)$ and $\text{ind}(z) = (1, 2, 4)$. Let $Y_1 = \{1, 2, 3\}$, $Y_2 = \{1, 2, 4\}$ and $Y_4 = \{1, 3, 5\}$.

Then

$$M_1 = \begin{pmatrix} 6 & 7 & 6 & 3 & 2 & 3 \\ 5 & 5 & 5 & 4 & 4 & 4 \\ 2 & 1 & 2 & 1 & 2 & 1 \end{pmatrix}, M_2 = \begin{pmatrix} 6 & 7 & 6 & 3 & 2 & 3 \\ 6 & 5 & 3 & 6 & 4 & 3 \\ 2 & 1 & 2 & 1 & 2 & 1 \end{pmatrix}, \text{ and } M_4 = \begin{pmatrix} 5 & 4 & 5 & 4 & 5 & 4 \\ 5 & 4 & 5 & 4 & 5 & 4 \\ 3 & 0 & 3 & 0 & 3 & 0 \end{pmatrix}$$

and

$$\hat{z}M_1 = (18, 18, 18, 12, 12, 12) = \begin{cases} 18 & \text{if } x_i \in Y_1 \\ 12 & \text{if } x_i \notin Y_1 \end{cases}, \hat{z}M_2 = (18, 18, 12, 18, 12, 12) = \begin{cases} 18 & \text{if } x_i \in Y_2 \\ 12 & \text{if } x_i \notin Y_2 \end{cases},$$

$$\text{and } \hat{z}M_4 = (18, 12, 18, 12, 18, 12) = \begin{cases} 18, & \text{if } x_i \in Y_4 \\ 12, & \text{if } x_i \notin Y_4, \end{cases}$$

so $(X, \mathcal{O}_1 \cup 2 \cdot \mathcal{O}_2 \cup \mathcal{O}_4)$ is a partial geometric design with parameters $(v, b, k, r; \alpha, \beta) = (6, 20, 3, 10; 12, 18)$

Example 54. Let $X = [12]$, let $G = \mathbb{Z}_{12}$, and suppose that \mathcal{B} consists of exactly two distinct 6-orbits. Then the partial geometric designs having G as a subgroup of their automorphism group can be obtained by taking the development of any one of the following sets of orbit representatives:

- $\{\{1, 2, 3, 4, 5, 9\}, \{1, 2, 4, 6, 8, 9\}\}$
- $\{\{1, 2, 3, 4, 6, 8\}, \{1, 2, 5, 6, 7, 9\}\}$
- $\{\{1, 2, 3, 4, 6, 8\}, \{1, 3, 4, 5, 8, 9\}\}$
- $\{\{1, 2, 3, 5, 6, 7\}, \{1, 2, 4, 6, 8, 9\}\}$
- $\{\{1, 3, 4, 5, 6, 8\}, \{1, 2, 4, 5, 6, 9\}\}$
- $\{\{1, 3, 5, 6, 7, 8\}, \{1, 2, 5, 6, 7, 9\}\}$
- $\{\{1, 3, 4, 5, 6, 8\}, \{1, 4, 5, 6, 8, 9\}\}$
- $\{\{1, 3, 5, 6, 7, 8\}, \{1, 3, 4, 5, 8, 9\}\}$

Example 55. Let $X = [6]$, σ be the permutation $(1, 2, 3, 4, 5)(6)$ and let $G = \langle \sigma \rangle$. The 3-orbits of X with respect to G are:

$$\begin{aligned}\mathcal{O}_1 &= \{\{1, 4, 5\}, \{3, 4, 5\}, \{1, 2, 3\}, \{2, 3, 4\}, \{1, 2, 5\}\}, \\ \mathcal{O}_2 &= \{\{2, 3, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \{2, 4, 5\}, \{1, 2, 4\}\}, \\ \mathcal{O}_3 &= \{\{1, 2, 6\}, \{1, 5, 6\}, \{2, 3, 6\}, \{3, 4, 6\}, \{4, 5, 6\}\}, \text{ and} \\ \mathcal{O}_4 &= \{\{1, 3, 6\}, \{2, 4, 6\}, \{1, 4, 6\}, \{3, 5, 6\}, \{2, 5, 6\}\},\end{aligned}$$

$$A_{3,1} = \begin{pmatrix} 3 & 3 & 3 & 3 & 3 & 0 \\ 3 & 3 & 3 & 3 & 3 & 0 \\ 2 & 2 & 2 & 2 & 2 & 5 \\ 2 & 2 & 2 & 2 & 2 & 5 \end{pmatrix},$$

and $z = (1, 0, 0, 1)$ is a solution to

$$zA_{k,1} = 5\mathbf{1}_6.$$

Note that $\hat{z} = (1, 1)$ and $\text{ind}(z) = (1, 4)$. Now let $Y_1 = \{1, 2, 3\}$ and $Y_4 = \{1, 3, 6\}$. Then,

$$M_1 = \begin{pmatrix} 6 & 7 & 6 & 4 & 4 & 0 \\ 3 & 2 & 3 & 2 & 2 & 6 \end{pmatrix} \text{ and } M_4 = \begin{pmatrix} 4 & 4 & 4 & 3 & 3 & 0 \\ 5 & 2 & 5 & 3 & 3 & 9 \end{pmatrix}$$

and

$$\hat{z}M_1 = (9, 9, 9, 6, 6, 6) = \begin{cases} 9 & \text{if } x_i \in Y_1 \\ 6 & \text{if } x_i \notin Y_1 \end{cases} \text{ and } \hat{z}M_4 = (9, 6, 9, 6, 6, 9) = \begin{cases} 9 & \text{if } x_i \in Y_4 \\ 6 & \text{if } x_i \notin Y_4 \end{cases}$$

so $(X, \mathcal{O}_1 \cup \mathcal{O}_4)$ is a partial geometric design with parameters $(v, b, k, r; \alpha, \beta) = (6, 10, 3, 5; 6, 9)$.

Remark 56. From Example 47, the design in Example 55 is also a 2-design with parameters $(6, 3, 2)$. Moreover, the parameters of this design satisfy the equation

$$\alpha = k(r - \beta + \alpha). \quad (3.4)$$

Partial geometric designs whose parameters satisfy Eq. (3.4) are indeed 2-designs with $\lambda = r - \beta + \alpha$ [43]. Thus, Theorem 51 implies the Kramer-Mesner theorem if the parameters of the partial geometric design satisfy Eq. (3.4).

3.4 Partial geometric difference family constructions

Let \mathcal{S} be a partial geometric difference family of a group G . It was shown in [44] that $(G, \text{Dev}(\mathcal{S}))$ is a partial geometric design admitting a group of automorphisms which acts regularly on the point set and semi-regularly on the block set.

In this section, we provide new constructions of partial geometric difference families. Our current interest lies in abelian groups. We will focus on elementary p -groups and cyclic groups. Our first construction benefits from the vector space $V = \mathbb{Z}_p^{s+1}$ and its hyperplanes.

Theorem 57. *For a prime p and a positive integer s , let $V = \mathbb{Z}_p^{s+1}$ be the $s + 1$ -dimensional vector space over \mathbb{Z}_p . Now let $r = \frac{p^{s+1}-1}{p-1} = mu$ and suppose H_0, H_1, \dots, H_{r-1} are the s -dimensional subspaces. Define $(H_i, j) = \{(\mathbf{x}, j) \mid \mathbf{x} \in H_i\}$ and*

$$B_i = (H_{im}, 0) \dot{\cup} (H_{im+1}, 1) \dot{\cup} \dots \dot{\cup} (H_{im+(m-1)}, m-1) = \bigcup_{k=0}^{m-1} (H_{im+k}, k).$$

Then $\mathcal{S} = \{B_0, B_1, \dots, B_{u-1}\}$ is a partial geometric difference family in $G = \mathbb{Z}_p^{s+1} \times \mathbb{Z}_m$ with parameters

$$\left(p^{s+1}m, p^s m, u; p^{2s-1} \left(m \binom{s+1}{s}_p - 1 \right), p^s \left((p^s - 1) \binom{s}{s-1}_p + (p^{s-1}(m-1) + 1) \binom{s+1}{s}_p \right) \right).$$

Proof. First, since each H_i is a hyperplane, by a simple application of the dimension sum theorem, $\dim(H_i \cap H_j) = s - 1$ for all distinct $i, j \in \{0, 1, \dots, r-1\}$. Next, we show that in the group ring $\mathbb{Z}[\mathbb{Z}_p^{s+1}]$,

$$H_i(X)H_j(X^{-1}) = \begin{cases} p^s \cdot H_i(X) & \text{if } i = j, \\ p^{s-1} \cdot \mathbb{Z}_p^{s+1}(X) & \text{if } i \neq j. \end{cases}$$

First, if $i = j$, for each $x \in H_i$, $x - H_i := \{x - y \mid y \in H_i\} = H_i$. Thus, in $\mathbb{Z}[\mathbb{Z}_p^{s+1}]$,

$$H_i(X)H_i(X^{-1}) = |H_i| \cdot H_i(X) = p^s \cdot H_i(X).$$

Now suppose $i \neq j$, and consider $z \in V$. Since $H_i \cup H_j = V$, $z = x - y$ for some $x \in H_i, y \in H_j$. Moreover, $z = (x + c) - (y + c)$ for each $c \in (H_i \cap H_j)$. Thus, the multiplicity of X^z in $H_i(X)H_j(X^{-1})$ is at least $|H_i \cap H_j| = p^{s-1}$. Finally, since $||z - y \mid z \in H_i, y \in H_j|| = p^{2s} = p^{s-1}|V|$, we must have that X^z occurs with multiplicity p^{s-1} for all $z \in V$ so

$$H_i(X)H_j(X^{-1}) = p^{s-1} \cdot \mathbb{Z}_p^{s+1}(X).$$

Now, in the group ring $\mathbb{Z}[\mathbb{Z}_p^{s+1} \times \mathbb{Z}_m]$,

$$\begin{aligned}
\Delta B_i(X) &= B_i(X)B_i(X^{-1}) \\
&= \left[\sum_{k=0}^{m-1} (H_{im+k}, k)(X) \right] \left[\sum_{k=0}^{m-1} (H_{im+k}, k)(X^{-1}) \right] \\
&= \sum_{k=0}^{m-1} (H_{im+k}, k)(X)(H_{im+k}, k)(X^{-1}) + \sum_{k=0}^{m-1} \sum_{l=0, l \neq k}^{m-1} (H_{im+k}, k)(X)(H_{im+l}, l)(X^{-1}) \\
&= p^s \sum_{k=0}^{m-1} (H_{im+k}, 0)(X) + \sum_{k=0}^{m-1} p^{s-1} \sum_{l=1}^{m-1} (\mathbb{Z}_p^{s+1}, l)(X) \\
&= p^s \sum_{k=0}^{m-1} (H_{im+k}, 0)(X) + mp^{s-1} \sum_{l=1}^{m-1} (\mathbb{Z}_p^{s+1}, l)(X).
\end{aligned}$$

So,

$$\begin{aligned}
\Delta(\mathcal{S})(X) &= \sum_{i=0}^{u-1} \Delta B_i(X) \\
&= \sum_{i=0}^{u-1} \left[p^s \sum_{k=0}^{m-1} (H_{im+k}, 0)(X) + mp^{s-1} \sum_{l=1}^{m-1} (\mathbb{Z}_p^{s+1}, l)(X) \right] \\
&= p^s \sum_{i=0}^{u-1} \sum_{k=0}^{m-1} (H_{im+k}, 0)(X) + p^{s-1} \begin{bmatrix} s+1 \\ s \end{bmatrix}_p \sum_{l=1}^{m-1} (\mathbb{Z}_p^{s+1}, l)(X).
\end{aligned}$$

Next, recall that the number of s -dimensional subspaces containing a given nonzero vector of

V is $\begin{bmatrix} s \\ s-1 \end{bmatrix}_p = \frac{p^s-1}{p-1}$. Thus,

$$\Delta(\mathcal{S})(X) = p^s \begin{bmatrix} s+1 \\ s \end{bmatrix}_p X^{(0,0)} + p^s \begin{bmatrix} s \\ s-1 \end{bmatrix}_p (\mathbb{Z}_p^{s+1} \setminus \mathbf{0}, 0)(X) + p^{s-1} \begin{bmatrix} s+1 \\ s \end{bmatrix}_p \sum_{l=1}^{m-1} (\mathbb{Z}_p^{s+1}, l)(X).$$

Now consider $x \in G$ and $B_i \in \mathcal{S}$. If $x \in B_i$ then $x \in (H_{im+k}, k)$ for some $0 \leq k \leq m-1$. Thus,

$$\begin{aligned}
\beta &= \sum_{y \in B_i} \delta(x-y) = \sum_{l=0}^{m-1} \sum_{y \in (H_{im+l}, l)} \delta(x-y) \\
&= \delta((\mathbf{0}, 0)) + \sum_{y \in (H_{im+k}, k) \setminus x} \delta(x-y) + \sum_{l=0, l \neq k}^{m-1} \sum_{y \in (H_{im+l}, l)} \delta(x-y) \\
&= \delta((\mathbf{0}, 0)) + \sum_{y \in (H_{im+k}, k) \setminus x} p^s \begin{bmatrix} s \\ s-1 \end{bmatrix}_p + \sum_{l=0, l \neq k}^{m-1} \sum_{y \in (H_{im+l}, l)} p^{s-1} \begin{bmatrix} s+1 \\ s \end{bmatrix}_p \\
&= p^s \begin{bmatrix} s+1 \\ s \end{bmatrix}_p + (p^s - 1)p^s \begin{bmatrix} s \\ s-1 \end{bmatrix}_p + (m-1)p^s p^{s-1} \begin{bmatrix} s+1 \\ s \end{bmatrix}_p.
\end{aligned}$$

If $x \notin B_i$, $x \in (H_{jm+k}, k)$ for some $j \neq i$, and

$$\begin{aligned}
\alpha &= \sum_{y \in B_i} \delta(x - y) \\
&= \sum_{l=0}^{m-1} \sum_{y \in (H_{im+l}, l)} \delta(x - y) \\
&= \sum_{y \in (H_{im+k}, k)} \delta(x - y) + \sum_{l=0, l \neq k}^{m-1} \sum_{y \in (H_{im+l}, l)} \delta(x - y) \\
&= \sum_{y \in (H_{im+k}, k)} p^s \begin{bmatrix} s \\ s-1 \end{bmatrix}_p + \sum_{l=0, l \neq k}^{m-1} \sum_{y \in (H_{im+l}, l)} p^{s-1} \begin{bmatrix} s+1 \\ s \end{bmatrix}_p \\
&= p^s p^s \begin{bmatrix} s \\ s-1 \end{bmatrix}_p + (m-1) p^s p^{s-1} \begin{bmatrix} s+1 \\ s \end{bmatrix}_p.
\end{aligned}$$

□

Next we provide an example concerning the Theorem 57.

Example 58. Consider $V = \mathbb{Z}_3^2$. Then $r = \begin{bmatrix} 2 \\ 1 \end{bmatrix}_3 = 4 = 2 \cdot 2$ and

$$\begin{aligned}
H_0 &= \{(0, 0), (0, 1), (0, 2)\} & H_1 &= \{(0, 0), (1, 0), (2, 0)\} \\
H_2 &= \{(0, 0), (1, 1), (2, 2)\} & H_3 &= \{(0, 0), (1, 2), (2, 1)\}.
\end{aligned}$$

Now define

$$\begin{aligned}
B_0 &= (H_0, 0) \cup (H_1, 1) = \{(0, 0), 0\}, \{(0, 1), 0\}, \{(0, 2), 0\}, \{(0, 0), 1\}, \{(1, 0), 1\}, \{(2, 0), 1\}\} \\
B_1 &= (H_2, 0) \cup (H_3, 1) = \{(0, 0), 0\}, \{(1, 1), 0\}, \{(2, 2), 0\}, \{(0, 0), 1\}, \{(1, 2), 1\}, \{(2, 1), 1\}\}.
\end{aligned}$$

Then $\mathcal{S} = \{B_0, B_1\}$ is a partial geometric difference family with parameters $(18, 6, 2; 21, 30)$ in $\mathbb{Z}_3^2 \times \mathbb{Z}_2$.

Our next theorem provides a construction method of partial geometric difference families from existing ones.

Theorem 59. Suppose $\mathcal{S} = \{S_1, \dots, S_n\}$ is a partial geometric difference family in $G = \mathbb{Z}_{v_1} \times \mathbb{Z}_{v_2} \times \dots \times \mathbb{Z}_{v_t}$, $t \geq 1$ and $v_i \in \mathbb{Z}^+$ for all $i \in [t]$, with parameters $(v, k, n; \alpha, \beta)$. If $\delta(x) = \delta(-x)$ for all $x \in G$, $\mathcal{S}' = \mathcal{S} \cup -\mathcal{S}$ is a partial geometric difference family in G with parameters $(v, k, 2n; 2\alpha, 2\beta)$.

Proof. First, note that $\Delta(-S_i) = -\Delta(S_i)$ for all $i \in [n]$. Thus, for all $x \in G$,

$$\delta_{S'}(x) = \delta_S(x) + \delta_S(-x) = 2\delta_S(x).$$

Now consider $x \in G$ and $B_i \in \mathcal{S}$.

$$\sum_{y \in B_i} \delta_{S'}(x - y) = 2 \sum_{y \in B_i} \delta_S(x - y) = \begin{cases} 2\beta_S & \text{if } x \in B_i, \\ 2\alpha_S & \text{if } x \notin B_i. \end{cases}$$

Now consider $x \in G$ and $-B_i \in -\mathcal{S}$.

$$\begin{aligned} \sum_{y \in -B_i} \delta_{S'}(x - y) &= \sum_{y \in B_i} \delta_{S'}(x + y) = 2 \sum_{y \in B_i} \delta_S(x + y) \\ &= 2 \sum_{y \in B_i} \delta_S(-x - y) = \begin{cases} 2\beta_S & \text{if } x \in -B_i, \\ 2\alpha_S & \text{if } x \notin -B_i. \end{cases} \end{aligned}$$

□

Corollary 60. *For \mathcal{S} prescribed in Theorem 57, $\mathcal{S}' = \mathcal{S} \cup -\mathcal{S}$ is also a partial geometric difference family.*

In the rest of this section we construct partial geometric difference families in cyclic groups.

Theorem 61. *Consider the ring $G = \mathbb{Z}_v$ where $v = p^u$ for some odd prime p and $u \geq 2$. Let H be the multiplicative subgroup of order p^{u-1} and let $R = \{r_1, r_2, \dots, r_{p-1}\}$ be any set of representatives for the cosets of H in \mathbb{Z}_v^\times . Finally, let $S = R \cup \{a\}$ where $a \equiv 0 \pmod{p}$. Then $\mathcal{S} = \{iS \mid i \in H\}$ is a partial geometric difference family in \mathbb{Z}_v with parameters $(p^u, p, p^{u-1}; p(p-1), p^u + p(p-1))$.*

Proof. First, recall that $\mathbb{Z}_{p^u}^\times$ is cyclic and $p+1$ has order p^{u-1} modulo p^u . Thus, $H = \langle p+1 \rangle = \{x \in G \mid x \equiv 1 \pmod{p}\}$ and the cosets of H in \mathbb{Z}_v^\times are $\{bH \mid b = 1, 2, \dots, p-1\}$. Therefore, when we reduce the elements of iS modulo p , we get precisely $\{0, 1, 2, \dots, p-1\}$. Thus, for each $x \in S$, $x - S$ consists of 0 and exactly one element congruent to j modulo p for each $j \in \{1, 2, \dots, p-1\}$. Hence, $\Delta(S)$ consists of 0 with multiplicity p and p elements congruent

to j modulo p for each $j \in \{1, 2, \dots, p-1\}$. Finally, since $\Delta\mathcal{S} = \bigcup_{i \in H} i\Delta(S)$, $\Delta\mathcal{S}$ contains each coset of H with multiplicity p and 0 with multiplicity p^u . That is,

$$\delta(x) = \begin{cases} p^u & \text{if } x = 0; \\ p & \text{if } x \not\equiv 0 \pmod{p}; \\ 0 & \text{if } x \equiv 0 \pmod{p} \text{ and } x \neq 0. \end{cases}$$

Now let $x \in G$ and $B \in \mathcal{S}$.

If $x \in B$, then

$$\sum_{y \in B} \delta(x-y) = \delta(0) + \sum_{y \in B \setminus \{x\}} \delta(x-y) = p^u + \sum_{y \in B \setminus \{x\}} p = p^u + p(p-1).$$

If $x \notin B$, then $x - B$ contains precisely one element congruent 0 modulo p and this element is nonzero. Call this element z . Then

$$\sum_{y \in B} \delta(x-y) = \sum_{y \in B \setminus \{z\}} p = p(p-1).$$

□

Theorem 62. Consider the ring $G = \mathbb{Z}_{3^u}$ for some $u \geq 2$. Let $a \in G$ such that $a \equiv 0 \pmod{3}$ and define $X := \{x \in G \mid x \leq \frac{3^u-1}{2}, x \not\equiv 0 \pmod{3}\}$. Then $\mathcal{S} = \{\{x, -x, a\} \mid x \in X\}$ is a partial geometric difference family in G with parameters $(3^u, 3, \frac{3^u-1}{2}; 6, 3(\frac{3^u-1}{2}) + 6)$.

Proof. First,

$$\Delta(\{x, -x, a\}) = [0, 0, 0, 2x, -2x, x+a, -x+a, x-a, -x-a].$$

Next, note that

$$\bigcup_{x \in X} \{x, -x\} = \mathbb{Z}_{3^u}^\times = \{x \in G \mid x \not\equiv 0 \pmod{3}\}.$$

Now since $2 \in \mathbb{Z}_{3^u}^\times$, $\bigcup_{x \in X} \{2x, -2x\} = \mathbb{Z}_{3^u}^\times$. Further, since $a \equiv 0 \pmod{3}$, we have that $\mathbb{Z}_{3^u}^\times + a = \mathbb{Z}_{3^u}^\times - a = \mathbb{Z}_{3^u}^\times$. Thus,

$$\delta(x) = \begin{cases} 3(\frac{3^u-1}{2}) & \text{if } x = 0; \\ 3 & \text{if } x \not\equiv 0 \pmod{3}; \\ 0 & \text{if } x \equiv 0 \pmod{3} \text{ and } x \neq 0. \end{cases}$$

Further note that if we reduce the elements of $\{x, -x, a\}$ modulo 3 we get $\{0, 1, 2\}$. Thus, for any $y \in G$, $y - \{x, -x, a\}$ contains exactly one element z congruent to 0 modulo 3. Further, $z = 0$ precisely when $y \in \{x, -x, a\}$. Therefore, for $x \in G$ and $B \in \mathcal{S}$,

$$\sum_{y \in B} \delta(x - y) = \begin{cases} 3\left(\frac{3^u - 1}{2}\right) + 2 \cdot 3 & \text{if } x \in B, \\ 2 \cdot 3, & \text{if } x \notin B. \end{cases}$$

□

Theorem 63. *Let $G = \mathbb{Z}_v$ where $v = pu$ for a prime $p \geq u$. Let $B_0 = \{b_0, b_1, \dots, b_{u-1}\}$ where $b_i \equiv i \pmod{u}$ and define $B_i = (iu + 1)B_0$ for $i = 0, 1, \dots, p-1$. If $x \not\equiv 0 \pmod{p}$ for all nonzero $x \in \Delta B_0$, then $\mathcal{S} = \{B_0, B_1, \dots, B_{p-1}\}$ is a partial geometric difference family with parameters $(v, u, p; u(u-1), u(u-1) + pu)$.*

Proof. First note that when we reduce the elements of B_i modulo u we get precisely $\{0, 1, \dots, u-1\}$. Thus, for each $x \in B_0$, $x - B_0$ consists of 0 and exactly one element congruent to j modulo u for each $j \in \{1, 2, \dots, u-1\}$. Hence, $\Delta(B_0)$ consists of 0 with multiplicity u and u elements congruent to j modulo u for each $j \in \{1, 2, \dots, u-1\}$.

Let $H = \langle u \rangle < G$. Now for any nonzero $z \in \Delta(B_0)$, $z \equiv j \pmod{u}$ for some $1 \leq j \leq u-1$ and $z \not\equiv 0 \pmod{p}$. Thus, $\{z(ui + 1) \mid i = 0, 1, \dots, p-1\} = H + j$. Therefore,

$$\Delta(\mathcal{S}) = \bigcup_{i=0}^{p-1} (iu + 1)\Delta(B_0) = \bigcup_{z \in B_0} H + (z \pmod{u})$$

consists of each coset $H + j$, $1 \leq j \leq u-1$, with multiplicity u and 0 with multiplicity v . That is,

$$\delta(x) = \begin{cases} v & \text{if } x = 0; \\ u & \text{if } x \not\equiv 0 \pmod{u}; \\ 0 & \text{if } x \equiv 0 \pmod{u} \text{ and } x \neq 0. \end{cases}$$

Now, as stated before, if we reduce the elements of B_i modulo u we get $\{0, 1, \dots, u - 1\}$. Thus, for any $y \in G$, $y - B_i$ contains exactly one element z congruent to 0 modulo u . Further, $z = 0$ precisely when $y \in B_i$. Therefore, for $x \in G$ and $B_i \in \mathcal{S}$,

$$\sum_{y \in B_i} \delta(x - y) = \begin{cases} v + (u - 1)u & \text{if } x \in B, \\ (u - 1)u & \text{if } x \notin B. \end{cases}$$

□

Example 64. Let $v = 20 = p \cdot u$ where $p = 5$ and $u = 4$. Then the family

$$\mathcal{S} = \{\{0, 1, 2, 3\}, \{0, 5, 10, 15\}, \{0, 9, 18, 7\}, \{0, 13, 19, 6\}, \{0, 11, 14, 17\}\}$$

is a partial geometric difference family in \mathbb{Z}_{20} with parameters $(20, 4, 5; 12, 32)$.

3.5 Concluding remarks

In this paper, we gave an analogue to the Kramer-Mesner for partial geometric designs. We also provided several new constructions of partial geometric difference families. As discussed earlier, if $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ is a partial geometric difference family in a group G , then $(G, \text{Dev}(\mathcal{S}))$ is a partial geometric design. The parameters of the partial geometric designs arising from our constructions in Section 4 are listed in Table 4.1.

Moreover, as mentioned in the Introduction, partial geometric designs were recently shown to produce directed strongly regular graphs²[12].

Theorem 65. [44] Let $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$ be a family of distinct k -subsets of a group G of order v . Suppose that \mathcal{S} is a partial geometric difference family with parameters $(v, k, n; \alpha, \beta)$ and $(P, \mathcal{B}) = (G, \text{Dev}(\mathcal{S}))$ is the associated partial geometric design with parameters $(v, vn, k, kn; \alpha, \beta)$.

Then

²A directed strongly regular graph with parameters $(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda, \mu)$ is, by definition, a directed graph on \mathbf{v} vertices without loops such that (i) every vertex has in-degree and out-degree \mathbf{k} , (ii) every vertex x has \mathbf{t} out-neighbors that are also in-neighbors of x , and (iii) the number of directed paths of length 2 from a vertex x to another vertex y is λ if there is an edge from x to y , and is μ if there is no edge from x to y [27].

Table 3.1 Parameters of partial geometric designs obtained from PGDFs

Here s and u are positive integers, $u \geq 2$, p is a prime, $\alpha_p = p^{2s-1} \left(p \begin{bmatrix} s \\ s-1 \end{bmatrix}_p + (m-1) \begin{bmatrix} s+1 \\ s \end{bmatrix}_p \right)$,
and $\beta_p = p^s \left((p^s - 1) \begin{bmatrix} s \\ s-1 \end{bmatrix}_p + (p^{s-1}(m-1) + 1) \begin{bmatrix} s+1 \\ s \end{bmatrix}_p \right)$.

v	b	k	α	β	(Th.#)	Notes
$p^{s+1}m$	$p^{s+1} \begin{bmatrix} s+1 \\ s \end{bmatrix}_p$	$p^s \begin{bmatrix} s+1 \\ s \end{bmatrix}_p$	α_p	β_p	12	$\begin{bmatrix} s+1 \\ s \end{bmatrix}_p = mu$
p^u	p^{2u-1}	p^u	$p(p-1)$	$p^u + p(p-1)$	17	
3^u	$\frac{3^u(3^u-1)}{2}$	$\frac{3(3^u-1)}{2}$	$\frac{3(3^u-1)}{2} + 6$	6	18	
v	vp	v	$u(u-1)$	$u(u-1) + pu$	19	$v = pu, p \geq u$

(i) the directed graph Γ whose vertex set is $V(\Gamma) = \{(p, B) \in P \times \mathcal{B} : p \notin B\}$ and adjacency is defined by $(p, B) \rightarrow (q, C)$ if and only if $p \in C$, is a directed strongly regular graph with parameters

$$(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda, \mu) = (vn(v-k), kn(v-k), k^2n - \alpha, k^2n - \beta, k^2n - \alpha);$$

(ii) the directed graph Γ' whose vertex set is $V(\Gamma') = \{(p, B) \in P \times \mathcal{B} : p \in B\}$ and adjacency is defined by $(p, B) \rightarrow (q, C)$ if and only if $(p, B) \neq (q, C)$ and $p \in C$, is a directed strongly regular graph with parameters

$$(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda, \mu) = (vkn, k^2n - 1, \beta - 1, \beta - 2, \alpha).$$

Thus, applying Theorem 65 to each of our constructions in Section 4, we obtain two directed strongly regular graphs whose parameters are prescribed above.

CHAPTER 4. LINKS BETWEEN ORTHOGONAL ARRAYS, ASSOCIATION SCHEMES AND PARTIAL GEOMETRIC DESIGNS

A paper submitted to *Designs, Codes, and Cryptography*

Kathleen Nowak, Oktay Olmez, and Sung-Yell Song

Abstract

In this paper, we show how certain three-class association schemes and orthogonal arrays give rise to partial geometric designs. We also investigate the connections between partial geometric designs and certain regular graphs having three or four distinct eigenvalues, three-class association schemes, orthogonal arrays of strength two and particular linear codes. We give various characterizations of these graphs, association schemes and orthogonal arrays in terms of partial geometric designs. We also give a list of infinite families of directed strongly regular graphs arising from the partial geometric designs obtained in this paper.

4.1 Introduction

Partial geometric designs (also known as $1\frac{1}{2}$ -designs) were recently shown to produce directed strongly regular graphs [12]. In [46] and [44] we uncovered which difference sets and difference families produce partial geometric designs. Here we take the next step and explore the link between these designs and other combinatorial structures. Specifically, we establish connections with strongly regular graphs, certain wreath product association schemes, three-class association schemes, and specific orthogonal arrays of strength two.

It is well-known that many strongly regular graphs give rise to symmetric 2-designs and partial geometric designs (cf. [9], [43], [54]). In particular, every complete multipartite regular

graph gives rise to a partial geometric design. Additionally, any strongly regular graph satisfying $\lambda = \mu$ gives rise to a symmetric 2 - (v, k, λ) design, which is, in turn, a partial geometric design. (See, for example, [43, 52, 29].) In fact it is shown that a strongly regular graph with parameters (v, k, λ, μ) gives rise to a partial geometric design if and only if it satisfies either $k = \mu$ or $\lambda = \mu$ (cf. Section 4.3 below).

Every strongly regular graph is realized as a relation graph of some association scheme. In particular, a nontrivial strongly regular graph and its complement are the relation graphs of a two-class association scheme. However, there are graphs that give rise to partial geometric designs but are not realized as relation graphs of association schemes. Our investigation into finding the source of partial geometric designs begins with studying the characteristics of the graphs that give rise to such designs. We observe that some of these graphs arise as the relation graphs of certain three-class association schemes. This observation leads us to explore the links between partial geometric designs, graphs, and association schemes. Some of these association schemes come from certain orthogonal arrays of strength two and linear codes. As a consequence, we are able to find an infinite family of partial geometric designs and give a list of directed strongly regular graphs arising from these partial geometric designs.

The organization of the paper is as follows. In the following section, we introduce notation that will be used throughout and recall some basic terms from the theory of designs and association schemes.

In Section 4.3, we characterize the strongly regular graphs that give rise to partial geometric designs.

In Section 4.4, we recall that the wreath product of an arbitrary association scheme with the trivial association scheme possesses a relation graph isomorphic to a strongly regular graph. Hence such a wreath product association scheme gives rise to a partial geometric design. Conversely, if an imprimitive association scheme of class three or more contains exactly one strongly regular relation graph, then such a scheme must be isomorphic to the wreath product of a scheme with a one-class association scheme.

In Section 4.5, we describe parameter sets of certain three-class association schemes that give rise to partial geometric designs. In particular, we show that if a 3-class symmetric self-

dual association scheme of order $3m^2$ satisfies certain parametric conditions, then its adjacency matrices A_0, A_1, A_2, A_3 satisfy the following identities for some constants α_i and β_i :

$$\begin{aligned} A_1^3 &= \beta_1 A_1 + \alpha_1 (J - A_1), \\ A_2^3 &= \beta_2 A_2 + \alpha_2 (J - A_2), \\ (A_3 + A_0)^3 &= \beta_3 (A_3 + A_0) + \alpha_3 (J - A_3 - A_0). \end{aligned}$$

In Section 4.6, we then provide concrete examples of such association schemes coming from Hamming codes and certain orthogonal arrays of strength two.

In Section 4.7, we provide the parameter sets of directed strongly regular graphs obtained from the partial geometric designs constructed in this paper by applying the relationship between partial geometric designs and directed strongly regular graphs given by Brouwer-Olmez-Song in [12]. Finally, we close with some last remarks on our construction of partial geometric designs.

4.2 Preliminaries

Here we recall some basic facts about block designs and association schemes. We also set the notation that will be used throughout the paper.

4.2.1 Designs

A *block design* is a pair (P, \mathcal{B}) where P is a finite set, the elements of which are called *points*, and \mathcal{B} is a finite collection (possibly multiset) of nonempty subsets of P called *blocks*.

A *tactical configuration*, often also called a *1-design*, with parameters (v, b, k, r) is a design (P, \mathcal{B}) with $|P| = v$ and $|\mathcal{B}| = b$ such that each block consists of k points and each point belongs to r blocks. A 2 - (v, k, λ) *design* is a 1-design satisfying the added condition that every pair of distinct points is contained in exactly λ blocks.

A *partial geometric design* with parameters $(v, b, k, r; \alpha, \beta)$ is a 1-design (P, \mathcal{B}) with parameters (v, b, k, r) satisfying the ‘partial geometric’ property: For every point $x \in P$ and every block $B \in \mathcal{B}$, the number of incident point-block pairs (y, C) such that $y \in B$ and $x \in C$ is α

if $x \notin B$ and is β if $x \in B$ for some constants α and β . That is,

$$|\{(y, C) : y \in B \cap C, C \ni x\}| = \begin{cases} \alpha & \text{if } x \notin B, \\ \beta & \text{if } x \in B. \end{cases}$$

If N is the point-block incidence matrix of a $(v, b, k, r; \alpha, \beta)$ -partial geometric design, then it satisfies

$$JN = kJ, \quad NJ = rJ, \quad NN^T N = \beta N + \alpha(J - N), \quad (4.1)$$

where N^T denotes the transpose of N , and J is the all-ones matrix. A 2 - (v, k, λ) design is partial geometric with $\alpha = k\lambda$ and $\beta = \lambda \frac{v-1}{k-1} + k\lambda - \lambda$. We will say that a partial geometric design (P, \mathcal{B}) is *symmetric* whenever $v = b$ (and so, $k = r$). When the design is symmetric, its parameters are simply denoted by $(v, k; \alpha, \beta)$, in short.

In this paper, by the phrase, “*graph $\Gamma = (V, E)$ gives rise to design (P, \mathcal{B}) ,” we mean that the adjacency matrix A of Γ is *equivalent* to the incidence matrix N of (P, \mathcal{B}) . That is, for each $v \in V$, if we let $N_v = \{x \in V : (x, v) \in E\}$ and $\mathcal{N} = \{N_v : v \in V\}$, the pair (V, \mathcal{N}) forms a design that is *isomorphic* to (P, \mathcal{B}) .¹*

4.2.2 Association schemes and their Bose-Mesner algebras

Let X be an n -element set, and let R_0, R_1, \dots, R_d be subsets of $X \times X := \{(x, y) : x, y \in X\}$ with $R_0 = \{(x, x) : x \in X\}$. Let A_i be the $n \times n$ $\{0, 1\}$ -matrix representing R_i : i.e.,

$$(A_i)_{xy} = \begin{cases} 1 & \text{if } (x, y) \in R_i \\ 0 & \text{otherwise.} \end{cases}$$

The pair $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ is called a d -*class (symmetric) association scheme* if A_0, A_1, \dots, A_d satisfy the following:

- (1) $A_0 + A_1 + \dots + A_d = J$, where J is the all-ones matrix and $A_0 = I$, the identity matrix,
- (2) for each $i \in \{0, 1, \dots, d\}$, $A_i^T = A_i$,
- (3) for any $h, i, j \in \{0, 1, \dots, d\}$, there exists a constant p_{ij}^h such that

$$A_i A_j = \sum_{h=0}^d p_{ij}^h A_h.$$

¹There exist bijections $f: V \rightarrow P$ and $\phi: \mathcal{N} \rightarrow \mathcal{B}$ such that $x \in N_v$ if and only if $f(x) \in \phi(N_v)$.

The matrices A_0, A_1, \dots, A_d defined above are called the *adjacency matrices* of \mathcal{X} , and the graphs $(X, R_1), (X, R_2), \dots, (X, R_d)$, are called the *relation graphs* of \mathcal{X} . The constants p_{ij}^h are called the *intersection numbers* of \mathcal{X} , and for any $(x, y) \in R_h$

$$p_{ij}^h = |\{z \in X : (x, z) \in R_i, (z, y) \in R_j\}|.$$

Let $B_i, i \in \{0, 1, \dots, d\}$, be the *ith intersection matrix* defined by

$$(B_i)_{jh} = p_{ij}^h.$$

Then $B_i B_j = \sum_{h=0}^d p_{ij}^h B_h$.

Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be an association scheme with its adjacency matrices A_0, A_1, \dots, A_d and intersection matrices B_0, B_1, \dots, B_d . Then the \mathbb{C} -space with basis $\{A_0, A_1, \dots, A_d\}$ is an algebra over the complex numbers, called the *Bose-Mesner algebra* of \mathcal{X} , denoted by $\mathcal{A}(\mathcal{X})$ or $\langle A_0, A_1, \dots, A_d \rangle$. The \mathbb{C} -algebra generated by $\{B_0, B_1, \dots, B_d\}$ is called the *intersection algebra* of \mathcal{X} . The Bose-Mesner algebra $\mathcal{A}(\mathcal{X})$ and the intersection algebra $\langle B_0, B_1, \dots, B_d \rangle$ are isomorphic \mathbb{C} -algebras induced by the correspondence $A_i \mapsto B_i$. (For more information, see for example, [3, 10].)

4.3 Strongly regular graphs with either $k = \mu$ or $\lambda = \mu$

Strongly regular graphs arise from various combinatorial structures, especially in connection with designs and codes. For a complete characterization of partial geometric designs as well as a thorough investigation of their connection to partial geometries and strongly regular graphs, we refer the readers to Bose, Shrikhande and Singh [8] and Neumaier [43]. In this section, we characterize which strongly regular graphs give rise to symmetric partial geometric designs.

Lemma 66. *Let Γ be a strongly regular graph with parameters (v, k, λ, μ) . Let A be the adjacency matrix of Γ . Then $A^3 = \beta A + \alpha(J - A)$ for some integers α and β if and only if either $\lambda = \mu$ or $k = \mu$. (In this case, $\alpha = (\lambda - \mu)\mu + \mu k$ and $\beta = (\lambda - \mu)^2 + k - \mu + (\lambda - \mu)\mu + \mu k$.)*

Proof. Given a strongly regular graph Γ with parameters (v, k, λ, μ) , the adjacency matrix A of Γ satisfies the identity:

$$A^2 = kI + \lambda A + \mu(J - I - A).$$

Thus, we have that

$$A^3 = \{(\lambda - \mu)^2 + (\lambda - \mu)\mu + k\mu + k - \mu\}A + (\lambda - \mu)(k - \mu)I + \{(\lambda - \mu)\mu + \mu k\}(J - A).$$

Therefore, there exist α and β such that $A^3 = \beta A + \alpha(J - A)$ if and only if

$$(\lambda - \mu)(k - \mu) = 0, (\lambda - \mu)^2 + k - \mu + (\lambda - \mu)\mu + \mu k = \beta \text{ and } (\lambda - \mu)\mu + \mu k = \alpha.$$

Hence the proof follows. \square

Every complete multipartite strongly regular graph can be viewed as the complement of c -copies of the complete graph K_n on n vertices for some integers c and n (where $c, n \geq 2$). We denote such a graph by $\overline{cK_n}$.

Corollary 67. *The complete multipartite strongly regular graph $\overline{cK_n}$ gives rise to a symmetric partial geometric design with parameters $(cn, (c - 1)n; (c^2 - 3c + 2)n^2, (c^2 - 3c + 3)n^2)$.*

Proof. This strongly regular graph has parameters

$$(v, k, \lambda, \mu) = (cn, (c - 1)n, (c - 2)n, (c - 1)n).$$

The result now follows from Lemma 66. \square

A strongly regular graph with parameters (v, k, λ, λ) is sometimes called a (v, k, λ) -graph. The adjacency matrix A of a (v, k, λ) -graph satisfies identity $A^2 = kI + \lambda(J - I)$; therefore, it gives a symmetric 2- (v, k, λ) -design. Since a symmetric 2- (v, k, λ) -design is a partial geometric design with parameters $(v, k; k\lambda, k\lambda + k - \lambda)$, so we also have:

Corollary 68. *A (v, k, λ) -graph gives rise to a partial geometric design with parameters*

$$(v, k; k\lambda, k\lambda + k - \lambda).$$

Remark 69. (1) *We note that both the Hamming graph $H(2, 4)$ and the Shrikhande graph are $(16, 6, 2)$ -graphs. Although these two graphs are non-isomorphic they give rise to the same 2- $(16, 6, 2)$ -design. (cf. [15, Ch.2 and Ch.4].) Hence, we have a partial geometric design with parameters $(v, k; \alpha, \beta) = (16, 6; 12, 16)$ as all 2-designs are partial geometric.*

(2) We also note that there are many (v, k, λ) -graphs: Examples of small graphs include $(35, 15, 6)$, $(35, 18, 9)$, $(36, 21, 12)$, $(45, 12, 3)$, $(63, 32, 16)$ and $(64, 36, 20)$. To see the current list of such strongly regular graphs, visit the homepage of E. Spence [52] or A. Brouwer [11].

4.4 Wreath product of a scheme by a one-class association scheme

In this section, we establish a connection between partial geometric designs and wreath products of association schemes. We show that every wreath product association scheme in which one factor is a trivial association scheme gives rise to a partial geometric design. It follows from the fact that such a wreath product association scheme has a relation graph which is strongly regular with $k = \mu$.

Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ and $\mathcal{Y} = (Y, \{S_j\}_{0 \leq j \leq e})$ be association schemes of order $|X| = m$ and $|Y| = n$, respectively. Let $\{A_i\}_{0 \leq i \leq d}$ and $\{C_j\}_{0 \leq j \leq e}$ be the sets of adjacency matrices of \mathcal{X} and \mathcal{Y} , respectively. Then the adjacency matrices of the wreath product $\mathcal{X} \wr \mathcal{Y}$ of \mathcal{X} and \mathcal{Y} are

$$I_n \otimes A_0, I_n \otimes A_1, \dots, I_n \otimes A_d, C_1 \otimes J_m, C_2 \otimes J_m, \dots, C_e \otimes J_m,$$

where $A \otimes C = (a_{ij}C)$ denotes the Kronecker product of $A = (a_{ij})$ and C . With this ordering of the adjacency matrices, the relation matrix of $\mathcal{X} \wr \mathcal{Y}$ is given by

$$R(\mathcal{X} \wr \mathcal{Y}) = I_n \otimes R(\mathcal{X}) + [R(\mathcal{Y}) + d(J_n - I_n)] \otimes J_m,$$

where $R(\mathcal{X}) = \sum_{h=0}^d hA_h$ and $R(\mathcal{Y}) = \sum_{h=0}^e hC_h$.

Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be an association scheme with its Bose-Mesner algebra $\mathcal{A}(\mathcal{X}) = \langle A_0, A_1, \dots, A_d \rangle$. For any relations R_i and R_j , define

$$R_i R_j := \left\{ R_h : p_{ij}^h \neq 0 \right\}.$$

Then, for a nonempty subset H of $\{0, 1, \dots, d\}$, $\{R_h\}_{h \in H}$ is called a *closed subset* if $R_i R_j \subseteq \{R_h\}_{h \in H}$ for any $i, j \in H$. If $\{R_h\}_{h \in H}$ is a closed subset, then the \mathbb{C} -space with basis $\{A_h\}_{h \in H}$ is a subalgebra of $\mathcal{A}(\mathcal{X})$, called a *Bose-Mesner subalgebra* of \mathcal{X} , denoted by \mathcal{A}_H or $\mathcal{A}_H(\mathcal{X})$.

Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be an association scheme with $\mathcal{A}(\mathcal{X}) = \langle A_0, A_1, \dots, A_d \rangle$, and let $\{R_h\}_{h \in H}$ be a closed subset of \mathcal{X} . Let $\mathcal{Y} = (Y, \{S_j\}_{0 \leq j \leq e})$ be an association scheme with its Bose-Mesner algebra $\mathcal{A}(\mathcal{Y}) = \langle C_0, C_1, \dots, C_e \rangle$. Let $\{S_g\}_{g \in G}$ be a closed subset of \mathcal{Y} . We say that the Bose-Mesner subalgebras $\mathcal{A}_H(\mathcal{X})$ and $\mathcal{A}_G(\mathcal{Y})$ are *exactly isomorphic* if there is a bijection $\pi : H \rightarrow G$ such that the linear map from $\mathcal{A}_H(\mathcal{X})$ to $\mathcal{A}_G(\mathcal{Y})$ induced by $A_h \mapsto C_{\pi(h)}$ for $h \in H$ is an algebra isomorphism.

The following properties of the Bose-Mesner algebra of a wreath product of association schemes (See [5, 6]) are useful for our discussion.

Lemma 70. *Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be an association scheme. Let \mathcal{K}_n denote the one-class association scheme whose nontrivial relation graph is the complete graph K_n . If $\mathcal{X} = \mathcal{Y} \wr \mathcal{K}_n$ for an association scheme $\mathcal{Y} = (Y, \{S_j\}_{0 \leq j \leq e})$ and \mathcal{K}_n , then $e = d - 1$ and, by renumbering R_1, R_2, \dots, R_d if necessary, the following hold.*

(i) $\{R_0, R_1, \dots, R_{d-1}\}$ is a closed subset of \mathcal{X} such that the Bose-Mesner subalgebra $\mathcal{A}_{[d-1]}$ with basis $\{A_0, A_1, \dots, A_{d-1}\}$ is exactly isomorphic to the Bose-Mesner algebra of \mathcal{Y} .

(ii) Let k_0, k_1, \dots, k_d denote the valency of \mathcal{X} , and let $m = \sum_{i=0}^{d-1} k_i$. Then $|Y| = m$ and

$$A_i A_d = k_i A_d, \quad 1 \leq i < d; \quad (4.2)$$

$$A_d^2 = m(n-1)(J_{mn} - A_d) + m(n-2)A_d \quad (4.3)$$

and

$$A_d^3 = m^2(n^2 - 3n + 2)(J_{mn} - A_d) + m^2(n^2 - 3n + 3)A_d. \quad (4.4)$$

Proof. Let C_j be the adjacency matrix of \mathcal{Y} corresponding to S_j , $0 \leq j \leq e$. Then the adjacency matrices A_i of $\mathcal{Y} \wr \mathcal{K}_n$ can be expressed as follows:

$$A_0 = I_n \otimes C_0, \quad A_1 = I_n \otimes C_1, \dots, A_{d-1} = I_n \otimes C_e, \quad A_d = (J_n - I_n) \otimes J_m.$$

Thus, $e = d - 1$ and

$$\begin{aligned}
A_d^2 &= ((J_n - I_n) \otimes J_m)^2 &= (J_n - I_n)^2 \otimes J_m^2 \\
&= ((n - 2)J_n + I_n) \otimes mJ_m \\
&= m(n - 2)(J_n - I_n) \otimes J_m + m(n - 1)I_n \otimes J_m \\
&= m(n - 2)A_d + m(n - 1)(J_{mn} - A_d).
\end{aligned}$$

This verifies that (4.3) holds. We then obtain the identity (4.4) by multiplying both sides of (4.3) by A_d and using (4.3) again to derive the desired form. It is clear that the valency k_i of R_i is equal to that of S_i , for $1 \leq i \leq d - 1$, and (4.2) holds. Obviously, $\{R_1, R_2, \dots, R_{d-1}\}$ is a closed subset, and the Bose-Mesner subalgebra with basis $\{A_0, A_1, \dots, A_{d-1}\}$ is exactly isomorphic to the Bose-Mesner algebra of \mathcal{Y} . \square

From (4.4), we have the following.

Theorem 71. *Let $\mathcal{X} = \mathcal{Y} \wr \mathcal{K}_n$ be the wreath product of association schemes \mathcal{Y} and \mathcal{K}_n . Let the adjacency matrices of \mathcal{X} be ordered such a way that $A_d = (J_n - I_n) \otimes J_m$ where $m = |Y|$. Then the A_d can be viewed as the incidence matrix of a symmetric partial geometric design with parameters $(mn, m(n - 1); m^2(n^2 - 3n + 2), m^2(n^2 - 3n + 3))$.*

Proof. It immediately follows from the fact that the relation graph (X, R_d) is a multipartite strongly regular graph. \square

4.5 Certain three-class self-dual association schemes of order $3m^2$

In this section we show that the relation graphs of certain three-class association schemes give rise to partial geometric designs.

In order to represent the parameters of an association scheme in a compact form, we recall the definition of its character table. Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be a symmetric association scheme of order $|X| = n$ with adjacency matrices A_0, A_1, \dots, A_d . Let $E_0 = \frac{1}{n}J, E_1, \dots, E_d$ denote the primitive idempotents in $\mathcal{A}(\mathcal{X})$. Then there are $p_j(i), q_i(j) \in \mathbb{C}$ for all $i, j \in \{0, 1, \dots, d\}$ such

that

$$A_j = \sum_{i=0}^d p_j(i)E_i \quad \text{and} \quad E_i = \frac{1}{n} \sum_{j=0}^d q_i(j)A_j.$$

The $(d+1) \times (d+1)$ matrices P and Q whose (i, j) -entries are defined by

$$P_{ij} = p_j(i) \quad \text{and} \quad Q_{ij} = q_j(i)$$

are called the *1st eigenmatrix* and *2nd eigenmatrix* of \mathcal{X} , respectively. The first eigenmatrix is often called the *character table* of the association scheme. We note that $PQ = nI$. An association scheme is said to be (*formally*) *self-dual* if $P = Q$. Next, note that if none of the relation graphs of a symmetric three-class association scheme are strongly regular, then every relation graph has four distinct eigenvalues [54].

Lemma 72. *Let \mathcal{Z} be a three-class symmetric association scheme of order $3m^2$ for some positive integer $m \equiv 0 \pmod{3}$. Then the following two statements are equivalent.*

(1) *The character table P of \mathcal{Z} is given by*

$$P = \begin{bmatrix} 1 & m(m-1) & m(m+1) & (m-1)(m+1) \\ 1 & m & 0 & -m-1 \\ 1 & 0 & -m & m-1 \\ 1 & -m & m & -1 \end{bmatrix}.$$

(2) *\mathcal{Z} is self-dual and its adjacency matrices A_i satisfy the following identities:*

$$\begin{aligned} A_1^3 &= m^2 A_1 + \frac{1}{3} m^2 (m-1)(m-2)J \\ A_2^3 &= m^2 A_2 + \frac{1}{3} m^2 (m+1)(m+2)J \\ (A_3 + I)^3 &= m^2 (A_3 + I) + \frac{1}{3} m^2 (m-1)(m+1)J. \end{aligned}$$

Proof. First, it is straightforward to verify that $P^2 = 3m^2 I$, and so \mathcal{Z} is self-dual. We can also calculate all the intersection numbers of \mathcal{Z} directly from the character table by using the basic identity:

$$p_{ij}^h = \frac{1}{n \cdot k_h} \sum_{\nu=0}^3 p_i(\nu) p_j(\nu) p_h(\nu) k_\nu$$

for $h, i, j \in \{0, 1, 2, 3\}$. Namely, the intersection matrices are given by:

$$\begin{aligned}
B_1 &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ m(m-1) & \frac{1}{3}m(m-2) & \frac{1}{3}m(m-1) & \frac{1}{3}m^2 - m \\ 0 & \frac{1}{3}m(m+1) & \frac{1}{3}m(m-1) & \frac{1}{3}m^2 \\ 0 & \frac{1}{3}m(m-2) - 1 & \frac{1}{3}m(m-1) & \frac{1}{3}m^2 \end{bmatrix} \\
B_2 &= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & \frac{1}{3}m(m+1) & \frac{1}{3}m(m-1) & \frac{1}{3}m^2 \\ m(m+1) & \frac{1}{3}m(m+1) & \frac{1}{3}m(m+2) & \frac{1}{3}m^2 + m \\ 0 & \frac{1}{3}m(m+1) & \frac{1}{3}m(m+2) - 1 & \frac{1}{3}m^2 \end{bmatrix} \\
B_3 &= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & \frac{1}{3}m(m-2) - 1 & \frac{1}{3}m(m-1) & \frac{1}{3}m^2 \\ 0 & \frac{1}{3}m(m+1) & \frac{1}{3}m(m+2) - 1 & \frac{1}{3}m^2 \\ (m-1)(m+1) & \frac{1}{3}m(m+1) & \frac{1}{3}m(m-1) & \frac{1}{3}m^2 - 2 \end{bmatrix}.
\end{aligned}$$

Second, by applying the basic identity

$$B_i B_j = \sum_{h=0}^3 p_{ij}^h B_h,$$

we obtain

$$B_i^3 = B_i^2 B_i = p_{ii}^0 B_0 B_i + p_{ii}^1 B_1 B_i + p_{ii}^2 B_2 B_i + p_{ii}^3 B_3 B_i$$

for $i = 1, 2, 3$, in the intersection algebra of \mathcal{Z} . Note that $B_0 B_i = B_i$. By plugging the values of p_{ij}^h in the second identity and using the first identity repeatedly, we obtain the following identities:

$$\begin{aligned}
B_1^3 &= m^2 B_1 + \frac{1}{3}m^2(m-1)(m-2)(B_0 + B_1 + B_2 + B_3) \\
B_2^3 &= m^2 B_2 + \frac{1}{3}m^2(m+1)(m+2)(B_0 + B_1 + B_2 + B_3) \\
(B_3 + B_0)^3 &= m^2(B_3 + B_0) + \frac{1}{3}m^2(m-1)(m+1)(B_0 + B_1 + B_2 + B_3)
\end{aligned}$$

Finally, we see that the desired identities are deduced from these identities by the isomorphism between the Bose-Mesner algebra $\langle A_0, A_1, A_2, A_3 \rangle$ and intersection algebra $\langle B_0, B_1, B_2, B_3 \rangle$. Thus (1) implies (2).

Conversely, if we multiply both sides of each identity in (2) by the all-ones vector \mathbf{j} , then for instance, from the first identity, we have

$$A_1^3 \mathbf{j} = m^2 A_1 \mathbf{j} + \frac{1}{3} m^2 (m-1)(m-2) J \mathbf{j}$$

or equivalently,

$$k_1^3 \mathbf{j} = m^2 k_1 \mathbf{j} + m^4 (m-1)(m-2) \mathbf{j}.$$

That is, we have

$$k_1^3 = m^2 k_1 + m^4 (m-1)(m-2);$$

and so, $k_1 = m(m-1)$. Similarly, we find $k_2 = m(m+1)$ and $k_3 + 1 = m^2$. Furthermore, since the all-ones matrix J has only one non-zero eigenvalue (which is $3m^2$) and the rest of them are zeros, from the identity $A_1^3 - m^2 A_1 = \frac{1}{3} m^2 (m-1)(m-2) J$, we see that the remaining possible eigenvalues for A_1 are $0, m, -m$. This is also true for the cases of A_2 and $A_3 + I$. Also we know that by the self-duality of the association scheme, possible multiplicities for these eigenvalues are k_1, k_2 , and k_3 . Now by using the row- and column-orthogonality of the character table, we can arrange the eigenvalues of A_1, A_2 and A_3 to obtain P . This completes the proof. \square

As an immediate consequence of this lemma, we have the following.

Theorem 73. *Let \mathcal{Z} be a three-class association scheme, and let A_0, A_1, A_2, A_3 be its adjacency matrices. Suppose that the character table P of \mathcal{Z} is given by*

$$P = \begin{bmatrix} 1 & m(m-1) & m(m+1) & (m-1)(m+1) \\ 1 & m & 0 & -m-1 \\ 1 & 0 & -m & m-1 \\ 1 & -m & m & -1 \end{bmatrix}.$$

Then \mathcal{Z} gives rise to three symmetric partial geometric designs coming from the incidence matrices A_1, A_2 and $A_3 + A_0$. In this case, the parameters $(v, k; \alpha, \beta)$ of corresponding partial geometric designs are given by

$$(3m^2, m(m-1); \frac{1}{3}m^2(m^2 - 3m + 2), \frac{1}{3}m^2(m^2 - 3m + 5)),$$

$$(3m^2, m(m+1); \frac{1}{3}m^2(m^2+3m+2), \frac{1}{3}m^2(m^2+3m+5)),$$

$$(3m^2, m^2; \frac{1}{3}m^2(m^2-1), \frac{1}{3}m^2(m^2+2)).$$

Remark 74. *Having a character table of an association scheme is equivalent to having the intersection matrices since the character table essentially generates all intersection numbers and vice versa. However, it is possible for more than one association scheme to have the same character table, and thus, the same intersection numbers. For example, it is well-known that the two strongly regular graphs with the same parameters $(16, 6, 2, 2)$ discussed in Remark 69 in Section 4.3, are relation graphs of two distinct two-class association schemes.*

4.6 The association schemes from codes and orthogonal arrays

In this section, we give concrete examples of the three-class association schemes described in the previous section. Our examples come as fusion schemes of the Hamming association scheme $H(d, 3)$ and are also obtained from a family of linear orthogonal arrays of strength two. As a result, we see an interesting link between the three-class association schemes and linear orthogonal arrays.

4.6.1 From Hamming schemes

Here we show that a three-class fusion scheme of $H(d, 3)$ for each odd $d \geq 3$ gives rise to partial geometric designs.

First we recall the definition of the Hamming scheme $H(d, q)$. Let S be a q -element set and let

$$V := S^d = \{(x_1, x_2, \dots, x_d) : x_j \in S, j = 1, 2, \dots, d\}.$$

Define the association relation between any $\mathbf{x} = (x_1, x_2, \dots, x_d)$ and $\mathbf{y} = (y_1, y_2, \dots, y_d) \in V$ according to the Hamming distance

$$\delta(\mathbf{x}, \mathbf{y}) := |\{j \in \{1, 2, \dots, d\} : x_j \neq y_j\}|;$$

that is, define

$$(\mathbf{x}, \mathbf{y}) \in R_i \Leftrightarrow \delta(\mathbf{x}, \mathbf{y}) = i.$$

Then $(V, \{R_i\}_{0 \leq i \leq d})$ is an association scheme called the d -class *Hamming scheme*, over S , denoted by $H(d, q)$.

First, we show that among the Hamming schemes of class three, $H(3, 3)$ is the only Hamming scheme that gives rise to partial geometric designs.

Proposition 75. *The relation graphs of the Hamming scheme $H(3, q)$ give rise to partial geometric designs if and only if $q = 3$.*

Proof. The eigenmatrices and the first intersection matrix of $H(3, q)$ are given by

$$P = Q = \begin{bmatrix} 1 & 3(q-1) & 3(q-1)^2 & (q-1)^3 \\ 1 & 2q-3 & (q-1)(q-3) & -(q-1)^2 \\ 1 & q-3 & -2q+3 & q-1 \\ 1 & -3 & 3 & -1 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 3(q-1) & q-2 & 2 & 0 \\ 0 & 2(q-1) & 2(q-2) & 3 \\ 0 & 0 & q-1 & 3(q-2) \end{bmatrix}$$

By direct calculation, it is shown that the intersection matrices satisfy the identity:

$$B_1^3 = 3(q^2 - 3q + 2)I + (q^2 + 3q - 3)B_1 + 6(q-2)B_2 + 6B_3.$$

By the algebra isomorphism between the Bose-Mesner algebra and the intersection algebra, it then follows that

$$A_1^3 = 3(q^2 - 3q + 2)I + (q^2 + 3q - 3)A_1 + 6(q-2)A_2 + 6A_3.$$

Therefore, when $q = 3$, we have

$$A_1^3 = 15A_1 + 6(J - A_1).$$

However, for $H(3, q)$ with $q \neq 3$, there is no way that we can express A_1^3 as a linear combination of A_1 and $J - A_1$. Therefore, we see that the first relation graph of $H(3, q)$ gives rise to a partial geometric design if and only if $q = 3$. By a similar calculation, we can verify that when $q = 3$,

$$B_2^3 = 69B_2 + 60(B_0 + B_1 + B_3), \quad (B_3 + B_0)^3 = 33(B_3 + B_0) + 24(B_1 + B_2),$$

or equivalently,

$$A_2^3 = 69A_2 + 60(J - A_2), \quad (A_3 + I)^3 = 33(A_3 + I) + 24(J - A_3 - I).$$

This completes the proof. \square

We note that $H(3, 3)$ has the same parameters as the three-class association scheme described in Lemma 72 with $m = 3$. Although there is no other Hamming scheme whose relation graphs give rise to partial geometric designs, there exists a three-class fusion scheme of $H(d, 3)$, for each odd $d \geq 3$, whose relation graphs give rise to partial geometric designs. Kageyama, Saha and Das in [35, Theorem 2] introduced the following three-class fusion scheme \mathcal{F} of $H(d, 3)$ which will be called the *KSD-scheme* in what follows.

Theorem 76. [35] Consider Hamming scheme $H(d, 3) = (V, \{R_i\}_{0 \leq i \leq d})$ with $d = 2l + 1$ for $l \geq 1$, and let $S_0 = R_0$ and

$$S_j = \bigcup_{i=0}^{\lfloor (d-j)/3 \rfloor} R_{3i+j}, \text{ for } j = 1, 2, 3$$

where $\lfloor (d-j)/3 \rfloor$ denotes the greatest integer less than or equal to $(d-j)/3$. Then $\mathcal{F} = (V, \{S_0, S_1, S_2, S_3\})$ is a three-class association scheme with the following intersection matrices:

$$B_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 3^{2l} + (-1)^l 3^l & 3^{2l-1} + 2(-1)^l 3^{l-1} & 3^{2l-1} + (-1)^l 3^{l-1} & 3^{2l-1} + (-1)^l 3^l \\ 0 & 3^{2l-1} - (-1)^l 3^{l-1} & 3^{2l-1} + (-1)^l 3^{l-1} & 3^{2l-1} \\ 0 & 3^{2l-1} + 2(-1)^l 3^{l-1} - 1 & 3^{2l-1} + (-1)^l 3^{l-1} & 3^{2l-1} \end{bmatrix}$$

$$B_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 3^{2l-1} - (-1)^l 3^{l-1} & 3^{2l-1} + (-1)^l 3^{l-1} & 3^{2l-1} \\ 3^{2l} - (-1)^l 3^l & 3^{2l-1} - (-1)^l 3^{l-1} & 3^{2l-1} - 2(-1)^l 3^{l-1} & 3^{2l-1} - (-1)^l 3^l \\ 0 & 3^{2l-1} - (-1)^l 3^{l-1} & 3^{2l-1} - 2(-1)^l 3^{l-1} - 1 & 3^{2l-1} \end{bmatrix}$$

$$B_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 3^{2l-1} + 2(-1)^l 3^{l-1} - 1 & 3^{2l-1} + (-1)^l 3^{l-1} & 3^{2l-1} \\ 0 & 3^{2l-1} - (-1)^l 3^{l-1} & 3^{2l-1} - 2(-1)^l 3^{l-1} - 1 & 3^{2l-1} \\ 3^{2l} - 1 & 3^{2l-1} - (-1)^l 3^{l-1} & 3^{2l-1} + (-1)^l 3^{l-1} & 3^{2l-1} - 2 \end{bmatrix}.$$

Remark 77. For every d , the association scheme \mathcal{F} belongs to the family of association schemes \mathcal{Z} described in Lemma 72. In fact, if l is odd, the two schemes \mathcal{F} and \mathcal{Z} have the same parameters with $m = 3^l$. For each even integer l , the parameters of \mathcal{F} are the same as those of \mathcal{Z} with $m = 3^l$ and the first and second association relations switched.

Corollary 78. For each $l \geq 1$, the relation graphs of the association scheme \mathcal{F} above give rise to three non-isomorphic symmetric partial geometric designs with parameters

$$\begin{aligned} & (3^{2l+1}, 3^{2l} + (-1)^l 3^l; 3^{4l-1} + (-1)^l 3^{3l} + 2 \cdot 3^{2l-1}, 3^{4l-1} + (-1)^l 3^{3l} + 5 \cdot 3^{2l-1}), \\ & (3^{2l+1}, 3^{2l} - (-1)^l 3^l; 3^{4l-1} - (-1)^l 3^{3l} + 2 \cdot 3^{2l-1}, 3^{4l-1} - (-1)^l 3^{3l} + 5 \cdot 3^{2l-1}), \\ & (3^{2l+1}, 3^{2l}; 3^{4l-1} - 3^{2l-1}, 3^{4l-1} + 2 \cdot 3^{2l-1}). \end{aligned}$$

Proof. The proof directly follows from the following identities of the intersection matrices:

$$\begin{aligned} B_1^3 &= \left(3^{4l-1} + (-1)^l 3^{3l} + 5 \cdot 3^{2l-1}\right) B_1 + \left(3^{4l-1} + (-1)^l 3^{3l} + 2 \cdot 3^{2l-1}\right) (B_0 + B_2 + B_3), \\ B_2^3 &= \left(3^{4l-1} - (-1)^l 3^{3l} + 5 \cdot 3^{2l-1}\right) B_2 + \left(3^{4l-1} - (-1)^l 3^{3l} + 2 \cdot 3^{2l-1}\right) (B_0 + B_1 + B_3), \\ (B_3 + B_0)^3 &= \left(3^{4l-1} + 2 \cdot 3^{2l-1}\right) (B_3 + B_0) + \left(3^{4l-1} - 3^{2l-1}\right) (B_1 + B_2). \end{aligned}$$

Thus three designs whose incidence matrices are A_1 , A_2 and $A_3 + I$ are obtained from this association scheme. \square

4.6.2 From orthogonal arrays of strength two

Our search for three-class association schemes whose relation graphs give rise to partial geometric designs continues in the context of orthogonal arrays and linear codes. Here we find another way to construct the KSD-schemes using orthogonal arrays of strength 2 coming from suitable linear codes. Taking the runs (codewords) as the elements of the underlying set and defining association relations according to the Hamming distances between the codewords, we obtain three-class association schemes that are isomorphic to KSD-schemes.

Let S be a set of q -symbols where $q \geq 2$, and let $I := \{1, 2, \dots, m\}$. Let $X = S^I$ be the set of all maps from I to S . Note that we can view each element $\mathbf{x} \in X$ as an m -tuple (x_1, x_2, \dots, x_m) with symbols x_i in S . A *code* is simply a subset C of X . In the case where $S = \mathbb{F}_q$ and C forms

a vector space over \mathbb{F}_q , we call C a *linear code*. Next, an N -element subset Y of X , viewed as an $N \times m$ array of symbols, is called an *orthogonal array of strength t and index λ* if every $N \times t$ subarray contains all possible q^t t -tuples exactly λ times. Following the notation of [31], we denote an orthogonal array Y with the above parameters by $OA(N, m, q, t)$ where $\lambda = N/q^t$. The rows of an $OA(N, m, q, t)$ are sometimes called the *runs* of the orthogonal array. In what follows, the runs of Y will be denoted $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_N$ with $\mathbf{y}_i = (y_{i1}, y_{i2}, \dots, y_{im})$. It will be clear whether we consider Y as an N -set or as an array from the context.

An orthogonal array is *linear* if it takes a finite field as its symbol set, and its rows form a vector space over the field. We will show that for every positive integer l , there exists a linear orthogonal array $OA(3^{2l+1}, 2l+3, 3, 2)$ coming from a certain linear $[2l+3, 2l+1]_3$ -code which gives an association scheme isomorphic to a KSD-scheme. First we have the following example.

Example 79. *Two mutually orthogonal Latin cubes of order 3 give an orthogonal array $OA(27, 5, 3, 2)$.*

The transpose of the orthogonal array is expressed as the following 5×27 array M .

$$M = \begin{pmatrix} 000 & 000 & 000 & 111 & 111 & 111 & 222 & 222 & 222 \\ 000 & 111 & 222 & 000 & 111 & 222 & 000 & 111 & 222 \\ 012 & 012 & 012 & 012 & 012 & 012 & 012 & 012 & 012 \\ 000 & 111 & 222 & 222 & 000 & 111 & 111 & 222 & 000 \\ 012 & 120 & 201 & 012 & 120 & 201 & 012 & 120 & 201 \end{pmatrix}$$

A 3-class association scheme is then obtained as follows:

(i) Let $Y := \{\mathbf{y}_i : i = 1, 2, \dots, 27\}$ be the set of columns of M (runs of $OA(27, 5, 3, 2)$).

(ii) Let $R_0 = \{(\mathbf{y}_i, \mathbf{y}_i) : \mathbf{y}_i \in Y\}$, and let

$$R_1 = \{(\mathbf{y}_i, \mathbf{y}_j) \in Y \times Y : \delta(\mathbf{y}_i, \mathbf{y}_j) = 2 \text{ or } 5\}$$

$$R_2 = \{(\mathbf{y}_i, \mathbf{y}_j) \in Y \times Y : \delta(\mathbf{y}_i, \mathbf{y}_j) = 3\}$$

$$R_3 = \{(\mathbf{y}_i, \mathbf{y}_j) \in Y \times Y : \delta(\mathbf{y}_i, \mathbf{y}_j) = 4\}$$

Then $\mathcal{Y} = (Y, \{R_i\}_{0 \leq i \leq 3})$ is an association scheme. Its character table is given by

$$P = Q = \begin{bmatrix} 1 & 6 & 8 & 12 \\ 1 & 3 & -4 & 0 \\ 1 & -3 & -1 & 3 \\ 1 & 0 & 2 & -3 \end{bmatrix},$$

and we have the following identities in the Bose-Mesner algebra of \mathcal{Y} :

$$A_1^3 = 15A_1 + 6(J - A_1), \quad (A_2 + I)^3 = 33(A_2 + I) + 24(J - A_2 - I) \quad \text{and} \quad A_3^3 = 69A_3 + 60(J - A_3).$$

Remark 80. (1) The above 3-class association scheme is shown to be isomorphic to $H(3, 3)$ discussed in Proposition 75. Here the isomorphism is established by the fact that all Hamming schemes except for $H(2, 4)$ are uniquely determined by their intersection numbers.

(2) This $OA(27, 5, 3, 2)$ can be also obtained as the codewords generated by the three vectors $[1, 0, 0, 1, 1]$, $[0, 1, 0, 0, 1]$ and $[0, 0, 1, 1, 0]$ over \mathbb{F}_3 in the five dimensional Hamming space $H(5, 3)$.

In the rest of this section, our alphabet S (the symbol set) will be finite field \mathbb{F}_q of order q . We will denote the code of length n and size N over the alphabet \mathbb{F}_q by $(n, N)_q$ or by $(n, N, d)_q$ if the minimum distance d is known. If the code is an m -dimensional subspace of the n -dimensional vector space \mathbb{F}_q^n , we denote it by $[n, m]_q$ -code (or $[n, m]$ -code if the field is clear from the context). We denote the dual code of a $[n, m]$ -code \mathcal{C} , by \mathcal{C}^\perp and its minimum distance by d^\perp , the dual distance of \mathcal{C} . Two linear codes are *isomorphic* if one can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a nonzero element of the field. Two linear orthogonal arrays are considered to be the same if the associated codes are isomorphic as linear codes.

In order to describe how we find linear orthogonal arrays $OA(3^{2l+1}, 2l + 3, 3, 2)$ from $[2l + 3, 2l + 1]_3$ -codes, we recall a few useful facts which link orthogonal arrays and linear codes. R. C. Bose [7] explicitly specified how the strength of a linear orthogonal array is determined by the associated code. Ph. Delsarte [21] specified connections between the codes and orthogonal arrays. Our results are based on the following theorem which states a special case of a more

profound result due to him. It suffices for our construction of orthogonal arrays as we chiefly concentrate on the linear case. (See [31, Ch. 4] for more information.)

Theorem 81. [21] *If \mathcal{C} is a $(n, N, d)_q$ linear code over \mathbb{F}_q with dual distance d^\perp then the codewords of \mathcal{C} form the rows of an $OA(N, n, q, d^\perp - 1)$ with entries from \mathbb{F}_q . Conversely, the rows of a linear $OA(N, n, q, t)$ over \mathbb{F}_q form a $(n, N, d)_q$ linear code over \mathbb{F}_q with dual distance $d^\perp \geq t + 1$. If the orthogonal array has strength t but not $t + 1$, d^\perp is precisely $t + 1$.*

Remark 82. *In particular, given q, m and fixed strength t , if the $m \times n$ generator matrix G for any $[n, m]_q$ -code \mathcal{C} has the property that every t -columns of G are linearly independent vectors in \mathbb{F}_q^m over \mathbb{F}_q , then the q^m codewords of \mathcal{C} form a linear orthogonal array $OA(q^m, n, q, t)$. For this, we note that G generates q^m codewords all of which become the runs of the $q^m \times n$ orthogonal array, say M . The $q^m \times t$ subarray obtained by taking any t -columns of M contains linear combinations of the rows of the corresponding t -columns of G ; and it contains each of q^t t -tuples of symbols exactly q^{m-t} times.*

Thus, in order to obtain orthogonal arrays of strength 2, we simply look at the generator matrices of all $[n, m]_q$ -codes over \mathbb{F}_q and pick the ones whose dual distance is 3. By Theorem 81 and Remark 82, we know that if such a $[2l + 3, 2l + 1]_3$ -code yields an orthogonal array, then it must be a $OA(3^{2l+1}, 2l + 3, 3, 2)$. Now we demonstrate an infinite family of orthogonal arrays that give rise to the three-class association schemes we seek.

Consider the $[2l + 3, 2l + 1]_3$ -code \mathcal{C} with generator matrix

$$G = \left[\begin{array}{c|cc} & & 1 & 1 \\ & & 0 & 1 \\ & I_{2l+1} & 1 & 0 \\ & & 0 & 0 \\ & & \vdots & \vdots \\ & & 0 & 0 \end{array} \right]$$

where I_{2l+1} denotes the $(2l + 1) \times (2l + 1)$ identity matrix. Then the dual code \mathcal{C}^\perp is generated

by

$$G^\perp = \begin{bmatrix} 1 & 0 & 1 & 0 & \cdots & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 & \cdots & 0 & 1 & 2 \end{bmatrix}$$

with its weight distribution $(1, 0, 0, 4, 2, 2, 0, \dots, 0)$. Thus, by Theorem 16, the codewords of the $(2l + 3, 3^{2l+1})_3$ -code \mathcal{C} with dual distance 3, form the rows of an $OA(3^{2l+1}, 2l + 3, 3, 2)$.

Next, consider the $[2l + 3, 2l + 1]_3$ -codes \mathcal{C}' with generator matrix

$$G' = \left[\begin{array}{c|cc} & & 0 & 0 \\ & & 0 & 0 \\ & & \vdots & \vdots \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & 0 & 0 \end{array} \right].$$

We can identify \mathcal{C}' as the Hamming space $H(2l + 1, 3)$ by viewing \mathcal{C}' as a natural embedding of \mathbb{F}_3^{2l+1} in \mathbb{F}_3^{2l+3} . Moreover, suppose we define

$$M_0 = \{\mathbf{0}\}, \quad M_i = \{\mathbf{x} \in \mathcal{C} \setminus \{\mathbf{0}\} : \delta_H(\mathbf{0}, \mathbf{x}) \equiv i \pmod{3}\} \quad \text{for } i = 1, 2, 3,$$

and the sets M'_i for \mathcal{C}' in the same manner. Then $\{M_i : i = 0, 1, 2, 3\}$ forms a partition of \mathcal{C} . In the same spirit, $\{M'_i : i = 0, 1, 2, 3\}$ forms a partition of \mathcal{C}' according to their Hamming weights. By Theorem 76, we know that

$$\{|M'_i| : i = 0, 1, 2, 3\} = \{1, 3^l(3^l + 1), 3^l(3^l - 1), 3^{2l} - 1\}.$$

By establishing a vector space isomorphism between \mathcal{C}' and \mathcal{C} as below, we can also see that

$$\{|M_i| : i = 0, 1, 2, 3\} = \{1, 3^l(3^l + 1), 3^l(3^l - 1), 3^{2l} - 1\}.$$

For this, let $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{2l+1}$ denote the rows of G' , as the basis vectors for \mathcal{C}' , and $\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_{2l+1}$ denote the rows of G , which form a basis for \mathcal{C} . Define a map $\phi : \mathcal{C}' \rightarrow \mathcal{C}$ by

$$\phi(\mathbf{e}_1) = \mathbf{r}_1 + \mathbf{r}_2 + \mathbf{r}_3, \quad \phi(\mathbf{e}_2) = \mathbf{r}_2, \quad \phi(\mathbf{e}_3) = \mathbf{r}_3,$$

and for $i > 3$,

$$\phi(\mathbf{e}_i) = \begin{cases} \mathbf{r}_i + \mathbf{r}_{i+1}, & \text{if } i \equiv 0 \pmod{2} \\ \mathbf{r}_{i-1} + 2\mathbf{r}_i, & \text{if } i \equiv 1 \pmod{2} \end{cases}.$$

It is clear that ϕ is a vector space isomorphism. Furthermore, this map ϕ maps M'_i to M_i setwise; namely, $\phi(M'_1) = M_2$, $\phi(M'_2) = M_1$ and $\phi(M'_3) = M_3$. For this, we recall that the sets M'_i and M_i were defined according to the Hamming weight of the codewords. Notice that a weight- s codeword \mathbf{x} can be expressed as $\sum_{h=1}^s \alpha_h \mathbf{e}_{j_h}$ for some $\alpha_h \in \mathbb{F}_3^*$ and some s -set $\{j_1, j_2, \dots, j_s\}$ with $1 \leq j_1 < j_2 < \dots < j_s \leq 2l + 1$ (where $\mathbb{F}_3^* = \mathbb{F}_3 - \{0\}$). So, we can express

$$M'_i = \left\{ \sum_{h=1}^s \alpha_h \mathbf{e}_{j_h} : 1 \leq j_1 < j_2 < \dots < j_s \leq 2l + 1, \alpha_h \in \mathbb{F}_3^*, s \equiv i \pmod{3}, 1 \leq s \leq 2l + 1 \right\}.$$

Then, by direct computation, it can be verified that

$$\phi(M'_i) = \left\{ \sum_{h=1}^s \alpha_h \phi(\mathbf{e}_{j_h}) : \sum_{h=1}^s \alpha_h \mathbf{e}_{j_h} \in M'_i \right\} \subseteq \begin{cases} M_2 & \text{if } i = 1 \\ M_1 & \text{if } i = 2 \\ M_3 & \text{if } i = 3 \end{cases}.$$

So, it follows that

$$\phi(M'_1) = M_2, \quad \phi(M'_2) = M_1, \quad \phi(M'_3) = M_3$$

$$\text{as } |M'_1| + |M'_2| + |M'_3| = |M_1| + |M_2| + |M_3| = 3^{2l+1} - 1.$$

As a consequence, we have the following.

Theorem 83. *1. For each $l \in \mathbb{N}$, there exists a linear $[2l + 3, 2l + 1]_3$ -code \mathcal{C} with dual distance 3, such that \mathcal{C} is partitioned into M_0, M_1, M_2, M_3 where $M_0 = \{\mathbf{0}\}$ and for $i = 1, 2, 3$, $M_i = \{\mathbf{x} \in \mathcal{C} \setminus \{\mathbf{0}\} : \delta_H(\mathbf{0}, \mathbf{x}) \equiv i \pmod{3}\}$ with cardinalities $|M_i| \in \{3^{2l} - 3^l, 3^{2l} + 3^l, 3^{2l} - 1\}$. In this case, any linear $[2l + 3, 2l + 1]_3$ -code equivalent to \mathcal{C} is an orthogonal array $OA(3^{2l+1}, 2l + 3, 3, 2)$.*

2. Defining relations on \mathcal{C} by

$$R_0 = \{(\mathbf{x}, \mathbf{x}) : \mathbf{x} \in \mathcal{C}\}$$

$$R_1 = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{C} \times \mathcal{C} : \delta_H(\mathbf{x}, \mathbf{y}) \equiv 1 \pmod{3}\}$$

$$R_2 = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{C} \times \mathcal{C} : \delta_H(\mathbf{x}, \mathbf{y}) \equiv 2 \pmod{3}\}$$

$$R_3 = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{C} \times \mathcal{C} : \mathbf{x} \neq \mathbf{y}, \delta_H(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod{3}\}$$

we obtain a three-class association scheme $\mathcal{W} = (\mathcal{C}, \{R_i\}_{0 \leq i \leq 3})$ which has the same parameters as those for the KSD-scheme \mathcal{F} for $d = 2l + 1$ defined in Theorem 76.

Proof. The statement (1) is summary of what we have discussed earlier. For statement (2), we recall that, under the map ϕ , all codewords of weight i in \mathcal{C}' are mapped to the codewords of weight $2i \pmod{3}$ in \mathcal{C} ; and thus, for any $\mathbf{x}, \mathbf{y} \in \mathcal{C}'$, $\delta_H(\mathbf{x}, \mathbf{y}) \equiv i \pmod{3}$ if and only if $\delta_H(\phi(\mathbf{x}), \phi(\mathbf{y})) \equiv 2i \pmod{3}$. Therefore, the three-class association scheme \mathcal{W} defined on \mathcal{C} and the KSD-scheme \mathcal{F} defined on $H(2l+1, 3)$ in Theorem 76 share the same parameter sets. That is, if the parameters of KSD scheme are p_{ij}^h , then those for \mathcal{W} are $p_{\sigma(i)\sigma(j)}^{\sigma(h)}$ where $\sigma = (12)$ is the transposition in S_3 . \square

We now give an example to illustrate what we have discussed in this subsection.

Example 84. *The linear $[7, 5]_3$ -code \mathcal{C} generated by*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

has weight distribution $(1, 4, 8, 24, 60, 82, 56, 8)$ and dual weight distribution $(1, 0, 0, 4, 2, 2, 0, 0)$. This code \mathcal{C} (and any code equivalent to \mathcal{C}) gives $OA(243, 7, 3, 2)$. By defining association relations by

$$\begin{aligned} R_0 &= \{(x, x) \mid x \in X\} \\ R_1 &= \{(x, y) \mid \delta_H(x, y) \in \{1, 4, 7\}\} \\ R_2 &= \{(x, y) \mid \delta_H(x, y) \in \{2, 5\}\} \\ R_3 &= \{(x, y) \mid \delta_H(x, y) \in \{3, 6\}\}, \end{aligned}$$

we obtain a three-class association scheme, described as \mathcal{W} . The intersection matrices of \mathcal{W} are given by

$$B_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 72 & 21 & 24 & 18 \\ 0 & 30 & 24 & 27 \\ 0 & 20 & 24 & 27 \end{bmatrix} \quad B_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 30 & 24 & 27 \\ 90 & 30 & 33 & 36 \\ 0 & 30 & 32 & 27 \end{bmatrix} \quad B_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 20 & 24 & 27 \\ 0 & 30 & 32 & 27 \\ 80 & 30 & 24 & 25 \end{bmatrix}.$$

and for this association scheme, we have the following identities in the Bose-Mesner algebra of \mathcal{W} :

$$\begin{aligned} A_1^3 &= 1593A_1 + 1512(J - A_1), \\ A_2^3 &= 3051A_2 + 2970(J - A_2), \\ (A_3 + I)^3 &= 2241(A_3 + I) + 2160(J - A_3 - I). \end{aligned}$$

Therefore, we obtain three partial geometric designs with parameters

$$(v, k; \alpha, \beta) = (243, 72; 1512, 1593), (243, 90; 2160, 2241), (243, 81; 2970, 3051).$$

4.7 Directed strongly regular graphs

Given a partial geometric design, Theorems 2.1 and 2.2 in [12] tell us how to construct two directed strongly regular graphs. One is defined on the flags of the design, while the other is defined on the antiflags. Here we list the parameters of the directed strongly regular graphs that we can obtain from the partial geometric designs constructed above.

Definition 85. *A directed strongly regular graph (DSRG) with parameters $(v, k, \mathfrak{t}, \lambda', \mu')$ is a directed graph on v vertices without loops such that*

- (1) *Every vertex has in-degree and out-degree k ,*
- (2) *Every vertex has \mathfrak{t} out-neighbors which are also in-neighbors, and*
- (3) *For any two distinct vertices x and y , the number of directed paths from x to y of length 2 is λ' if $x \rightarrow y$ and is μ' otherwise.*

We observe that the adjacency matrix of a DSRG with parameters $(v, k, \mathfrak{t}, \lambda', \mu')$ has the property that

$$AJ = JA = kJ \quad \text{and} \quad A^2 = \mathfrak{t}I + \lambda'A + \mu'(J - I - A).$$

Theorem 86. [12] *Let (P, \mathcal{B}) be a 1-design. The following three statements are equivalent.*

1. *(P, \mathcal{B}) is a partial geometric design.*

2. The directed graph Γ defined by $V(\Gamma) = \{(p, B) \in P \times \mathcal{B} : p \in B\}$ with the adjacency

$$(p, B) \rightarrow (q, C) \text{ if and only if } (p, B) \neq (q, C) \text{ and } p \in C,$$

is a DSRG.

3. The directed graph Γ' defined by $V(\Gamma') = \{(p, B) \in P \times \mathcal{B} : p \notin B\}$ with adjacency

$$(p, B) \rightarrow (q, C) \text{ if and only if } p \in C,$$

is a DSRG.

Remark 87. According to this theorem, any symmetric partial geometric design with parameters $(v, k; \alpha, \beta)$ gives rise to two DSRGs whose parameters $(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda', \mu')$ are given by

$$(v(v-k), k(v-k), k^2 - \alpha, k^2 - \beta, k^2 - \alpha) \text{ and } (vk, k^2 - 1, \beta - 1, \beta - 2, \alpha).$$

Therefore, from the partial geometric designs we have obtained in this paper, (in Theorem 73, Corollary 78 and Theorem 83) we obtain the DSRGs with the following parameters.

Table 4.1 Parameters of DSRGs obtained from partial geometric designs
(Here $m = 3^l$ for every positive integer l .)

\mathbf{v}	\mathbf{k}	\mathbf{t}	λ'	μ'
$3m^3(2m+1)$	$m^2(m-1)(2m+1)$	$\frac{1}{3}m^2(2m^2-3m+1)$	$\frac{1}{3}m^2(2m^2-3m-2)$	$\frac{1}{3}m^2(2m^2-3m+1)$
$3m^3(m-1)$	$m^2(m-1)^2-1$	$\frac{1}{3}m^2(m^2-3m+5)-1$	$\frac{1}{3}m^2(m^2-3m+5)-2$	$\frac{1}{3}m^2(m^2-3m+2)$
$3m^3(2m-1)$	$m^2(m+1)(2m-1)$	$\frac{1}{3}m^2(2m^2+3m+1)$	$\frac{1}{3}m^2(2m^2+3m-2)$	$\frac{1}{3}m^2(2m^2+3m+1)$
$3m^3(m+1)$	$m^2(m+1)^2-1$	$\frac{1}{3}m^2(m^2+3m+5)-1$	$\frac{1}{3}m^2(m^2+3m+5)-2$	$\frac{1}{3}m^2(m^2+3m+2)$
$3m^2(2m^2+1)$	$(m^2-1)(2m^2+1)$	$\frac{1}{3}(2m^2-1)(m^2-1)$	$\frac{1}{3}(2m^4-8m^2+3)$	$\frac{1}{3}(2m^2-1)(m^2-1)$
$3m^2(m^2-1)$	$(m^2-1)^2-1$	$\frac{1}{3}m^2(m^2+2)-1$	$\frac{1}{3}m^2(m^2+2)-2$	$\frac{1}{3}m^2(m^2-1)$

4.8 Concluding remarks

We examined graphs, association schemes, and orthogonal arrays as possible sources of partial geometric designs. At the end of our search we focused on the orthogonal arrays associated with a particular family of three-class association schemes. However, as we mentioned in the Introduction, there are graphs that give rise to partial geometric designs but are not realized as relation graphs of association schemes. In fact, there are many such graphs obtained from orthogonal arrays. On the set of runs of an orthogonal array, by defining the adjacency of any two codewords according to their Hamming distance, we obtain many graphs that give rise to partial geometric designs. So as not to extend this paper much further, we shall close with just one example. As such examples are abundant, further research is required on the topic.

Example 88. Consider the $[7, 5]$ -code \mathcal{C} over \mathbb{F}_3 with generator matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

This code \mathcal{C} has weight distribution $(1, 0, 12, 34, 42, 96, 46, 12)$ and dual weight distribution $(1, 0, 0, 2, 0, 0, 6, 0)$.

Hence it gives an $OA(3^5, 7, 3, 2)$ with $\lambda = 3^3$. As before, the code \mathcal{C} (or any code that are equivalent to \mathcal{C}) define $X = \mathcal{C}$ and

$$\begin{aligned} R_0 &= \{(x, x) \mid x \in X\} \\ R_1 &= \{(x, y) \mid \delta_H(x, y) \in \{1, 4, 7\}\} \\ R_2 &= \{(x, y) \mid \delta_H(x, y) \in \{2, 5\}\} \\ R_3 &= \{(x, y) \mid \delta_H(x, y) \in \{3, 6\}\} \end{aligned}$$

Then the partition $\{R_i\}_{0 \leq i \leq 3}$ of $X \times X$ does not form an association scheme. However, the

adjacency matrices A_i of the graphs (X, R_i) for $i = 1, 2, 3$ satisfy the following identities:

$$A_1^3 = 1215A_1 + 486(J - A_1),$$

$$A_2^3 = 5589A_2 + 4860(J - A_2),$$

$$(A_3 + I)^3 = 2673(A_3 + I) + 1944(J - A_3 - I).$$

Thus, taking each of A_1, A_2 and $A_3 + I$ as the incidence matrix of a symmetric design, we get three partial geometric designs with parameters

$$(v, k; \alpha, \beta) = (243, 54; 486, 1215), (243, 108; 4860, 5589), (243, 81; 1944, 2673).$$

CHAPTER 5. SUMMARY AND DISCUSSION

5.1 General discussion

The connection between difference families and designs was established in Section 1.3. It was shown that certain difference families yield designs with well-behaved automorphism groups. In this dissertation we set out to answer the following question: Does every (named) design have a difference family analogue? We were able to answer this question in the affirmative for partial geometric designs. In Chapter 2, we introduced partial geometric difference families. We showed that the partial geometric designs admitting a group of automorphisms which acts regularly on the point set and semi-regularly on the block set are precisely those arising from partial geometric difference families. We then constructed infinite families of partial geometric difference families in Galois rings. In Chapter 3 we extended our study of partial geometric difference families. We gave a construction method that can be used to determine the existence or nonexistence of partial geometric designs having specified automorphisms. Finally, in Chapter 4, we examined the relationship between partial geometric designs and three class association schemes. Specifically, we described the parameter sets of certain three-class association schemes that give rise to partial geometric designs. We then provided examples of such association schemes coming from Hamming codes and certain orthogonal arrays of strength two.

5.2 Recommendations for future research

We were able to answer the question posed above for partial geometric designs but the general question still remains open. The designs produced by different types of difference families are used in a variety of applications. The designs coming from classical difference

families are used to produce binary sequences with two level autocorrelation and the designs coming from divisible difference families are used to produce optical orthogonal codes. This begs the question: Where can we apply the designs coming from partial geometric difference families? Finally in Chapter 4 we found that orthogonal arrays associated with a particular family of three-class association schemes are a source of partial geometric designs. However, we also gave examples of graphs that give rise to partial geometric designs but are not realized as relation graphs of association schemes. This raises the question: Can we characterize such graphs?

BIBLIOGRAPHY

- [1] K. T. Arasu. Sequences and arrays with desirable correlation properties. *Information Security, Coding Theory and Related Combinatorics*, 29:136–171, 2011.
- [2] K. T. Arasu, C. Ding, T. Helleseth, P. Kumar, and H. Martinsen. Almost difference sets and their sequences with optimal autocorrelation. *IEEE Trans. Inform. Theory*, 47(7):2934–2943, 2001.
- [3] E. Bannai and T. Ito. *Algebraic combinatorics. I. Association schemes*. Benjamin/Cummings, Menlo Park, CA, 1984.
- [4] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. Cambridge University Press, Cambridge, 1999.
- [5] G. Bhattacharyya. *Terwilliger algebras of wreath products of association schemes*. PhD thesis, Iowa State University, 2008.
- [6] G. Bhattacharyya, S.Y. Song, and R. Tanaka. On terwilliger algebras of wreath products of one-class association schemes. *J. Alg. Combin.*, 31(3):455–466, 2010.
- [7] R. C. Bose. On some connections between the design of experiments and information theory. *Bull. Internat. Statist. Inst.*, 38(4):257–271, 1961.
- [8] R. C. Bose, S. S. Shrikhande, and N. M. Singhi. Edge regular multigraphs and partial geometric designs with an application to the embedding of quasi-residual designs. *Colloquie Internazionale sulle Teorie Combinatorie*, 1:49–81, 1976.
- [9] A. E. Brouwer. *The CRC Handbook of Combinatorial Designs*, chapter Strongly Regular Graphs, pages 667–685. CRC Press, New York, 1996.

- [10] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Springer-Verlag, Berlin, 1989.
- [11] A. E. Brouwer and S. A. Hobart. Parameters of directed strongly regular graphs. <http://www.win.tue.nl/~aeb/>, 2014.
- [12] A. E. Brouwer, O. Olmez, and S. Y. Song. Directed strongly regular graphs from $1\frac{1}{2}$ -designs. *Europ. J Combin.*, 33(6):1174–1177, 2012.
- [13] M. Buratti. Recursive constructions for difference matrices and relative difference families. *J. Combin. Designs*, 6:165–182, 1998.
- [14] M. Buratti, Y. Wei, D. Wu, P. Fan, and M. Cheng. Relative difference families with variable block sizes and their related oocs. *IEEE Trans. Inf. Theory*, 57:7489–7497, 2011.
- [15] P. J. Cameron and J. H. van Lint. *Designs, Graphs, Codes and their Links*. Cambridge University Press, Cambridge, 1991.
- [16] Y. Chang and C. Ding. Constructions of external difference families and disjoint difference families. *Designs, Codes, and Cryptography*, 40:167–185, 2006.
- [17] F. R. K. Chung, J. A. Salehi, and V. K. Wei. Optical orthogonal codes: design, analysis, and applications. *IEEE Trans. Inform. Theory*, 35:595–604, 1989.
- [18] C. J. Colbourn and J. H. Dinitz, editors. *The CRC Handbook of Combinatorial Designs*. CRC Press, Boca Raton, 2006.
- [19] T. W. Cusick, C. Ding, and A. Renvall, editors. *Stream Ciphers and Number Theory*. North-Holland Elsevier, Amsterdam, The Netherlands, 1998.
- [20] J. A. Davis. Almost difference sets and reversible difference sets. *Arch Math*, 59:595–602, 1992.
- [21] Ph. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Research Reports Suppl.*, 10, 1973.

- [22] C. Ding. Cyclic codes from cyclotomic sequences of order four. *Finite Fields and Their Applications*, 23:8–34, 2013.
- [23] C. Ding, T. Helleseth, and K. Y. Lam. Several classes of sequences with three-level autocorrelation. *IEEE Trans. Inform. Theory*, 45:2606–2612, 1999.
- [24] C. Ding, T. Helleseth, and H. Martinsen. New families of binary sequences with optimal three-level autocorrelation. *IEEE Trans. Inform. Theory*, 47(1):428–433, 2001.
- [25] C. Ding, A. Pott, and Q. Wang. Constructions of almost difference sets from finite fields. *Designs, Codes, and Cryptography*, 72(3):581–592, 2014.
- [26] C. Ding and J. Yin. Construction of almost difference families. *Discrete Mathematics*, 308:4941–4954, 2008.
- [27] A. Duval. A directed graph version of strongly regular graphs. *J. Combin. Theory (A)*, 47:71–100, 1988.
- [28] S. Furino. Difference families from rings. *Discrete Mathematics*, 97:177–190, 1991.
- [29] J. M. Goethals and J. J. Seidel. Strongly regular graphs derived from combinatorial designs. *Canad. J. Math.*, 22:597–614, 1970.
- [30] S. W. Golomb. *Digital Communication With Space Application*. Prentice-Hall, Los Altos, CA, 1982.
- [31] A. S. Hedayat, N. J. A. Sloane, and J. Stufken. *Orthogonal Arrays: Theory and Applications*. Springer-Verlag, New York, 1999.
- [32] T. Helleseth and P. V. Kumar. *Handbook of Coding Theory*, chapter Sequences with low correlation. Elsevier, Amsterdam, The Netherlands, 1998.
- [33] B. Huang and D. Wu. Cyclotomic constructions of external difference families and disjoint difference families. *J. Combin. Designs*, 17:333–341, 2009.
- [34] D. Jungnickel and A. Pott. Perfect and almost perfect sequences. *Discrete Applied Mathematics*, 95:331–359, 1999.

- [35] S. Kageyama, G. M. Saha, and A. D. Das. Reduction of the number of associate classes of hypercubic association schemes. *Ann. Inst. Statist. Math.*, 30:115–123, 1978.
- [36] J. H. Kim and H. Y. Song. Existence of cyclic hadamard difference sets and its relation to binary sequences with ideal autocorrelation. *J. Commun. and Networks*, 1:14–18, 1999.
- [37] E. S. Kramer and D. M. Mesner. t -designs on hypergraphs . *Discrete Mathematics*, 15:263–296, 1976.
- [38] D. L. Kreher and S. P. Radziszowski. The existence of simple $6 - (14, 7, 4)$ designs. *J. Combin. Theory, Series A*, 43:237–243, 1986.
- [39] Q. Lu and D. Wu. Constructions of (q, k, λ, t, q) almost difference families . *Frontiers of Mathematics in China*, 9:377–386, 2014.
- [40] S. L. Ma. Partial difference sets. *Discrete Mathematics*, 52:75–89, 1984.
- [41] S. L. Ma. A survey of partial difference sets. *Designs, Codes, and Cryptography*, 4:221–261, 1994.
- [42] J. L. Massey and P. Mathys. The collision channel without feedback. *IEEE Trans. Inf. Theory*, 31:192–204, 1985.
- [43] A. Neumaier. $t_{\frac{1}{2}}$ -designs. *J. Combin. Theory, Series A*, 28(3):226–248, 1980.
- [44] K. Nowak, O. Olmez, and S. Y. Song. Partial geometric difference families. *J. Combin. Designs*, to appear, 10.1002/jcd.21416 2014.
- [45] W. Ogata, K. Kurosawa, D. R. Stinson, and H. Saido. New combinatorial designs and their applications to authentication codes and secret sharing schemes. *Discrete Mathematics*, 279:383–405, 2004.
- [46] O. Olmez. Symmetric $1\frac{1}{2}$ -designs and $1\frac{1}{2}$ -difference sets. *J. Combin. Designs*, 22(6):252–269, 2014.
- [47] O. Olmez and S. Y. Song. Some families of directed strongly regular graphs obtained from certain finite incidence structures. *Graphs and Combinatorics*, 30:1529–1549, 2014.

- [48] J. A. Salehi. Emerging optical code-division multiple-access communications systems. *IEEE Network*, 3:31–39, 1989.
- [49] J. A. Salehi and M. P. Vecchi. Neuromorphic networks based on sparse optical orthogonal codes. *Neural Information Processing Systems-Natural and Synthetic*, 3:814–823, 1988.
- [50] J. Singer. A theorem on finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43:377–385, 1938.
- [51] N. J. A Sloane and J. G. Thompson. The nonexistence of a certain Steiner system $s(3, 12, 112)$. *J. Combin. Theory, Series A*, 30:209–236, 1981.
- [52] E. Spence. Strongly regular graphs. <http://www.maths.gla.ac.uk/~es/>, 2014.
- [53] D. R. Stinson. *Combinatorial Designs: Construction and Analysis*. Springer-Verlag, New York, 2004.
- [54] E. van Dam. Three-class association schemes. *J. Alg. Combin.*, 10(1):67–107, 1999.
- [55] E. R. van Dam and E. Spence. Combinatorial designs with two singular values ii. partial geometric designs. *Linear Algebra and its Applications*, 396:303–316, 2005.
- [56] X. Wang and J. Wang. A note on cyclic difference families. *Discrete Mathematics*, 311:628–633, 2001.
- [57] X. Wang and J. Wang. Partitioned difference families and almost difference sets. *Journal of Statistical Planning and Inference*, 141:1899–1909, 2011.
- [58] R. M. Wilson. Cyclotomy and difference families in elementary abelian groups. *J. Number Theory*, 4:17–47, 1972.
- [59] Q. Xiang. Recent progress in algebraic design theory. *Finite Field and Their Applications*, 11:622–653, 2005.
- [60] H. Zhao. On balanced optimal $(18u, \{3, 4\}, 1)$ optical orthogonal codes. *J. Combin. Designs*, 20:290–303, 2012.