分类号： 05B30 单位代码：

学 号： 11335044

浙江大学

博士学位论文

中文论文题目： 关于差集的关联结构及其应用

英文论文题目： **Incidence Structures Related to Difference Sets and Their Applications**

申请人姓名：Jerod Evan Michel

指导教师：Feng Tao

专业名称：Mathematics

研究方向：Combinatorics

所在学院：Zhejiang University

论文提交日期_____

Dedication

I would like to dedicate the writing of this thesis to my wife, Gao Rong, without whose help I would not have been able.

Acknowledgement

I would like to take this opportunity to express my gratitude for those who aided me with all of the various aspects of conducting research. First and foremost, I would like to thank Dr. Feng Tao for his guidance, patience, and words of encouragement which have, more than once, given me hope to complete my graduate studies. I would also like to thank my committee members for their efforts and contributions, and the School of Mathematics at Zhejiang University for providing me with excellent facilities to carry out research. Also, I would like to express my gratitude for the scholarship provided by the China Scholarship Council.

Abstract

In this thesis we study incidence structures that are related to difference sets and almost difference sets. We first discuss t-adesigns, which were coined by Cunsheng Ding in "Codes from Difference Sets" (2015). It is clear that 2-adesigns are partially balanced incomplete block designs which naturally arise in many combinatorial and statistical problems. We discuss some of their basic properties and give several constructions of 2-adesigns (some of which correspond to new almost difference sets and some to new almost difference families), as well as two constructions of 3-adesigns. We discuss basic properties of the incidence matrices and make an initial investigation into the codes which they generate. We find that many of the codes have good parameters in the sense they are optimal or have relatively high minimum distance. We then turn our discussion to partial geometric difference sets which were coined by Oktay Olmez in "Symmetric $1\frac{1}{2}$-Designs and $1\frac{1}{2}$-Difference Sets" (2012), and partial geometric difference families, which were coined by Kathleen Nowak et al. in "Partial Geometric Difference Families" (2014). Using Galois rings and Galois fields, we construct several infinite classes of partial geometric difference sets, and partial geometric difference families, with new parameters. Furthermore, these partial geometric difference sets (and partial geometric difference families) correspond to new infinite families of directed strongly regular graphs. We also discuss some of the links between partially balanced designs, 2-adesigns and partial geometric designs, and make an investigation into when a 2-adesign is a partial geometric design.

目　　次

Chapter 1. General Overview and Introduction

In this chapter we give a brief history of the theory of combinatorial designs and related combinatorial objects. We then give a brief explanation of our motivations as well as an overview of the thesis.

The conception of combinatorial designs lies in the work of Fisher and Yates in the 1930's [27], [51]. Combinatorial designs have an important impact on coding theory and graph theory. For instance, Delsarte's thesis presented many powerful uses of combinatorial designs toward coding theory and graph theory [15]. Combinatorial designs have extensive applications in many fields, including finite geometry [16], [30], design of experiments [9], [28], cryptography [13], [47], and authentication codes and secret sharing schemes [40], [47].

A design is a pair $(X, \mathcal{A})$ where X is a set of elements called *points*, and $\mathcal{A}$ is a collection (i.e. a multiset) of nonempty subsets of X called *blocks*. If v, k, λ and t are positive integers such that $v \geq k \geq 2$, and $t \geq 1$, a $t-(v, k, \lambda)$ design is a design $(X, \mathcal{A})$ where $|X| = v$, each block contains exactly k points, and every t-subset of points of X is contained in exactly λ blocks. A $2-(v, k, \lambda)$ design if often referred to as a (v, k, λ) balanced incomplete block design, or a (v, k, λ)-BIBD. Further reading on combinatorial designs can be found in [6], [12] and [47].

Difference sets are a powerful tool for obtaining new disigns. If G is an (additive) group of order v, let k and λ be integers such that $v > k \geq 2$. Then a (v, k, λ) *difference set* in G is a subset $D \subseteq G$ such that $|D| = k$, and the multiset $[x - y \mid x, y \in D, x \neq y]$ contains every element in $G \setminus \{0\}$ exactly λ times. The use of cyclic difference sets and methods for the construction of symmetric block designs date back to R. C. Bose and his seminal paper in 1939 [5]. Further reading on difference sets can be found in [21], [32] and [36].

One generalization of the difference set is the almost difference set. Two different types of almost difference sets were introduced by Davis (1992) [14] and Ding (1994) [18]. The definition we will use is a unified version of the two formulated by Ding et al. in 2001 [22]. If G is an (additive) group of order v, let k, λ and t be integers such that $v > k \geq 2$ and $t \geq 1$. A

(v, k, λ, t) *almost difference set* in G is a subset $D \subseteq G$ such that $|D| = k$ and the multiset $[x - y \mid x, y \in D, x \neq y]$ contains t elements of $G \setminus \{0\}$ exactly λ times, and $v - t - 1$ elements exactly $\lambda + 1$ times. Further reading on almost difference sets can be found in [21], [23] and [38]. Difference sets [32] and almost difference sets [38] also have applications in many areas such as digital communications [22], [54], sequence design [48], [52], and CDMA and cryptography [13].

Recently, several generalizations of combinatorial designs related to difference sets and almost difference sets have been introduced and shown to be applicable to coding theory and graph theory. Ding and Yin, in 2008, introduced the almost difference family. Constructions and applications of almost difference families can be found in [24] and [49]. Ding, in 2015, coined the t-adesign (or t-almost design). Constructions of t-adesigns and applications to coding theory can be found in [21], [24] and [35].

Olmez, in 2013, introduced the partial geometric difference set. These give a way of constructing new partial geometric designs, which are geometric objects coined by Bose et al. in 1976 [8] and studied further by Neumaier in 1980 [37]. It is clear that partial geometric designs have several applications in graph theory, coding theory and cryptography [7], [9], [41], [43]. It was shown by Brouwer et al. in [9] that directed strongly regular graphs can be obtained from partial geometric designs. In [43], Olmez showed that certain partial geometric difference sets can be used to construct plateaued functions. Constructions of new partial geometric designs from symplectic geometry over finite fields were given by Z. Chai et al. in [11] (also see [53]). Nowak et al., in 2014, introduced the partial geometric difference family. Constructions and applications to graph theory can be found in [34] and [39].

This dissertation will provide new constructions of t-adesigns and discuss the parameters of their related codes. We will also give new constructions of partial geometric difference sets and partial geometric difference families as well as discuss their associated graphs, all of which are directed strongly regular graphs with new parameters.

The organization of this dissertation is as follows. In Chapter 2, we give preliminary facts and definitions on the theory of finite incidence structures, difference sets, linear codes, strongly regular graphs and directed strongly regular graphs. In Chapter 3 we discuss t-adesigns and give several new constructions as well as an investigation of their related codes. In Chapter 4 we discuss partial geometric difference sets and partial geometric difference families and give several new constructions. We also give a discussion of their associated directed strongly regular graphs.

Chapter 2. Preliminaries

0.1 Incidence Structures and Partial Geometric Designs

An *incidence structure* is a pair $(V, \mathcal{B})$ where V is a finite set of points and $\mathcal{B}$ is a finite set of blocks composed of points of V. For a given point $u \in V$, its *replication number* is the number of blocks of $\mathcal{B}$ in which it occurs, and is denoted by r_u. Given two distinct points $u, w \in V$, their *index* is the number of blocks in which they occur together, and is denoted r_{uw}. A *tactical configuration* is an incidence structure $(V, \mathcal{B})$ where the cardinalities of blocks in $\mathcal{B}$ and the replication numbers of points in V are both constant.

Let $(V, \mathcal{B})$ be a tactical configuration where $|V| = v$, each block has cardinality k, and each point has replication number r. We call a member (u, B) of $V \times \mathcal{B}$ a *flag* if $u \in B$, and an *antiflag* if $u \notin B$. For each point $u \in V$ and each block $B \in \mathcal{B}$, let $s(u, B)$ denote the number of flags $(w, C) \in V \times \mathcal{B}$ such that $w \in B \setminus \{u\}, u \in C$ and $C \neq B$. If there are integers α' and β' such that

$$s(u, B) = \begin{cases} \alpha', \text{ if } u \notin B, \\ \beta', \text{ if } u \in B, \end{cases}$$

as (u, B) runs over $V \times \mathcal{B}$, then we say that $(V, \mathcal{B})$ is a *partial geometric design* with parameters $(v, k, r; \alpha', \beta')$.

0.2 Difference Sets and Almost Difference Sets

Let G be a finite additive group with identity 0. Let k and λ be positive integers such that $2 \leq k < v$. A (v, k, λ) *difference set* in G is a subset $D \subseteq G$ that satisfies the following properties:

- $|D| = k$,
- the multiset $\{x - y \mid x, y \in D, x \neq y\}$ contains every member of $G \setminus \{0\}$ exactly λ times.

Almost difference sets are a generalization of difference sets. A (v, k, λ, t) *almost difference set* in G is a subset $D \subseteq G$ that satisfies the following properties:

- $|D| = k$,
- the multiset $\{x - y \mid x, y \in D, x \neq y\}$ contains t members of $G \setminus \{0\}$ which appear λ times and $v - 1 - t$ members of $G \setminus \{0\}$ which appear $\lambda + 1$ times.

Let G be an additive group of order v. A k-element subset $D \subseteq G$ has *difference levels* $\mu_1 < \cdots < \mu_s$ if there exist integers $t_1, ..., t_s$ such that the multiset

$$M = \{g - h \mid g, h \in D\}$$

contains exactly t_i members of $G \setminus \{0\}$ each with multiplicity μ_i for all i, $1 \leq i \leq s$. We will denote the t_i members of the multiset M with multiplicity μ_i by T_i. Note that the T_i's form a partition of $G \setminus \{0\}$. It is easy to see that in the case where $s = 1$, D is a difference set [32], and in the case where $s = 2$ and $\mu_2 = \mu_1 + 1$, D is an almost difference set [38]. In this correspondence we are concerned only with those structures having two difference levels, and all groups are assumed to be additive. The basic equation describing a k-element subset $D \subseteq G$ with difference levels $\mu_1 < \mu_2$ is given by

$$\mu_1 t + \mu_2(v - 1 - t) = k(k - 1). \tag{0-1}$$

Let V be a v-set and $\mathcal{B}$ a collection of subsets of V, called blocks, each having cardinality k. If there are positive integers $\mu_1 < \mu_2$ such that every subset of V of cardinality t is incident with exactly μ_i blocks for $i = 1$ or 2, and for each $i, i = 1, 2$, there exists a subset of V of cardinality t that is incident with exactly μ_i blocks, then we say that the incidence structure $(V, \mathcal{B})$ has *t-levels* $\mu_1 < \mu_2$. We denote $|\mathcal{B}|$ by b. An incidence structure $(V, \mathcal{B})$ is called *symmetric* if $b = v$. In the case where $s = 2$, $(V, \mathcal{B})$ is a partially balanced incomplete block design, and if $\mu_2 = \mu_1 + 1$, we call $(V, \mathcal{B})$ a t-(v, k, μ_1) *adesign* (or simply a t-*adesign*), which was coined by Ding in [21]. It is easy to see that in the case where $s = 1$, $(V, \mathcal{B})$ is simply a t-design [47].

We call the set $\{D + g \mid g \in G\}$ of translates of D, denoted by $Dev(D)$, the *development* of D. We have the following lemmas whose proofs are omitted as they are simple counting exercises.

Lemma 0.2.1. *Let D be a (v, k, λ) almost difference set in an Abelian group G. Then $(G, Dev(D))$ is a 2-(v, k, λ) adesign.*

Let $(V, \mathcal{B})$ be an incidence structure with t-levels $\mu_1 < \mu_2$. Let A be a v by b matrix whose rows and columns are indexed by points and blocks respectively and whose (i, j)-th entry is 1 if the point corresponding to the ith row is incident with the block corresponding to the jth row, and 0 otherwise. We call A the *incidence matrix* of $(V, \mathcal{B})$. We will denote the $n \times n$ identity and all-one matrices by I_n and J_n respectively, or, when it is clear from the context, simply by I and J.

Lemma 0.2.2. *Let D be a k-subset of an Abelian group G of cardinality v with the two difference levels $\mu_1 < \mu_2$. Let A be the $v \times v$ incidence matrix of the symmetric incidence structure $(G, Dev(D))$. Then*

$$A^T A = AA^T = kI + \mu_1 A_1 + \mu_2(J - A - I). \tag{0-2}$$

0.3 Partial Geometric Difference Sets and Partial Geometric Difference Families

Let G be a finite (additive) Abelian group and $S \subset G$. Let $\Delta(S)$ denote the multiset $\{x - y \mid x, y \in S\}$. For a family $\mathcal{S} = \{S_1, ..., S_n\}$ of subsets of G, we let $\Delta(\mathcal{S})$ denote the multiset union $\bigsqcup_{i=1}^{n} \Delta(S_i)$. For a subset $S \subset G$ we let $\delta_S(z)$ denote $|\{(x, y) \in S \times S \mid z = x - y\}|$. For a family $\mathcal{S} = \{S_1, ..., S_n\}$ of subsets of G we let $\delta_{S_i}(z)$ denote $|\{(x, y) \in S_i \times S_i \mid z = x - y\}|$.

Let v, k and n be integers with $v > k > 2$. Let G be a group of order v. Let $\mathcal{S} = \{S_1, ..., S_n\}$ be a collection of distinct k-subsets of G. If there are constants α, β such that for each $x \in G$ and each $i \in \{1, ..., n\}$,

$$\sum_{y \in S_i} \sum_{i=1}^{n} \delta_{S_i}(x - y) = \begin{cases} \alpha, \text{ if } x \notin S_i, \\ \beta, \text{ if } x \in S_i, \end{cases}$$

then we say $\mathcal{S}$ is a *partial geometric difference family* with parameters $(v, k, n; \alpha, \beta)$. For details on the relationship between partial geometric difference families and difference families the reader is referred to [39]. When $n = 1$ and $\mathcal{S} = \{S\}$, we simply say that S is a *partial geometric difference set* with parameters are $(v, k; \alpha, \beta)$. For details on the relationship between partial geometric difference sets and difference sets the reader is referred to [42].

Again let G be a group and $\mathcal{S} = \{S_1, ..., S_n\}$ a collection of distinct k-subsets of G. We call the multiset union of translates $\bigsqcup_{i=1}^{n} \{S_i + g \mid g \in G\}$ the *development* of $\mathcal{S}$, and denote it by $Dev(\mathcal{S})$. By the proof of Theorem 3 in [39] we have the following.

Theorem 0.3.1. *Let $\mathcal{S} = \{S_1, ..., S_n\}$ be a collection 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 $(v, k, kn; \alpha', \beta')$ where $\alpha' = \sum_{y \in S_i} \sum_{i=1}^{n} \delta_{S_i}(x - y)$ for $x \notin S_i$, and $\beta' = \sum_{y \in S_i \setminus \{x\}} \sum_{i=1}^{n} (\delta_{S_i}(x - y) - 1)$ for $x \in S_i$ (see Remark 0.3.1).*

Remark 0.3.1. *The parameters for the corresponding partial geometric designs seem to disagree in Lemma* 2.4 *of* [42] *and Theorem* 3 *of* [39]. *To see this, the reader should compare Definition* 2.2 *of* [42] *to Definition* 1 *of* [39].

0.4 Strongly Regular Graphs and Digraphs

For a more detailed introduction to directed strongly regular graphs the reader is referred to [41] and [33]. In this paper all graphs are assumed to be loopless and simple. Let Γ be an undirected graph with v vertices. Let A denote the adjacency matrix of Γ. Then Γ is called a *strongly regular graph* with parameters (v, k, λ, μ) if

$$A^2 = kI + \lambda A + \mu(J - I - A) \text{ and } AJ = JA = kJ.$$

A directed graph Γ with adjacency matrix A is said to be a *directed strongly regular graph* with parameters (v, k, t, λ, μ) if

$$A^2 = tI + \lambda A + \mu(J - I - A) \text{ and } AJ = JA = kJ.$$

The following theorems were proved in [9].

Theorem 0.4.1. *Let $(V, \mathcal{B})$ be a tactical configuration, and let Γ be the directed graphs with vertex set*

$$\mathcal{V} = \{(u, B) \in V \times \mathcal{B} \mid u \notin B\}$$

and adjacency given by

$$(u, B) \to (w, C) \text{ if and only if } u \in C.$$

Then Γ is directed strongly regular if and only if $(V, \mathcal{B})$ is a partial geometric design.

Theorem 0.4.2. *Let $(V, \mathcal{B})$ be a tactical configuration, and let Γ be the directed graphs with vertex set*

$$\mathcal{V} = \{(u, B) \in V \times \mathcal{B} \mid u \in B\}$$

and adjacency given by

$$(u, B) \to (w, C) \text{ if and only if } (u, B) \neq (w, C) \text{ and } u \in C.$$

Then Γ is directed strongly regular if and only if $(V, \mathcal{B})$ is a partial geometric design.

0.5 Linear Codes

A linear binary *code* C of *length* n and *dimension* k (or simply an $[n, k]$ code), is a k-dimensional linear subspace of the n-dimensional binary vector space $\mathbb{F}_2^n$. The *dual* $C^\perp$ of an $[n, k]$ code C is the $[n, n-k]$ code that is the orthogonal space of C with respect to the inner product of the binary field. Any basis of C is called a *generator matrix* of C, and any basis of $C^\perp$ is called a *parity check matrix* of C. The Hamming distance between two vectors $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ is the number of indices i such that $x_i \neq y_i$. The Hamming *weight* of a vector is the number of its nonzero coordinates. The minimum distance d of a code is smallest possible distance between pairs of distinct codewords. An $[n, k]$ code C is *self-orthogonal* if $C \subseteq C^\perp$. An $[n, k]$ code C is *optimal* if, given its length and dimension, has the largest possible minimum distance. The best codes for a given length and dimension can be found in the code tables in [29].

0.6 Group Ring Notation

For any finite group G the *group ring* $\mathbb{Z}[G]$ is defined as the set of all formal sums of elements of G, with coefficients in $\mathbb{Z}$. The operations "+" and "·" on $\mathbb{Z}[G]$ are given by

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

and

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{g,h \in G} a_g b_h (g + h).$$

where are $a_g, b_g \in \mathbb{Z}$.

The group ring $\mathbb{Z}[G]$ is a ring with multiplicative identity $\mathbf{1} = \underline{Id}$, where Id is the identity element of G, and for any subset $X \subset G$, we denote by $\underline{X}$ the sum $\sum_{x \in X} x$, and we denote by $\underline{X}^{-1}$ the sum $\sum_{x \in X} (-x)$.

0.7 Cyclotomic Classes and Cyclotomic Numbers

Let q be a prime power, and γ a primitive element of $\mathbb{F}_{q^2}$. The *cyclotomic classes* of order e are given by $C_i^e = \gamma^i \langle \gamma^e \rangle$ for $i = 0, 1, ..., e-1$. Define $(i,j)_e = |C_i^e \cap (C_j^e + 1)|$. It is easy to see there are at most e^2 different cyclotomic numbers of order e. When it is clear from the context, we simply denote $(i,j)_e$ by (i,j). We will need the following lemma.

Lemma 0.7.1. [38] *Let $q = ef + 1$ be a prime power for some positive integers e and f. In the group ring $\mathbb{Z}[\mathbb{F}_q]$ we have*

$$\underline{C_i^e}\underline{C_j^e} = a_{ij}\mathbf{1} + \sum_{k=0}^{e-1}(j-i, k-i)_e \underline{C_k^e}$$

where

$$a_{ij} = \begin{cases} f, \text{ if } m \text{ is even and } j = i, \\ f, \text{ if } m \text{ is odd and } j = i + \frac{e}{2}, \\ 0, \text{ otherwise.} \end{cases}$$

Chapter 3. Adesigns

0.8 Introduction

We will assume some familiarity with combinatorial design theory. A t-(v, k, λ) *design* (with $v > k > t > 0$) is an incidence structure $(V, \mathcal{B})$ where V is a set of v points and $\mathcal{B}$ is a collection of k-subsets of V (called blocks), such that any t-subset of V is contained in exactly λ blocks. When $t = 2$, a t-design is sometimes referred to as a balanced incomplete block design. Denoting the number of blocks by b and the number of blocks containing a given point by r, the identities

$$bk = vr$$

and

$$r(k-1) = (v-1)\lambda$$

restrict the possible parameter sets. A t-(v, k, λ) design in which $b = v$ and $r = k$ is called *symmetric*, and any two blocks meet in λ points. A t-(v, k, λ) design is called *quasi-symmetric* if there are exactly two intersection numbers among pairs of blocks. The *dual* $(V, \mathcal{B})^{\perp}$ of an incidence structure $(V, \mathcal{B})$ is the incidence structure $(\mathcal{B}, V)$ with the roles of points and blocks interchanged. A symmetric incidence structure always has the same parameters as its dual.

We will also assume familiarity with difference sets and almost difference sets. For the convenience of the reader we recall the following definitions. Let G be a finite additive group with identity 0. Let k and λ be positive integers such that $2 \leq k < v$. A (v, k, λ) *difference set* in G is a subset $D \subseteq G$ that satisfies the following properties:

- $|D| = k$,
- the multiset $\{x - y \mid x, y \in D, x \neq y\}$ contains every member of $G \setminus \{0\}$ exactly λ times.

Almost difference sets are a generalization of difference sets. A (v, k, λ, t) *almost difference set* in G is a subset $D \subseteq G$ that satisfies the following properties:

- $|D| = k$,
- the multiset $\{x - y \mid x, y \in D, x \neq y\}$ contains t members of $G \setminus \{0\}$ which appear λ times and $v - 1 - t$ members of $G \setminus \{0\}$ which appear $\lambda + 1$ times.

One motivation for studying t-adesigns is in constructing linear codes. Also, due to their having extensive applications, it is worthwhile to study the combinatorial objects arising from almost difference sets. In Section 0.16 we give three constructions of 2-adesigns from quadratic residues, several constructions of 2-adesigns which are almost difference families are given in Section 0.17, and some constructions of 2-adesigns from symmetric t-designs are given in Section 0.11. In Section 0.18 we discuss 3-adesigns and two constructions are given, and in Section 0.13 we discuss the codes of t-adesigns (and some related structures), and include some of the codes with good parameters in a table. Section 0.19 closes the chapter.

0.9 Constructions of 2-adesigns from Quadratic Residues

Cyclotomic classes have proven to be a powerful tool for constructing difference sets and almost difference sets, e.g. see [22], [23], [38]. Let q be a prime power, $\mathbb{F}_q$ a finite field, and e a divisor of $q - 1$. Denote $\frac{q-1}{e}$ by f. For a primitive element α of $\mathbb{F}_q$ let D_0^e denote $\langle \alpha^e \rangle$, the multiplicative group generated by α^e, and let

$$D_i^e = \alpha^i D_0^e, \text{ for } i = 1, 2, ..., e - 1.$$

We call D_i^e the *cyclotomic classes* of order e. The *cyclotomic numbers* of order e are defined to be

$$(i, j)_e = \left| D_i^e \cap (D_j^e + 1) \right|.$$

It is easy to see there are at most e^2 different cyclotomic numbers of order e. When it is clear from the context, we simply denote $(i, j)_e$ by (i, j). The cyclotomic numbers (h, k) of order e have the following properties ([17]):

$$(h, k) = (e - h, k - h), \tag{0-3}$$

$$(h, k) = \begin{cases} (k, h), & \text{if } f \text{ even}, \\ (k + \frac{e}{2}, h + \frac{e}{2}), & \text{if } f \text{ odd}. \end{cases} \tag{0-4}$$

Our first three constructions make use of quadratic residues. We will need the following lemma [17].

Lemma 0.9.1. *If $q \equiv 1$ (mod 4) then the cyclotomic numbers of order two are given by*

$$\begin{aligned}(0,0) &= \frac{q-5}{4},\\ (0,1) &= (1,0) = (1,1) = \frac{q-1}{4}.\end{aligned}$$

If $q \equiv 3$ (mod 4) then the cyclotomic numbers of order two are given by

$$\begin{aligned}(0,1) &= \frac{q+1}{4},\\ (0,0) &= (1,0) = (1,1) = \frac{q-3}{4}.\end{aligned}$$

We are ready to give our first construction.

Theorem 0.9.1. *Let q be an odd prime power and α a primitive member of $\mathbb{F}_q$. Define $C_i = \{z \in \mathbb{Z}_{q-1} \mid \alpha^z \in D_i^2 - 1\}$ for $i = 0, 1$. Then the incidence structure $(\mathbb{Z}_{q-1} \cup \{\infty\}, Dev^\infty(C_0) \cup Dev(C_1))$, where $Dev^\infty(C_0)$ denotes the blocks of $Dev(C_0)$ each modified by adjoining the point "∞", is a 2-$(q, \frac{q-1}{2}, \frac{q-5}{2})$ adesign.*

Proof: We will denote $\{\alpha^z \mid z \in C_i\}$ by α^{C_i}. For $w \in \mathbb{Z}_{q-1}$ we have

$$|C_0 \cap (C_0 + w)| = \left|\alpha^{C_0} \cap \alpha^{C_0+w}\right|$$

which, since α^z is nonzero and

$$|((D_0^2 - 1) \setminus \{0\}) \cap ((D_0^2 - \alpha^w) \setminus \{0\})| = |((D_0^2 \setminus \{1\}) - 1) \cap ((\alpha^w D_0^2 \setminus \{\alpha^w\}) - \alpha^w)|,$$

is

$$\begin{cases} |(D_0^2 \setminus \{1\}) \cap (D_0^2 \setminus \{\alpha^w\} + (1 - \alpha^w))| & \text{if } w \text{ even},\\ |(D_0^2 \setminus \{1\}) \cap (D_1^2 \setminus \{\alpha^w\} + (1 - \alpha^w))| & \text{if } w \text{ odd}.\end{cases}$$

Since $\alpha^w(1 - \alpha^w)^{-1} = (1 - \alpha^w)^{-1} - 1$, this becomes

$$\begin{cases} |(D_0^2 \setminus \{(1 - \alpha^w)^{-1}\}) \cap (D_0^2 \setminus \{(1 - \alpha^w)^{-1} - 1\} + 1)| & \text{if } w \text{ even},\\ |(D_0^2 \setminus \{(1 - \alpha^w)^{-1}\}) \cap (D_1^2 \setminus \{(1 - \alpha^w)^{-1} - 1\} + 1)| & \text{if } w \text{ odd},\end{cases}$$

which simplifies to

$$\begin{cases} |D_0^2 \cap (D_0^2+1) \setminus \{(1-\alpha^w)^{-1}\}| & \text{if } w \text{ even}, \\ |D_0^2 \cap (D_1^2+1) \setminus \{(1-\alpha^w)^{-1}\}| & \text{if } w \text{ odd}. \end{cases}$$

There are four cases depending on the parity of w and whether $(1-\alpha^w)^{-1} \in D_0^2$ or D_1^2. By Lemma 0.9.1 we have

$$|C_0 \cap (C_0+w)| = \begin{cases} (0,0)-1 & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_0^2, \\ (0,0) & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ (0,1)-1 & \text{if } w \text{ odd and } (1-\alpha^w)^{-1} \in D_0^2, \\ (1,0)-1 & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_0^2. \end{cases}$$

Thus if $q \equiv 1 (\text{mod } 4)$ then

$$|C_0 \cap (C_0+w)| = \begin{cases} \frac{q-9}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_0^2, \\ \frac{q-5}{4} & \text{otherwise}, \end{cases}$$

and if $q \equiv 3 (\text{mod } 4)$ then

$$|C_0 \cap (C_0+w)| = \begin{cases} \frac{q-3}{4} & \text{if } w \text{ odd and } (1-\alpha^w)^{-1} \in D_0^2 \text{ or if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-7}{4} & \text{otherwise}. \end{cases}$$

Also, we have

$$|C_1 \cap (C_1+w)| = \begin{cases} |D_1^2 \cap (D_1^2+1) + (1-\alpha^w)| & \text{if } w \text{ even}, \\ |D_1^2 \cap (D_1^2+1) + (1-\alpha^w)| & \text{if } w \text{ odd}. \end{cases}$$

Thus if $q \equiv 1 (\text{mod } 4)$ then

$$|C_1 \cap (C_1+w)| = \begin{cases} \frac{q-5}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-1}{4} & \text{otherwise}. \end{cases}$$

and if $q \equiv 3 (\text{mod } 4)$ then

$$|C_1 \cap (C_1+w)| = \begin{cases} \frac{q+1}{4} & \text{if } w \text{ odd and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-3}{4} & \text{otherwise}. \end{cases}$$

We need to compute the number of blocks of $(\mathbb{Z}_{q-1}, Dev(C_0) \cup Dev(C_1))$ in which an arbitrary pair of points appear. Consider the incidence structures $(\mathbb{Z}_{q-1}, Dev(C_i))$ for $i = 0, 1$. Let $C_i^{\perp}, (C_i +$

$w)^{\perp}$ denote the points of the dual structures $(Dev(C_i), \mathbb{Z}_{q-1})$ corresponding to the blocks $C_i, C_i + w$. We have that $(\mathbb{Z}_{q-1}, Dev(C_i))$ is a symmetric incidence structure and by Lemma 0.2.2 the number of blocks of $(\mathbb{Z}_{q-1}, Dev(C_0) \cup Dev(C_1))$ in which the points $C_i^{\perp}, (C_i + w)^{\perp}$ appear is, if $q \equiv 1 (\text{mod } 4)$,

$$\begin{cases} \frac{q-9}{4} + \frac{q-1}{4} = \frac{2q-10}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_0^2, \\ \frac{q-5}{4} + \frac{q-5}{4} = \frac{2q-10}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-5}{4} + \frac{q-1}{4} = \frac{2q-6}{4} & \text{otherwise,} \end{cases}$$

and if $q \equiv 3 (\text{mod } 4)$,

$$\begin{cases} \frac{q-3}{4} + \frac{q-3}{4} = \frac{2q-6}{4} & \text{if } w \text{ odd and } (1-\alpha^w)^{-1} \in D_0^2, \\ \frac{q-7}{4} + \frac{q+1}{4} = \frac{2q-6}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-7}{4} + \frac{q-3}{4} = \frac{2q-10}{4} & \text{otherwise.} \end{cases}$$

It is easy to see that the block sizes of the incidence structures $(\mathbb{Z}_{q-1}, Dev(C_0))$ and $(\mathbb{Z}_{q-1}, Dev(C_1))$ are $\frac{q-3}{2}$ and $\frac{q-1}{2}$ respectively and that the number of blocks containing a given point in $(\mathbb{Z}_{q-1}, Dev(C_0))$ is $\frac{2q-6}{4}$. Then the incidence structure $(\mathbb{Z}_{q-1} \cup \{\infty\}, Dev^{\infty}(C_0) \cup Dev(C_1))$, where $Dev^{\infty}(C_0)$ denotes the blocks of $Dev(C_0)$ each modified by adjoining the point ∞, is a 2-adesign. □

Note that appending the symbol "∞" to certain blocks in a combinatorial design has been done before, e.g. see Chapter 8 of [31]. Our constructions in this section also use this symbol only, rather than extending complimentary blocks to obtain a 3-design, we first consider various other ways of obtaining a set of blocks where any two have lengths differing by at most one, and then extend the shorter blocks to obtain a 2-adesign.

Example 0.9.1. *With $q = 11$ and C_i defined as in Theorem 0.9.1 we get that $(\mathbb{Z}_{10} \cup \{\infty\}, Dev^{\infty}(C_0) \cup Dev(C_1))$ is a 2-$(10, 5, 3)$ adesign with blocks:*

$$\begin{array}{ccccc} \{0,1,3,4,8\} & \{1,3,4,6,7\} & \{2,4,5,7,8\} & \{0,2,3,7,9\} & \{3,5,6,8,9\} \\ \{0,1,5,7,8\} & \{1,2,4,5,9\} & \{0,2,3,5,6\} & \{0,4,6,7,9\} & \{1,2,6,8,9\} \\ \{2,5,6,7,\infty\} & \{0,1,6,9,\infty\} & \{3,6,7,8,\infty\} & \{1,4,5,6,\infty\} & \{0,1,2,7,\infty\} \\ \{1,2,3,8,\infty\} & \{2,3,4,9,\infty\} & \{4,7,8,9,\infty\} & \{0,5,8,9,\infty\} & \{0,3,4,5,\infty\} \end{array}$$

The next two constructions will use the following lemmas.

Lemma 0.9.2. [1] *Let p be a prime. The number of pairs of consecutive quadratic residues mod p is*

$$N(p) = \frac{1}{4}(p - 4 - (-1)^{\frac{p-1}{2}})$$

and the number of pairs of consecutive quadratic non-residues mod p is

$$N'(p) = \frac{1}{4}(p - 2 + (-1)^{\frac{p-1}{2}}).$$

In the sequel we will sometimes use the following lemma without making reference to it.

Lemma 0.9.3. [3] *Let $p \equiv 1(mod\ 4)$ be a prime. Then the set of quadratic residues mod p forms a $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{2})$ almost difference set in $\mathbb{Z}_p$.*

Lemma 0.9.4. *Let $p \equiv 1(mod\ 4)$ be a prime and $D \subseteq \mathbb{Z}_p$ be the set of quadratic residues. Two distinct points $x, y \in D$ occur together in exactly $\frac{p-5}{4}$ translates of D if and only if $x - y$ is a quadratic residue. Dually, $D + x$ and $D + y$ are translates of D with $x - y \in D$ if and only if $|(D + x) \cap (D + y)| = \frac{p-5}{4}$.*

Proof: Let $x, y \in D$ be distinct. Denote $\frac{p-5}{4}$ by λ. Without loss of generality we can take $y = 1$. Let

$$D, D + \alpha_1, ..., D + \alpha_{\lambda-1}$$

be precisely the λ translates of D in which x and 1 appear together. Then

$$x = x_1 + \alpha_1 = \cdots = x_{\lambda-1} + \alpha_{\lambda-1}$$

for some distinct quadratic residues $x_1, ..., x_{\lambda-1}$ and

$$1 = y_1 + \alpha_1 = \cdots = y_{\lambda-1} + \alpha_{\lambda-1}$$

for some distinct quadratic residues $y_1, ..., y_{\lambda-1}$. Now suppose that $x - 1$ is a quadratic non-residue. Then

$$x - 1 = x_1 - y_1 = \cdots = x_{\lambda-1} - y_{\lambda-1}.$$

Since $p \equiv 1(\text{mod } 4)$ we have $(x-1)^{-1}$ is also a quadratic nonresidue. Then we have

$$1 = (x-1)^{-1}x - (x-1)^{-1} = (x-1)^{-1}x_i - (x-1)^{-1}y_i$$

for $i = 1, ..., \lambda - 1$. This gives precisely λ pairs of consecutive non-residues, these being the *only* pairs of consecutive quadratic non-residues. But this contradicts Lemma 0.9.2, from which we have that the number of pairs of consecutive quadratic non-residues is $\lambda + 1$. The condition is necessary and sufficient, and the dual argument follows from the fact that the 2-adesign $(\mathbb{Z}_p, Dev(D))$ is symmetric. □

We are now ready to construct two more families of 2-adesigns.

Theorem 0.9.2. *Let $p \equiv 1(mod\ 4)$ be a prime greater than 5, and let $D \subseteq \mathbb{Z}_p$ be the set of quadratic residues. Let $\mathcal{B} = \{b \cap D \mid b \in Dev(D), b \neq D\}$, and let $\mathcal{B}_\infty$ be the set containing all members of $\mathcal{B}$ of size $\frac{p-1}{4}$, as well as all members of $\mathcal{B}$ of size $\frac{p-5}{4}$ modified by adjoining the point ∞. Then $(D \cup \{\infty\}, \mathcal{B}_\infty)$ is a 2-$(\frac{p+1}{2}, \frac{p-1}{4}, \frac{p-9}{4})$ adesign.*

Proof: Let $x, y \in D$ be distinct. Denote $\frac{p-5}{4}$ by λ and $\frac{p-1}{2}$ by k. If x and y appear together in exactly λ translates of D, then x and y appear together in exactly λ blocks in $\mathcal{B}_\infty$. Similarly, if x and y appear together in $\lambda + 1$ translates of D then x and y appear together in $\lambda + 1$ blocks in $\mathcal{B}_\infty$. We want to show that x and ∞ appear together in exactly λ blocks in $\mathcal{B}_\infty$. Without loss of generality, we can take $x = 1$. There are $k - 1$ blocks in $\mathcal{B}_\infty$ containing 1. Let

$$D, D + \alpha_1, ..., D + \alpha_w$$

be precisely the translates of D containing 1. By Lemma 0.9.4, if $|D \cap (D + \alpha_i)| = \lambda$, then α_i is a quadratic residue. If $y + \alpha_i = 1$ then we have a pair $y, -\alpha_i$ of consecutive quadratic residues. By Lemma 0.9.2, the number of pairs of consecutive quadratic residues is exactly λ.

To see that there are pairs $x, y \in D$ of distinct points appearing in $\lambda - 1$ blocks as well as those appearing in λ blocks, suppose that $y_1, ..., y_{k-1}$ be the $k - 1$ points in $D \setminus \{1\}$. We can again, without loss of generality, take $x = 1$. Suppose that 1 and y_i appear together in exactly λ translates of D for each i, $1 \leq i \leq k - 1$. Then $y_i - 1 \in D$ for all y_i. By Lemma 0.9.2 this gives too many pairs of consecutive quadratic residues, which completes the proof. □

Example 0.9.2. *With $p = 13$ we apply Theorem 0.9.2 and get that $(D \cup \{\infty\}, \mathcal{B}_\infty)$ is a 2-$(7, 3, 1)$ adesign and $\mathcal{B}_\infty$ contains the following blocks:*

$$\{4, 10, \infty\} \quad \{3, 4, 10\} \quad \{1, 3, 12\} \quad \{4, 9, 12\}$$

$$\{4, 12, \infty\} \quad \{10, 12, \infty\} \quad \{1, 3, \infty\} \quad \{1, 9, \infty\}$$

$$\{1, 4, 9\} \quad \{1, 10, 12\} \quad \{3, 9, 10\} \quad \{3, 9, \infty\}$$

Let $\mathcal{B}$ and $\mathcal{B}_\infty$ be defined as in Theorem 0.9.2. The second construction is the following.

Theorem 0.9.3. *Let $p \equiv 1 (mod\ 4)$ be a prime greater than 5, and let $D \subseteq \mathbb{Z}_p$ be the set of quadratic residues. Let $\bar{\mathcal{B}}_\infty$ be the set of complements of members of $\mathcal{B}_\infty$ in $\mathbb{Z}_p \cup \{\infty\}$. Then $(D \cup \{\infty\}, \bar{\mathcal{B}}_\infty)$ is a 2-$(\frac{p+1}{2}, \frac{p+3}{4}, \frac{p-5}{4})$ adesign.*

Proof: Let $x, y \in D \cup \{\infty\}$ be distinct. Denote $\frac{p-5}{4}$ by λ and $\frac{p-1}{2}$ by k. Suppose x and y appear together in λ blocks in $\mathcal{B}_\infty$. Then there are λ blocks in $\bar{\mathcal{B}}_\infty$ not containing x or y. Also there are $k - 1$ blocks in $\bar{\mathcal{B}}_\infty$ not containing x and $k - 1$ blocks not containing y. Then the number of blocks in $\bar{\mathcal{B}}_\infty$ containing x and y is

$$|\bar{\mathcal{B}}_\infty| - (|\{b \in \bar{\mathcal{B}}_\infty \mid x \notin b\}| + |\{b \in \bar{\mathcal{B}}_\infty \mid y \notin b\}|) + |\{b \in \bar{\mathcal{B}}_\infty \mid x, y \notin b\}|$$

which is easily seen to be $\lambda + 1$. A similar calculation shows that if x and y appear together in $\lambda - 1$ blocks in $\mathcal{B}_\infty$ then x and y appear together in λ blocks $\bar{\mathcal{B}}_\infty$. □

Example 0.9.3. *With $p = 13$ we apply Theorem 0.9.3 and get that $(D \cup \{\infty\}, \bar{\mathcal{B}}_\infty)$ is a 2-$(7, 4, 2)$ adesign and $\bar{\mathcal{B}}_\infty$ contains the following blocks:*

$$\{1, 3, 9, 12\} \quad \{4, 9, 10, \infty\} \quad \{1, 3, 9, 10\} \quad \{4, 9, 10, 12\}$$

$$\{3, 9, 10, \infty\} \quad \{1, 4, 12, \infty\} \quad \{1, 9, 12, \infty\} \quad \{1, 3, 10, \infty\}$$

$$\{1, 3, 4, 9\} \quad \{3, 4, 10, 12\} \quad \{3, 4, 9, \infty\} \quad \{1, 4, 10, 12\}$$

0.10 Constructions of 2-adesigns that are Almost Difference Families

Suppose G is a finite Abelian group of order v in which the identity element is denoted "0". Let k and λ be positive integers such that $2 \leq k < v$. A (v, k, λ) *difference family* in G is a collection of subsets $D_0, ..., D_l$ of G such that

- $|D_i| = k$ for all $i, 0 \leq i \leq l$,
- the multiset union $\cup_{i=1}^{l}\{x - y \mid x, y \in D_i, x \neq y\}$ contains each member of $G \setminus \{0\}$ with multiplicity λ,

and a (v, k, λ, t) *almost difference family* is defined similarly only the multiset union $\cup_{i=1}^{l}\{x - y \mid x, y \in D_i, x \neq y\}$ contains t members of $G \setminus \{0\}$ with multiplicity λ and $v - t - 1$ members of G with multiplicity $\lambda + 1$.

It is trivial that an almost difference family is a 2-adesign. All of the 2-adesigns in this section are also almost difference families, however, our treatment will still be in terms of 2-adesigns.

Our next two constructions make use of quadratic residues. We will need the following lemma [17].

Lemma 0.10.1. *Let $q = 4f + 1 = x^2 + 4y^2$ be a prime power with $x, y \in \mathbb{Z}$ and $x \equiv 1$ (mod 4) (here, y is two-valued depending on the choice of the primitive root α defining the cyclotomic classes). The five distinct cyclotomic numbers of order four for odd f are*

$$\begin{aligned}
(0,0) &= (2,2) = (2,0) = \frac{q-7+2x}{16},\\
(0,1) &= (1,3) = (3,2) = \frac{q+1+2x-8y}{16},\\
(1,2) &= (0,3) = (3,1) = \frac{q+1+2x+8y}{16},\\
(0,2) &= \frac{q+1-6x}{16},\\
\textit{all others} &= \frac{q-3-2x}{16},
\end{aligned}$$

and those for even f are

$$\begin{aligned}(0,0) &= \frac{q-11-6x}{16},\\ (0,1) &= (1,0)=(3,3)=\frac{q-3+2x+8y}{16},\\ (0,2) &= (2,0)=(2,2)=\frac{q-3+2x}{16},\\ (0,3) &= (3,0)=(1,1)=\frac{q-3+2x-8y}{16},\\ \textit{all others} &= \frac{q+1-2x}{16}.\end{aligned}$$

When computing difference levels of a subset C of a group G, it is sometimes convenient to use the difference function which is defined as $d(w)=|C\cap(C+w)|$ where $C+w$ denotes the set $\{c+w \mid c\in C\}$. We are now ready to give our first construction of a 2-adesign that is a difference family.

Theorem 0.10.1. *Let $q=4f+1=x^2+4y^2$ be a prime power with f odd. Let $C_0=D_0^4\cup D_1^4, C_1=D_0^4\cup D_2^4$, and $C_2=D_0^4\cup D_3^4$. Then $(\mathbb{F}_q, Dev(C_0)\cup Dev(C_1)\cup Dev(C_2))$ is a 2-$(q,\frac{q-1}{2},\frac{3q-11}{4})$ adesign.*

Proof: Let $w^{-1}\in D_h^4$. First we let C denote $D_i^4\cup D_{i+1}^4$. Then when we expand $|C\cap(C+w)|$ we get

$$\left|D_{i+h}^4\cap(D_{i+h}^4+1)\right|+\left|D_{i+h}^4\cap(D_{i+h+1}^4+1)\right|+\left|D_{i+h+1}^4\cap(D_{i+h}^4+1)\right|+\left|D_{i+h+1}^4\cap(D_{i+h+1}^4+1)\right|$$

whence

$$\begin{aligned}|C\cap(C+w)| &= (i+h,i+h)+(i+h,i+h+1)+(i+h+1,i+h)+(i+h+1,i+h+1)\\ &= \begin{cases}\frac{q-2y-3}{4} & \text{for } i=0 \text{ and } h=0 \text{ or } 2,\\ \frac{q+2y-3}{4} & \text{for } i=0 \text{ and } h=1 \text{ or } 3,\\ \frac{q-2y-3}{4} & \text{for } i=3 \text{ and } h=0 \text{ or } 2,\\ \frac{q+2y-3}{4} & \text{for } i=3 \text{ and } h=1 \text{ or } 3.\end{cases} \quad \text{(by Lemmas 0.9.1 and 0.10.1)}\end{aligned}$$

We also have

$$|C_j\cap(C_j+w)| = \begin{cases}\frac{q-5}{4} & \text{for } j=0 \text{ or } 2,\\ \frac{q-1}{4} & \text{for } j=1 \text{ or } 3.\end{cases}$$

Now consider the incidence structures $(\mathbb{F}_q, DevC_i)$ for $j = 0, 1, 2$. Let $C_j^{\perp}, (C_j + w)^{\perp}$ denote the points of the dual structures $(Dev(C_j), \mathbb{F}_q)$ corresponding to the blocks $C_j, C_j + w$. We have that $(\mathbb{F}_q, Dev(C_j))$ is a symmetric incidence structure and by Lemma 0.2.2 the number of blocks of $(\mathbb{F}_q, Dev(C_0) \cup Dev(C_1) \cup Dev(C_2))$ which the points $C_j^{\perp}, (C_j + w)^{\perp}$ appear in is

$$\begin{cases} \frac{3q-11}{4} & \text{if } w^{-1} \in D_0^4 \cup D_2^4, \\ \frac{3q-7}{4} & \text{if } w^{-1} \in D_1^4 \cup D_3^4. \end{cases}$$

□

Another construction is the following.

Theorem 0.10.2. *Let $q = 4f + 1 = x^2 + 4y^2$ be a prime power with f even and $x = 1$ or -3. Then $(\mathbb{F}_q, Dev(D_0^4) \cup Dev(D_2^4))$ is a 2-$(q, \frac{q-1}{4}, \frac{q-7-2x}{8})$ adesign.*

Proof: We have, by Lemma 0.10.1,

$$\begin{aligned} \left|D_i^4 \cap (D_i^4 + w)\right| &= \left|D_h^4 \cap (D_h^4 + 1)\right| \\ &= (i + h, i + h) \\ &= \begin{cases} \frac{q-11-6x}{16} & \text{if } h = 0, i = 0 \text{ or } h = 2, i = 2, \\ \frac{q-3+2x-8y}{16} & \text{if } h = 1, i = 0 \text{ or } h = 2, i = 2, \\ \frac{q-3+2x}{16} & \text{if } h = 2, i = 0 \text{ or } h = 3, i = 2, \\ \frac{q-3+2x+8y}{16} & \text{for } h = 3, i = 0 \text{ or } h = 0, i = 2. \end{cases} \end{aligned}$$

Now consider the incidence structures $(\mathbb{F}_q, Dev(D_i^4))$ for $i = 0, 2$. Let $C_i^{\perp}, (C_i + w)^{\perp}$ denote the points of the dual structures $(Dev(D_i^4), \mathbb{F}_q)$ corresponding to the blocks $C_i, C_i + w$. We have that $(\mathbb{F}_q, Dev(C_i))$ is a self-dual incidence structure and by Lemma 0.2.2 the number of blocks of $(\mathbb{F}_q, Dev(D_0^4) \cup Dev(D_2^4))$ which the points $C_i^{\perp}, (C_i + w)^{\perp}$ appear in is

$$\begin{cases} \frac{2q-14-4x}{16} & \text{if } w^{-1} \in D_0^4 \cup D_2^4, \\ \frac{2q-6+4x}{16} & \text{if } w^{-1} \in D_1^4 \cup D_3^4. \end{cases}$$

Thus, we have $(\mathbb{F}_q, Dev(D_0^4) \cup Dev(D_2^4))$ is a 2-adesign whenever $x = 1$, or -3. □

We close this section with yet a few more constructions. Now let q be an odd prime power, and $C \subseteq \mathbb{F}_q$. According to [38], if

1. $C = D_i^4 \cup D_{i+1}^4$, $q \equiv 5(\text{mod } 8)$ and $q = s^2 + 4$ with $s \equiv 1(\text{mod } 4)$, or
2. $C = D_0^8 \cup D_1^8 \cup D_2^8 \cup D_5^8$, $q = l^2$ where l is a prime power of form $l = t^2 + 2 \equiv 3(\text{mod } 8)$, or
3. $C = \cup_{i \in I} D_i^{\sqrt{q}+1}$ where $I \subseteq \{0, 1, .., \sqrt{q}\}$ with $|I| = \frac{\sqrt{q}+1}{2}$ and $q = l^2$ for some prime power l,

then C is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{2})$ almost difference set in $\mathbb{F}_q$.

It is easy to show, also, that if q is an odd prime power, $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ is a 2-$(q, \frac{q-1}{2}, \frac{2q-6}{4})$ design. We then have the following.

Theorem 0.10.3. *Let q be an odd prime power, and $C \subseteq \mathbb{F}_q$. If*

1. $C = D_i^4 \cup D_{i+1}^4$, $q \equiv 5(\textit{mod } 8)$ *and* $q = s^2 + 4$ *with* $s \equiv 1(\textit{mod } 4)$, *or*
2. $C = D_0^8 \cup D_1^8 \cup D_2^8 \cup D_5^8$, $q = l^2$ *where l is a prime power of form* $l = t^2 + 2 \equiv 3(\textit{mod } 8)$, *or*
3. $C = \cup_{i \in I} D_i^{\sqrt{q}+1}$ *where* $I \subseteq \{0, 1, .., \sqrt{q}\}$ *with* $|I| = \frac{\sqrt{q}+1}{2}$, *$I$ contains both even and odd numbers, and $q = l^2$ for some prime power l,*

then $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2) \cup Dev(C))$ *is a* 2-$(q, \frac{q-1}{2}, \frac{3q-11}{4})$ *adesign.*

0.11 Constructions of 2-adesigns from Symmetric Designs

Let $(V, \mathcal{B})$ be an incidence structure with $|\mathcal{B}| = b$. The numbers of blocks in which given single points appear (called the *replication numbers*) become the block sizes of the dual $(V, \mathcal{B})^\perp$, and the intersection numbers among pairs of blocks become the numbers of blocks of $(V, \mathcal{B})^\perp$ in which any two points appear. Then the following is clear.

Lemma 0.11.1. *Let $(V, \mathcal{B})$ be an incidence structure with $|\mathcal{B}| = v$, and in which the replication numbers are a constant k and the intersection numbers among pairs of blocks are integers λ and $\lambda + 1$. Then $(V, \mathcal{B})^\perp$ is a* 2-(b, k, λ) *adesign.*

Remark 0.11.1. *The dual of a quasi-symmetric design whose intersection numbers x, y are such that $y - x = 1$ is always a 2-adesign.*

In [3] constructions of almost difference sets from difference sets were introduced. In this section we further generalize this idea. We will use the following lemma which is actually a trivial construction in itself.

Lemma 0.11.2. *Let $(V, \mathcal{B})$ be a symmetric 2-(v, k, λ) design. Let $\mathbf{b}_1, ..., \mathbf{b}_k$ be any k blocks in $\mathcal{B}$. Let "∞" denote a point. Let $\mathcal{B}'$ denote the blocks of $\mathcal{B}$ modified by adjoining the point "∞" to each of $\mathbf{b}_1, ..., \mathbf{b}_k$. Then $(V, \mathcal{B}')^{\perp}$ is a 2-(v, k, λ) adesign.*

Proof: The replication numbers in the incidence structure $(V, \mathcal{B}')$ are all k, and the intersection numbers among pairs of blocks in $\mathcal{B}'$ are λ and $\lambda + 1$. The result follows from Lemma 0.11.1. □

Note that the number of times which Lemma 0.11.2 can be applied to any given symmetric 2-(v, k, λ) design is $\lfloor \frac{v}{k} \rfloor$.

The following theorem gives another construction.

Theorem 0.11.1. *Let $(V, \mathcal{B})$ be a symmetric 2-(v, k, λ) design. Let $\mathbf{b} = \{b_1, ..., b_k\}$ be a block. Suppose that $\mathbf{b}_1, ..., \mathbf{b}_k$ are k blocks not equal to $\mathbf{b}$ such that*

1. *$b_i \notin \mathbf{b}_i$ for all $i, 1 \leq i \leq k$, and*
2. *$b_j \in \mathbf{b}_l$ implies $b_l \notin \mathbf{b}_j$ for all $j \neq l, 1 \leq j, l \leq k$.*

Let $\mathcal{B}'$ denote the blocks of $\mathcal{B}$ modified by adjoining the point b_i to the block $\mathbf{b}_i$ for all $i, 1 \leq i \leq k$, and then removing the block $\mathbf{b}$. Then $(V, \mathcal{B}')^{\perp}$ is a 2-(v, k, λ) adesign.

Proof: It is easy to see that the replication numbers of $(V, \mathcal{B}')$ are all k. The second condition in the statement ensures that the intersection numbers among pairs of blocks of $\mathcal{B}'$ are either λ or $\lambda + 1$. The result then follows from Lemma 0.11.1. □

Next, we show how to construct almost difference sets from planar difference sets. The following constructions are not optimal but, for certain dimensions, give the best known value for d_1. A (v, k, λ) difference set is called planar if $\lambda = 1$. It is easy to show that, given a planar difference

set D in an (additive) Abelian group G of order v, if we choose any $a_0 \in G \setminus D$ such that $2a_0$ cannot be written as the sum of two distinct members of D, then $D \cup \{a_0\}$ will be an almost difference set with $\lambda = 1$. This is simply due to the fact that, because of the way we chose a_0, we cannot have $a_0 - a = b - a_0$ for any $a, b \in D$, thereby forcing each member of G to appear as a difference of two distinct members of $D \cup \{a_0\}$ only one or two times.

Again, let D be a $(v, k, 1)$ difference set in an Abelian group G of order v. Also let $\kappa : G \to \mathbb{Z}_2 \times G$ by $x \mapsto (0, x)$. Suppose $a_0, ..., a_{s-1} \in G$ are such that the differences $(1, \tau)$ in $\kappa(D) \cup \{(1, a_0), ..., (1, a_{s-1})\}$ cover $\{1\} \times G$ each having multiplicity at most 2, that exactly one of the a_is is a member of D, and twice any a_i is not the sum of two other distinct a_is. If there is at least one difference in $\kappa(D) \cup \{(1, a_0), ..., (1, a_{s-1})\}$ having multiplicity 1, then since the difference $(1, 0)$ occurs exactly twice (because exactly one of the a_is is in D), we have both 1 and 2 occurring as multiplicities. No difference can occur with multiplicity greater than 2 since G is planar and twice any a_i is not the sum of two other distinct a_is. We also have the differences in $\kappa(D) \cup \{(1, a_0), ..., (1, a_{s-1})\}$ covering $\mathbb{Z}_2 \times G$: the differences $(0, \tau)$ cover $\{0\} \times G$ due to G being a planar difference set and we have assumed that the differences $(1, \tau)$ cover $\{1\} \times G$. This discussion is summarized in the following.

Theorem 0.11.2. *Let D be a $(v, k, 1)$ difference set in an (additive) Abelian group G. Suppose $a_0, ..., a_{s-1} \in G$ are such that the differences $(1, \tau)$ in $\kappa(D) \cup \{(1, a_0), ..., (1, a_{s-1})\}$ cover $\{1\} \times G$ each having multiplicity at most 2, that exactly one of the a_is is a member of D, and twice any a_i is not the sum of two other distinct a_is. If there is at least one difference in $\kappa(D) \cup \{(1, a_0), ..., (1, a_{s-1})\}$ having multiplicity 1 then $\kappa(D) \cup \{(1, a_0), ..., (1, a_{s-1})\}$ is a $(2v, k + s, 1, t)$ almost difference set in $\mathbb{Z}_2 \times G$. The resulting symmetric 2-adesign $(\mathbb{Z}_2 \times G,$ Dev$(\kappa(D) \cup \{(1, a_0), ..., (1, a_{s-1})\}))$ has parameters $(2v, k + s, 1)$.*

Example 0.11.1. *Consider the Singer difference set $D = \{1, 2, 4\}$ in $\mathbb{Z}_7$. With $a_0 = 0$ we have $2a_0$ is not the sum of two distinct members of D, and $\kappa(D) \cup \{(1, 0)\}$ is a $(14, 4, 0, 1)$ almost difference set in $\mathbb{Z}_{14}$. With $a_1 = 1$ we have $\kappa(D) \cup \{(1, 0), (1, 1)\}$ is a $(14, 5, 1, 6)$ almost difference set in $\mathbb{Z}_{14}$*

Example 0.11.2. *Consider the Singer difference set $D = \{0, 1, 5, 11\}$ in $\mathbb{Z}_{13}$. With $a_0 = 10$, we have $2a_0$ is not the sum of two distinct members of D, and it is easily checked that $\kappa(D) \cup \{(1, 10)\}$ is a $(26, 5, 0, 5)$ almost difference set in $\mathbb{Z}_{26}$. With $a_1 = 11$ we have that $\kappa(D) \cup \{(1, a_0), (1, a_1)\}$*

is a $(26, 6, 1, 11)$ *almost difference set.*

Example 0.11.3. *Now consider the Singer difference set* $D = \{0, 3, 13, 15, 20\}$ *in* $\mathbb{Z}_{21}$. *We have* $\{9, 13, 16\}$ *are such that the differences* $(1, \tau)$ *cover* $\{1\} \times \mathbb{Z}_{21}$ *with multiplicities no more than* 2 *and that* 13 *is the only member that is also in* D. *It is also easy to see that the difference* $(1, 9)$ *can only occur as the difference* $(1, 9) - (0, 0)$. *Thus we have* $\kappa(D) \cup \{(1, 9), (1, 13), (1, 16)\}$ *is a* $(42, 8, 1, 16)$ *almost difference set.*

0.12 Constructions of 3-adesigns

In this section we will give two constructions each of which produce infinitely many 3-adesigns.

Our first constructions makes use of quadratic residues.

Theorem 0.12.1. *Let* $q \equiv 3 (mod\ 4)$ *be an odd prime power. Then* $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ *is a* 3-$(q, \frac{q-1}{2}, \frac{q-7}{4})$ *adesign.*

Proof: Denote $\frac{q-1}{2}$ by k and $\frac{q-3}{4}$ by λ'. Let $x, y, z \in \mathbb{F}_q$ be arbitrary. To count the number of blocks in which x, y, z appear together, we first count the number of blocks of $Dev(D_0^2) \cup Dev(D_1^2 \cup \{0\})$ in which x, y, z appear together. Suppose that the three points x, y, z appear in μ blocks in $Dev(D_0^2)$. Using the fact that $(\mathbb{F}_q, Dev(D_0^2))$ is a 2-(q, k, λ') design, a simple counting argument gives that there are $q - 3k + 3\lambda' - \mu$ blocks in $Dev(\overline{D_0^2}) := Dev(D_1^2 \cup \{0\})$ containing x, y, z. Thus, there are $q - 3k + 3\lambda' = \lambda'$ blocks in $Dev(D_0^2) \cup Dev(\overline{D_0^2})$ containing x, y, z. Since $w \in D_1^2 \cup \{0\} + w$ for all $w \in \mathbb{F}_q$, we want to know how many of the $q - 3k + 3\lambda' - \mu$ blocks in $Dev(\overline{D_0^2})$ are also in $\{\overline{D_0^2} + x, \overline{D_0^2} + y, \overline{D_0^2} + z\}$. Without loss of generality suppose that both $\overline{D_0^2} + x$ and $\overline{D_0^2} + y$ contain the three points x, y, z. Then we must have $y - x, z - x \notin D_0^2$ and $x - y, z - y \notin D_0^2$. But this would imply that $x - y, y - x \in D_1^2$ where both $x - y$ and $y - x$ are nonzero. But this is impossible as the additive inverse of any member of D_1^2 cannot also be a member whenever $q \equiv 3 (\text{mod } 4)$. Then no more than one of the blocks $\overline{D_0^2} + x, \overline{D_0^2} + y, \overline{D_0^2} + z$ can contain all three of x, y, z. We now need to show that there are two different 3-levels, i.e. that $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ is not a 3-design, but a 3-adesign. To show this we assume that $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ is a 3-(q, k, λ)-design for some λ. Then the number of blocks must be

given by $\lambda\frac{\binom{q}{3}}{\binom{k}{3}}$. The only choices for λ are λ' or $\lambda'-1$. If $\lambda=\lambda'$ then we get that $q-5=q-4$. If $\lambda=\lambda'-1$ then we get that $(q-3)(q-5)=(q-7)(q-2)$. Either way we get a contradiction, which completes the proof. □

Example 0.12.1. *With $q=11$ we apply Theorem 0.12.1 and get that $(\mathbb{Z}_{11}, Dev(D_0^2)\cup Dev(D_1^2))$ is a 3-$(11,5,1)$ adesign with blocks:*

$$\{1,3,4,5,9\}\quad \{2,4,5,6,10\}\quad \{0,3,5,6,7\}\quad \{1,4,6,7,8\}\quad \{2,5,7,8,9\}\quad \{0,4,5,6,8\}$$

$$\{3,6,8,9,10\}\quad \{0,4,7,9,10\}\quad \{0,1,5,8,10\}\quad \{0,1,2,6,9\}\quad \{1,2,3,7,10\}\quad \{1,5,6,7,9\}$$

$$\{0,2,3,4,8\}\quad \{2,6,7,8,10\}\quad \{0,3,7,8,9\}\quad \{1,4,8,9,10\}\quad \{0,2,5,9,10\}$$

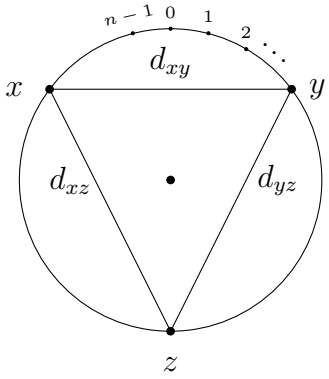
$$\{0,1,3,6,10\}\quad \{0,1,2,4,7\}\quad \{1,2,3,5,8\}\quad \{2,3,4,6,9\}\quad \{3,4,5,7,10\}$$

Our second construction is related to graphs, though it is simple enough to avoid graph-theoretical preliminaries.

Theorem 0.12.2. *Let n (≥ 7) be an odd integer not divisible by 3. Consider, for fixed $a\in\mathbb{Z}_n$, all pairs $\{a-i \pmod n, a+i \pmod n\}$ for $i=1,\cdots,\frac{n-1}{2}$. The union of any two distinct pairs gives a block consisting of four points. Denote, for fixed $a\in\mathbb{Z}_n$, the set of all blocks obtained in this way by B_a. Then $(\mathbb{Z}_n, \cup_{a\in\mathbb{Z}_n}B_a)$ is a 3-$(n,4,2)$ adesign.*

Proof: Arrange all the points in a circle as is shown in the graph below. For any three points $x,y,z\in\mathbb{Z}_n$, denote $|x-y|$, $|x-z|$, $|y-z|$ by d_{xy}, d_{xz}, d_{yz} respectively.

Since n is not divisible by 3, $d_{xy}=d_{xz}=d_{yz}$ cannot happen. Then suppose two of them are equal. Without loss of generality, suppose $d_{xz}=d_{yz}$. Then when x and y are in a pair, z must be the fixed point so that there is no block containing all three of x,y and z. When x and z are in a pair or y and z are in pair, we can find exactly one block containing the three points in each case. If d_{xy}, d_{xz} and d_{yz} are distinct, then we can find one block containing these three points when any two points are in pair, in which case we have three blocks containing these three points together.



□

Example 0.12.2. *With $n = 7$ we apply Theorem 0.12.2 and get that $(\mathbb{Z}_7, \cup_{a\in\mathbb{Z}_7} B_a)$ is a 3-$(7, 4, 2)$ adesign with blocks:*

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

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

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

Let $(V, \mathcal{B})$ be an incidence structure. Let $p \in V$, and define $\mathcal{B}_p = \{\mathcal{B} \setminus \{p\} \mid \mathcal{B} \in \mathcal{B} \text{ and } p \in \mathcal{B}\}$. We call the incidence structure $(V \setminus \{p\}, \mathcal{B}_p)$ the *contraction* of $(V, \mathcal{B})$ at p. It is clear that contracting at points of a 3-adesign will give a 2-adesign as long as not all 3-sets of points occur in the same number of blocks of the contraction.

Example 0.12.3. *The contraction at the point $p = 1$ of the 3-$(11, 5, 1)$ adesign in Example 0.12.1 is a symmetric 2-$(10, 4, 1)$ adesign with the ten blocks:*

$$\{3,4,5,9\} \quad \{4,6,7,8\} \quad \{0,5,8,10\} \quad \{0,2,6,9\} \quad \{2,3,7,10\}$$

$$\{4,8,9,10\} \quad \{0,3,6,10\} \quad \{0,2,4,7\} \quad \{2,3,5,8\} \quad \{5,6,7,9\}$$

Remark 0.12.1. *Interestingly, a contraction at any point of the incidence structure* $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ *from Theorem 0.12.1 gives a symmetric* $2\text{-}(q-1, \frac{q-3}{2}, \frac{q-7}{4})$ *adesign and, since it contains punctured translates of both* D_0^2 *and* D_1^2*, cannot be the development of any almost difference set.*

0.13 Related Codes

0.13.1 Cyclic Codes

We assume some familiarity with cyclic codes. For more details on the subject the reader is referred to [21]. An $[n, k]$ code C over $\mathbb{F}_2$ is called *cyclic* if $(c_0, c_1, ..., c_{n-1}) \in C$ implies that the circular shift $(c_{n-1}, c_0, ..., c_{n-2})$ is also in C. By identifying any vector $(c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_2^n$ with the polynomial

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_2 [x] / (x^n - 1),$$

any linear code C of length n over $\mathbb{F}_2$ corresponds to a subset of $\mathbb{F}_2 [x] / (x^n - 1)$. The code is cyclic if and only if the corresponding subset is an ideal in the ring $\mathbb{F}_2 [x] / (x^n - 1)$. Note that every ideal of $\mathbb{F}_2 [x] / (x^n - 1)$ is principal. Let $g(x) \in \mathbb{F}_2 [x] / (x^n - 1)$ be monic and of minimum degree, and let $C = \langle g(x) \rangle$. Then $g(x)$ is called the *generator polynomial* of C, and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check* polynomial. The dimension of C is given by the degree of $h(x)$.

The following theorem is easy to prove.

Lemma 0.13.1. *Let* D *be subset of* $\mathbb{Z}_n$ *with two difference levels. Define* $D(x) = \sum_{i \in D} x^i \in \mathbb{F}_2 [x]$, $g(x) = gcd(x^n - 1, D(x))$*, and* $h(x) = (x^n - 1)/g(x)$*. Then the code* $C = \langle g(x) \rangle$ *is an* $[n, k]$ *cyclic code where* $k = deg(h(x))$*.*

0.13.2 Known Results on Cyclic Codes from 2-adesigns

It is known that when $p \equiv 1 (\text{mod } 4)$ the code $C = \langle D_0^2(x) \rangle$ is a quadratic residue code if 2 is a square in $\mathbb{F}_p^*$, and a trivial cyclic code otherwise [21]. When $p = 9 + 4y^2 \equiv 1 (\text{mod } 4)$ resp. $p = 49 + 4y^2 \equiv 1 (\text{mod } 4)$ is a prime, D_0^4 resp. $D_0^4 \cup \{0\}$ is an almost difference set [38]. If D is either of these almost difference sets, then some parameters for the code $C = \langle D(x) \rangle$ are known and can be found in [20]. When p_1 and p_2 are primes such that $p_2 - p_1 = 4$, the set $E = E_1^{(2)} \cup \{p_1, 2p_1, ..., (p_2 - 1)p_1\}$, where $E_1^{(2)} = \{0 \le i \le p_1 p_2 \mid \frac{i}{p_1 p_2} = -1\}$, is an almost difference set [38], and some of the parameters of $C = \langle E(x) \rangle$ are known and can be found in [19]. Lastly,

when q is a prime power and α a generator of $\mathbb{F}_{q^2}^*$, the set $D_q = \{0 \leq i \leq n-1 \mid Tr(\alpha^i) = 1\}$ is a planar almost difference set (i.e. with difference levels 0 and 1), and the code $C = \langle D_q(x) \rangle$ has parameters $[q^2-1, q+1, q-1]$ [21]. There are many other constructions of almost difference sets, and the parameters of their linear codes are open in general.

0.13.3 Cyclic Codes from Sets with Two Difference Levels

Sets with two difference levels that are not almost difference sets can also generate codes with good parameters. For example, when $q \equiv 1 (\text{mod } 8)$ is a prime power with unique representation $q = x^2 + 4y^2 = a^2 + 2b^2$ where $x, a \equiv 1 (\text{mod } 4)$, and α is a generator of $\mathbb{F}_q^*$, we can define $D = D_0^8 \cup D_1^8 \cup D_2^8 \cup D_5^8$ and $\Delta_j = |(D + \alpha^j \cap D|$. It was shown in [23] that

$$\Delta_0 = \Delta_2 = \Delta_4 = \Delta_6 = \frac{16q - 48 + 8x - 8a - 16y}{64} \tag{0-5}$$

$$\Delta_1 = \Delta_5 = \frac{16q - 80 - 16x + 16a - 32y}{64} \tag{0-6}$$

$$\Delta_3 = \Delta_7 = \frac{16q - 16}{64}. \tag{0-7}$$

Thus, if $3(a-x)-2y = 4$, we have that $(\mathbb{F}_q, Dev(D))$ is an incidence structure with two difference levels given by $\mu_1 = \frac{16q-48+8x-8a-16y}{64}$ and $\mu_2 = \frac{16q-16}{64}$.

Example 0.13.1. *With $q = 73$ we have the unique representation is given by $x = -3, y = 4$ and $a = 1, b = 6$. Thus the two difference levels are $\mu_1 = 16$ and $\mu_2 = 18$. Since the difference levels are $\equiv 0 (\text{mod } 2)$, the inner product over the field $\mathbb{F}_2$ of any two rows of the incidence matrix will be 0, making the code $C = \langle D(x) \rangle$ self-orthogonal. We checked using MAGMA, and C is a $[73, 18, 24]$ code. According the code tables in* [29]*, the best binary code with length 73 and dimension 18 has minimum weight 24.*

We also have computed the following example using cyclotomic classes of order ten. The cyclotomic numbers of order ten are known and can be found in[50].

Example 0.13.2. *Let $q = 151$, and define $D = D_4 \cup D_5 \cup D_8 \cup D_9$. Then D has the two difference levels $\mu_1 = 22$ and $\mu_2 = 24$ and the code $C = \langle D(x) \rangle$ is self-orthogonal. We checked using MAGMA, and C is a $[151, 30, 48]$ code. According the code tables in* [29]*, the best binary code with length 151 and dimension 30 has minimum weight 48.*

Lemma 0.13.2. *Let A be a $v \times v$ incidence matrix of the symmetric incidence structure $(G, \mathcal{B})$ obtained from the development of some k-subset D in the Abelian group G (where $|G| = v$) with difference levels $\mu_1 < \cdots < \mu_s$. Suppose that $k \equiv \mu_1 \equiv \cdots \equiv \mu_s (mod\ 2)$.*

1. *If k is even the binary code of length v with generator matrix A is self-orthogonal.*
2. *If k is odd the matrix*

$$\begin{bmatrix} 1 & \\ \vdots & A \\ 1 & \end{bmatrix}$$

generates a binary self-orthogonal code of length $v + 1$.

Proof: By Lemma 0.2.2 we can see that, in both cases, the weights of the rows of the generator matrix are all even and the inner product of any two rows is even as well. □

We will refer to an incidence structure $(V, \mathcal{B})$ whose incidence matrix generates a self-orthogonal code simply as *self-orthogonal*.

We will use the following lemma.

Lemma 0.13.3. *Let $(G, \mathcal{B})$ be a symmetric incidence structure coming from the development of a k-subset D of the Abelian group G (where $|G| = v$) with difference levels μ_1 and μ_2. Let t denote the number of members of $G \setminus \{0\}$ which appear μ_1 times in the multiset $\{x - y \mid x, y \in D, x \neq y\}$. The the number of pairs of points in G appearing in exactly μ_1 blocks in $\mathcal{B}$ is $\frac{vt}{2}$ and the number of pairs of points of V appearing in μ_2 blocks is $\frac{v(v-1-t)}{2}$.*

Proof: For each $x \in V$, there are t points in $V \setminus \{x\}$ each appearing together with x in exactly μ_1 blocks. Thus, there are $\frac{vt}{2}$ pairs of points of V appearing in μ_1 blocks. Similarly, there are $\frac{v(v-1-t)}{2}$ pairs of points of V appearing in μ_2 blocks. It is easily seen that $\frac{vt}{2} + \frac{v(v-1-t)}{2} = \binom{v}{2}$. □

We were able to come up with the following bound on the minimum distance of a code generated by a self-orthogonal incidence structure with two difference levels. However, as is clear from Examples 0.13.1 and 0.13.2, there is much room for improvement.

Theorem 0.13.1. *Let A be the incidence matrix of a self-orthogonal incidence structure $(G, \mathcal{B})$ coming from the development of a k-subset D of the Abelian group G (where $|G| = v$) with difference levels μ_1 and μ_2. Let t denote the number of members of $G \setminus \{0\}$ which appear μ_1 times in the multiset $\{x - y \mid x, y \in D, x \neq y\}$. The dual of the binary code with generator matrix A has minimum distance*

$$d \geq \frac{(\mu_2 + k) + \sqrt{(\mu_2 + k)^2 + 4\mu_2(\mu_2 - \mu_1)vt}}{2\mu_2}.$$

Proof: Let S be a minimal set of linearly dependent columns of A. Then every row of A must intersect an even number of these columns in 1s. Let n_i denote the number of rows of A intersecting exactly i columns of S in 1s. Let $d = |S|$. Since every column of A contains k 1s (because the incidence structure $(G, \mathcal{B})$ is symmetric) and the scalar product (over the reals) of any two columns is either μ_1 or μ_2, using Lemma 0.13.3 we have

$$\sum 2in_{2i} = kd$$

and

$$\sum 2i(2i-1)n_{2i} = \mu_2 d(d-1) - (\mu_2 - \mu_1)vt.$$

Subtracting the first equation from the second we have

$$\sum 2i(2i-2)n_{2i} = d((d-1)\mu_2 - k) - (\mu_2 - \mu_1)vt \geq 0.$$

On one hand we get that $d((d-1)\mu_2 - k) \geq (\mu_2 - \mu_1)vt \geq 0$ and on the other hand we get that $d^2\mu_2 - d(\mu_2 + k) - (\mu_2 - \mu_1)vt \geq 0$. The result follows from solving the quadratic. □

0.13.4 Noncyclic Codes from Adesigns

In general, the parameters of codes generated from adesigns are open. Using MAGMA we have computed the parameters of the codes generated by the transpose of the incidence matrix of many of our constructions. We have included the parameters and construction information in the following two tables.

Table 0-1 **Parameters of codes from new 2-adesigns computed by MAGMA**

2-adesign ref	(v, k, λ)	no. of blocks	code parameters	best d	optimal
Theorem 0.9.1	$(11, 5, 3)$	20	$[20, 11, 4]$	5	no
Theorem 0.9.1	$(19, 9, 7)$	36	$[36, 19, 7]$	8	no
Theorem 0.9.2	$(9, 4, 2)$	16	$[16, 8, 5]$	5	yes
Theorem 0.9.2	$(21, 10, 8)$	40	$[40, 20, 9]$	9	no
Theorem 0.9.3	$(9, 5, 4)$	16	$[16, 9, 4]$	4	yes
Theorem 0.9.3	$(21, 11, 10)$	40	$[40, 21, 8]$	8	no
Theorem 0.10.1	$(13, 6, 7)$	39	$[39, 12, 12]$	14	no
Theorem 0.10.1	$(29, 14, 19)$	87	$[87, 28, 22]$	24	no
Theorem 0.10.1	$(53, 26, 37)$	159	$[159, 52, 36]$	35	no
Theorem 0.10.2	$(17, 4, 1)$	34	$[34, 16, 6]$	8	no
Theorem 0.10.2	$(73, 18, 8)$	146	$[146, 72, 20]$	22	no

Note: The column "best d" contains the best known minimum distances according to [29].

Remark 0.13.1. *The* $[159, 52, 36]$ *code corresponding to the* 2-$(53, 26, 37)$ *adesign in Table 0-1 actually improves the lower bound for the minimum weight given in* [29] *for the best binary code with length* 53 *and dimension* 26*.*

Table 0-2 **Parameters of codes from new 3-adesigns computed by MAGMA**

3-adesign ref	(v, k, λ)	no. of blocks	code parameters	best d	optimal
Theorem 0.12.1	$(7, 3, 0)$	14	$[14, 7, 4]$	4	yes
Theorem 0.12.1	$(19, 9, 3)$	38	$[38, 19, 8]$	8	no
Theorem 0.12.2	$(7, 4, 2)$	21	$[21, 6, 8]$	8	yes
Theorem 0.12.2	$(11, 4, 2)$	110	$[110, 10, 40]$	50	no

Note: The column "best d" contains the best minimum distances according to [29].

Remark 0.13.2. *The code corresponding to the* 3-$(7, 4, 2)$ *adesign in Table 0-2 is in fact an optimal, projective two-weight* $[21, 6, 8]$ *code, and so is an optimal code that corresponds to a strongly regular graph* [10].

Remark 0.13.3. *The codes corresponding to the* 3-$(7, 3, 0)$ *and* 3-$(19, 9, 3)$ *adesigns in Table 0-2 are both extremal self-dual codes* [46].

0.14 Closing Remarks

We have investigated some generalizations of combinatorial designs arising from almost difference sets, especially the t-adesigns. We have discussed some of their basic properties and have given several constructions for 2-adesigns, and two contructions for 3-adesigns. Many of the codes arising from these structures have good parameters, as was discussed in Section 7, and we have included some of these in the tables of the previous section. Questions concerning the parameters of the codes arising from adesigns are open in general and, as good codes are arising from many of these structures, further investigation would be worthwhile.

Chapter 4. Partial Geometric Difference Families

0.15 Introduction

In this chapter we discuss partial geometric difference sets and partial geometric difference families, which were introduced by Olmez in [42] and Nowak et al. [39]. Here it was also shown that partial geometric difference sets and partial geometric difference families give partial geometric designs. In this chapter we construct several new classes of partial geometric difference sets and partial geometric difference families, thereby giving new directed strongly regular graphs, and we also discuss some of their links to partially balanced designs and 2-adesigns, and make an investigation into when a 2-adesign is a partial geometric design.

This chapter is organized as follows. In Section 0.16 we construct four classes of partial geometric difference sets, in Section 0.17 we construct six classes of partial geometric difference families, in Section 0.18 we discuss some of the links between partially balanced designs, 2-adesigns, and partial geometric designs, and investigate when a 2-adesign is a partial geometric design. Section 0.19 concludes the chapter.

0.16 New Partial Geometric Difference Sets

We will need the following lemmas.

Lemma 0.16.1. [4] *Let q be a prime power and let C_i, for $i = 0, 1, ..., q$ denote the cyclotomic classes of order $q+1$ in $\mathbb{F}_{q^2}$. Then the cyclotomic numbers are given by*

$$\begin{aligned} (0,0) &= q-2, \\ (i,i) = (i,0) = (0,i) &= 0, \\ (i,j) &= 1, (0 \neq i \neq j). \end{aligned}$$

Lemma 0.16.2. [39] *Let p be a prime and let C_i, for $i = 0, 1, ..., p$ denote the cyclotomic classes of order $p+1$ in $\mathbb{F}_{p^2}$. Let $S_i = C_i \cup \{0\}$ for $i = 0, 1, ..., p$. If $x \notin S_j$ then $|(x - S_j) \cap C_i| = 1$ for each $i \in \{0, 1, ..., p\} \setminus \{j\}$.*

The following is our first construction.

Theorem 0.16.1. *Let $p > 2$ be a prime and let C_i, for $i = 0, 1, ..., p$, denote the cyclotomic classes of order $p+1$ in $\mathbb{F}_{p^2}$. Let $S_i = C_i \cup \{0\}$ for $i = 0, 1, ..., p$. Let $i', j' \in \{0, 1, ..., p\}$ be fixed with $i' \neq j'$. Let $m \equiv 0 \ (mod\ 2)$ be a positive integer, and define*

$$\Omega_l = l + \{0, 2, ..., m-2\} \subset \mathbb{Z}_m \text{ for } l = 0, 1.$$

Then $S_{i'j'} = \Omega_0 \times S_{i'} \cup \Omega_1 \times S_{j'}$ is a partial geometric difference set in $(\mathbb{Z}_m \times \mathbb{F}_{p^2}, +)$ with parameters $(mp^2, mp; \frac{3}{4}m^2p, (\frac{m}{2})^2p(p+3))$.

Proof: First note that $S_0 \cong \mathbb{F}_p$, and $S_{i'}, S_{j'}$ are both subgroups of $(\mathbb{F}_{p^2}, +)$. For each $z \in \mathbb{F}_{p^2}$ and each $i \in \{0, 1, .., p\}$ we have

$$\delta_{S_i}(z) = \begin{cases} |S_i|, \text{ if } z \in S_i \\ 0, \text{ otherwise} \end{cases} = \begin{cases} p, \text{ if } z \in S_i, \\ 0, \text{ otherwise.} \end{cases} \tag{0-8}$$

We first calculate β. Suppose that $(h, z) \in S_{i'j'}$. Then we have

$$(h, z) - S_{i'j'} = \begin{cases} \Omega_0 \times S_{i'} \cup \Omega_1 \times (z - S_{j'}), \text{ if } h \in \Omega_0, z \in S_{i'}, \\ \Omega_1 \times (z - S_{i'}) \cup \Omega_0 \times S_{j'}, \text{ if } h \in \Omega_1, z \in S_{j'}. \end{cases} \tag{0-9}$$

Denote the number of occurrences of u in $\Delta(S_{i'j'})$ by n_u. Then $\sum_{(h',z') \in S_{i'j'}} \delta_{S_{i'j'}}((h, z) - (h', z'))$ can be written

$$\begin{cases} \sum_{v \in \Omega_0 \times \{0\}} n_v + \sum_{v \in \Omega_0 \times (S_{i'} \setminus \{0\})} n_v + \sum_{v \in \Omega_1 \times ((z - S_{j'}) \setminus \{z\})} n_v + \sum_{v \in \Omega_1 \times \{z\}} n_v, \text{ if } h \in \Omega_0, z \in S_{i'}, \\ \sum_{v \in \Omega_0 \times \{0\}} n_v + \sum_{v \in \Omega_0 \times (S_{j'} \setminus \{0\})} n_v + \sum_{v \in \Omega_1 \times ((z - S_{i'}) \setminus \{z\})} n_v + \sum_{v \in \Omega_1 \times \{z\}} n_v, \text{ if } h \in \Omega_1, z \in S_{j'}. \end{cases}$$

which, by (0-9), in both cases gives $\beta = 2(\frac{m}{2})^2p + (\frac{m}{2})^2(p-1)p + (\frac{m}{2})^2p + (\frac{m}{2})^2p = (\frac{m}{2})^2p(p+3)$.

We now calculate α. Suppose that $(h,z) \notin S_{i'j'}$. We have

$$(h,z) - S_{i'j'} = \begin{cases} \Omega_0 \times (z - S_{i'}) \cup \Omega_1 \times S_{j'}, \text{ if } h \in \Omega_0, z \in S_{j'}, \\ \Omega_1 \times S_{i'} \cup \Omega_0 \times (z - S_{j'}), \text{ if } h \in \Omega_1, z \in S_{i'}, \\ \Omega_0 \times (z - S_{i'}) \cup \Omega_1 \times (z - S_{j'}), \text{ if } h \in \Omega_0, z \notin S_{i'} \cup S_{j'}, \\ \Omega_1 \times (z - S_{i'}) \cup \Omega_0 \times (z - S_{j'}) \text{ if } h \in \Omega_1, z \notin S_{i'} \cup S_{j'}. \end{cases} \tag{0-10}$$

Using Lemma 0.16.2, it is easy to see that (h,w), where $h \in \Omega_0$, $w \in (z - S_{i'}) \cap S_{j'}$ and $z \notin S_{i'}$, appears $\frac{m}{2}p$ times in $\Delta(S_{i'j'})$, and each member of $\Omega_1 \times S_{j'}$ appears m times. Similarly, $(0,w)$, where $w \in S_{i'} \cap (z - S_{j'})$ and $z \notin S_{j'}$, appears $(\frac{m}{2})^2 p$ times in $\Delta(S_{i'j'})$, and each member of $\Omega_1 \times S_{i'}$ appears m times.

We need to consider the two cases $h \in \Omega_0, z \notin S_{i'} \cup S_{j'}$ and $h \in \Omega_1, z \notin S_{i'} \cup S_{j'}$. Notice

$$\begin{aligned} \underline{\Delta(S_{i'j'})} = \underline{S_{i'j'}S_{i'j'}^{-1}} &= (\underline{\Omega_0 \times S_{i'} \cup \Omega_1 \times S_{j'}})(\underline{\Omega_0 \times S_{i'} \cup \Omega_1 \times S_{j'}})^{-1} \\ &= \frac{m}{2}(\Omega_0, \underline{S_{i'}S_{i'}^{-1}}) + \frac{m}{2}(\Omega_1, \underline{S_{i'}S_{j'}^{-1}}) + \frac{m}{2}(\Omega_1, \underline{S_{j'}S_{i'}^{-1}}) + \frac{m}{2}(\Omega_0, \underline{S_{j'}S_{j'}^{-1}}) \\ &= \frac{m}{2}(\Omega_0, p(\underline{S_{i'} \cup S_{j'}})) + \frac{m}{2}(\Omega_1, \underline{S_{i'}S_{j'}^{-1}} + \underline{S_{j'}S_{i'}^{-1}}). \end{aligned} \tag{0-11}$$

Since $C_i \cap C_j = \emptyset$ for $i \neq j$ and $f = \frac{p^2-1}{p+1}$ is even, we have by Lemma 0.7.1 that

$$\underline{C_i C_j^{-1}} = \underline{C_i C_j} = \sum_{l=0}^{p} (j-i, l-i)\underline{C_l} = \sum_{l \neq i,j} (j-i, l-i)\underline{C_l}.$$

Thus, by using (0-10) and Lemma 0.16.1, we can see that in the case where $h \in \Omega_0$ and $z \notin S_{i'} \cup S_{j'}$, each member of $\Omega_1 \times (z - S_{j'})$ appears m times in $\Delta(S_{i'j'})$, and a member (h,w), where $h \in \Omega_0$ and $w \in (z - S_{i'}) \cap S_{j'}$, appears $\frac{m}{2}p$ times. Similarly, in the case where $h \in \Omega_1$ and $w \notin S_{i'} \cup S_{j'}$, each member of $\Omega_1 \times (z - S_{i'})$ appears m times in $\Delta(S_{i'j'})$, and a member (h,w), where $h \in \Omega_0$ and $w \in S_{i'} \cap (z - S_{j'})$, appears $\frac{m}{2}p$ times. Thus we have $\alpha = \sum_{(h',z') \in S_{i'j'}} \delta_{S_{i'j'}}((h,z) - (h',z')) = (\frac{m}{2})^2 p + m(\frac{m}{2})p = \frac{3}{4}m^2 p$. □

Example 0.16.1. *Let $p = 5$ and $m = 4$. Let γ be a generator of $\mathbb{F}_{5^2}^*$. Then by Theorem 0.16.1*

$$S_{1,0} = \{(0,0), (0,\gamma), (0,\gamma^7), (0,\gamma^{13}), (0,\gamma^{19}), (2,0), (2,\gamma), (2,\gamma^7), (2,\gamma^{13}),$$
$$(2,\gamma^{19}), (1,0), (1,1), (1,2), (1,3), (1,4), (3,0), (3,1), (3,2), (3,3), (3,4)\}$$

is a $(100, 20; 60, 160)$ partial geometric difference set in $\mathbb{Z}_4 \times \mathbb{F}_{5^2}$. By Theorem 0.3.1 this yields a partial geometric design with parameters $(100, 20, 20; 60, 102)$ whence, via Theorem 0.4.2, a directed strongly regular graph with parameters $(2000, 399, 140, 139, 60)$.

We give another construction of partial geometric difference sets in products of Abelian groups.

Theorem 0.16.2. *Let p be a prime and let C_i, for $i = 0, 1, ..., p$, denote the cyclotomic classes of order $p+1$ in $\mathbb{F}_{p^2}$. Let $S_i = C_i \cup \{0\}$ for $i = 0, 1, ..., p$. Let $i', j' \in \{0, 1, ..., p\}$ be fixed with $i' \neq j'$. Let $\{0, 3\}, \{1, 4\} \subset \mathbb{Z}_6$. Then $S_{i'j'} = \{0, 3\} \times S_{i'} \cup \{1, 4\} \times S_{j'}$ is a partial geometric difference set in $(\mathbb{Z}_6 \times \mathbb{F}_{p^2}, +)$ with parameters $(6p^2, 4p; 8p, 20p)$.*

Proof: We have already established in (0-8) that

$$\delta_{S_i}(z) = \begin{cases} p, \text{ if } z \in S_i, \\ 0, \text{ otherwise.} \end{cases}$$

To calculate β we suppose that $(h, z) \in S_{i'j'}$. Then we have

$$(h, z) - S_{i'j'} = \begin{cases} \{0, 3\} \times S_{i'} \cup \{2, 5\} \times (z - S_{j'}), \text{ if } h \in \{0, 3\}, z \in S_{i'}, \\ \{1, 4\} \times (z - S_{i'}) \cup \{0, 3\} \times S_{j'}, \text{ if } h \in \{1, 4\}, z \in S_{j'}. \end{cases} \quad (0\text{-}12)$$

If we denote the number of occurrences of u in $\Delta(S_{i'j'})$ by n_u then, using (0-12), we have

$$\begin{aligned} \beta = \sum_{(h',z') \in S_{i'j'}} \delta_{S_{i'j'}}((h, z) - (h', z')) &= \sum_{v \in \{0,3\} \times \{0\}} n_v + \sum_{v \in \{0,3\} \times (S_{i'} \setminus \{0\})} n_v + \sum_{v \in \{2,5\} \times (z - S_{j'})} n_v \\ &= 8p + 8p + 4p \\ &= 20p. \end{aligned}$$

We now calculate α. There are seven expressions for $(h, z) - S_{i'j'}$ depending on whether h is contained in $\{0, 3\}, \{1, 4\}$ or $\{2, 5\}$, and whether z is contained in $S_{i'}$ or $S_{j'}$, or contained in neither. These are simple to compute and we do not list them. Using Lemma 0.16.2 it is easy to see that (h, w), where $h \in \{0, 3\}$ and $w \in (z - S_{j'})$ for $z \notin S_{i'}$, appears $2p$ times in $\Delta(S_{i'j'})$, and each member of $\{2, 5\} \times S_{j'}$ appears $2p$ times. The cases where $h \in \{1, 4\}, z \in S_{i'}$, where $h \in \{2, 5\}, z \in S_{j'}$, and where $h \in \{2, 5\}, z \in S_{i'}$, are similar to the previous case. We need to consider the cases where $z \notin S_{i'} \cup S_{j'}$. Notice

$$\begin{aligned} \underline{\Delta(S_{i'j'})} = \underline{S_{i'j'} S_{i'j'}^{-1}} &= (\underline{\{0, 3\} \times S_{i'} \cup \{1, 4\} \times S_{j'}})(\underline{\{0, 3\} \times S_{i'} \cup \{1, 4\} \times S_{j'}})^{-1} \\ &= 2(\{0, 3\}, \underline{S_{i'} S_{i'}^{-1}}) + 2(\{2, 5\}, \underline{S_{i'} S_{j'}^{-1}}) + 2(\{1, 4\}, \underline{S_{j'} S_{i'}^{-1}}) + 2(\{0, 3\}, \underline{S_{j'} S_{j'}^{-1}}) \\ &= 2((\{0, 3\}, p(\underline{S_{i'} \cup S_{j'}})) + (\{2, 5\}, \underline{S_{i'} S_{j'}^{-1}}) + (\{1, 4\}, \underline{S_{j'} S_{i'}^{-1}})) \end{aligned}$$

Since $C_i \cap C_j = \emptyset$ for $i \neq j$ and $f = \frac{p^2-1}{p+1}$ is even, we have by Lemma 0.7.1 that

$$\underline{C_i C_j^{-1}} = \underline{C_i C_j} = \sum_{l=0}^{p} (j-i, l-i)\underline{C_l} = \sum_{l \neq i,j} (j-i, l-i)\underline{C_l}.$$

Thus, by using the expressions for $(h,z) - S_{i'j'}$ and Lemma 0.16.1, we can see that, in the case where $h \in \{0,3\}$ and $z \notin S_{i'} \cup S_{j'}$, each member of $\{2,5\} \times (z - S_{j'})$ appears twice in $\Delta(S_{i'j'})$, and a member (h,w), where $h \in \{0,3\}$ and $w \in (z - S_{i'}) \cap S_{j'}$, appears $2p$ times. The cases where $h \in \{1,4\}, z \notin S_{i'} \cup S_{j'}$ and where $h \in \{2,5\}, z \notin S_{i'} \cup S_{j'}$ are similar. Thus we can conclude that $\alpha = \sum_{(h',z') \in S_{i'j'}} \delta_{S_{i'j'}}((h,z) - (h',z')) = 8p$. □

Example 0.16.2. *Let $p = 3$. Let γ be a generator of $\mathbb{F}_{3^2}$. Then by Theorem 0.16.2*

$$S_{1,0} = \{(0,0), (0,\gamma), (0,\gamma^5), (3,0), (3,\gamma), (3,\gamma^5), (1,0), (1,1), (1,2), (4,0), (4,1), (4,2)\}$$

is a $(54, 12; 24, 60)$ partial geometric difference set in $\mathbb{Z}_6 \times \mathbb{F}_{3^2}$. By Theorem 0.3.1 this yields a partial geometric design with parameters $(54, 12, 12; 24, 26)$ whence, via Theorem 0.4.2, a directed strongly regular graph with parameters $(648, 143, 48, 47, 24)$.

We next construct partial geometric difference sets from planar functions. For a more detailed introduction to planar functions the reader is referred to [3] and [21].

Let $(A,+)$ and $(B,+)$ be Abelian groups of order n and m respectively. Let $f : A \to B$ be a function. One measure of the nonlinearity of f is given by $P_f = \max_{0 \neq a \in A} \max_{b \in B} Pr(f(x+a) - f(x) = b)$, where $Pr(E)$ denotes the probability of the event E. The function f is said to have *perfect nonlinearity* if $P_f = \frac{1}{m}$. The following lemma gives many examples of perfect nonlinear functions in finite fields. For a more complete list of the known perfect nonlinear functions, the reader is referred to Section 1.7 of [21].

Lemma 0.16.3. [3] *The power function x^s from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$, where p is an odd prime, has perfect nonlinearity $P_f = \frac{1}{p^m}$ for the following values of s:*

1. *$s = 2$,*
2. *$s = p^k + 1$, where $m/gcd(m,k)$ is odd,*
3. *$s = (3^k + 1)/2$, where $p = 3$, k is odd, and $gcd(m,k) = 1$.*

We will use the following lemma.

Lemma 0.16.4. [3] *Let f be a function from an Abelian group $(A,+)$ of order n to another Abelian group $(B,+)$ of order n with perfect nonlinearity $P_f = \frac{1}{n}$. Define $C_b = \{x \in A \mid f(x) = b\}$ and $C = \bigcup_{b\in B}\{b\} \times C_b \subset B \times A$. Then*

$$|C \cap (C + (w_1, w_2))| = \begin{cases} n, \text{ if } (w_1, w_2) = (0, 0), \\ 0, \text{ if } w_1 \neq 0, w_2 = 0, \\ 1, \text{ otherwise}. \end{cases}$$

The following is a construction.

Theorem 0.16.3. *Let f be a function from an Abelian group $(A,+)$ of order n to another Abelian group $(B,+)$ of order n with perfect nonlinearity $P_f = \frac{1}{n}$. Define $C_b = \{x \in A \mid f(x) = b\}$ and $C = \bigcup_{b\in B}\{b\} \times C_b \subset B \times A$. Then C is a partial geometric difference set in $A \times B$ with parameters $(n^2, n; n-1, 2n-1)$.*

Proof: Suppose $(h, z) \in C$. Then we have

$$\begin{aligned} \beta = (h,z) - C &= \bigcup_{b\in B}\{h-b\} \times (z - C_b) \\ &= \bigcup_{b\in B}\{h-b\} \times \{z - x \mid z, x \in A, f(x) = b\}. \end{aligned}$$

Denote the number of occurrences of u in $\Delta(C)$ by n_u. Define $V_1 = \bigcup_{b\in B\setminus\{h\}}\{h-b\} \times \{0\}$ and $V_2 = \bigcup_{b\in B}\{h-b\} \times \{z - x \mid x, z \in A, z \neq x, f(x) = b\}$. Then, using Lemma 0.16.4, we have

$$\begin{aligned} \sum_{(h',z')\in C} \delta((h,z) - (h',z')) &= n_{(0,0)} + \sum_{v\in V_1} n_v + \sum_{v\in V_2} n_v \\ &= n + 0 + (n-1) \\ &= 2n - 1. \end{aligned}$$

Now suppose $(h, z) \notin C$. Define $U = \bigcup_{b\in B\setminus\{f(0)\}}\{h-b\} \times \{z - x \mid x \in A, f(x) = b\}$. Then,

using Lemma 0.16.4, we have

$$\begin{aligned}\alpha = \sum_{(h',z')\in C} \delta((h,z)-(h',z')) &= n_{(h-f(0),0)} + \sum_{v\in U} n_v \\ &= 0 + (n-1) \\ &= n-1.\end{aligned}$$

□

Corollary 0.16.1. *Let $f(x) = x^s$ be a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$, where p is an odd prime. Define $C_b = \{x \in \mathbb{F}_{p^m} \mid f(x) = b\}$ and $C = \bigcup_{b\in\mathbb{F}_{p^m}} \{b\} \times C_b \subset \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. If:*

1. *$s = 2$,*
2. *$s = p^k + 1$, where $m/gcd(m,k)$ is odd, or*
3. *$s = (3^k+1)/2$, where $p = 3$, k is odd, and $gcd(m,k) = 1$.*

Then $(\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, Dev(C))$ is a partial geometric difference set with parameters $(p^{2m}, p^m; p^m - 1, 2p^m - 1)$.

Example 0.16.3. *Let $p = 3$ and $m = 2$. Let $f(x) = x^2$. The set $C = \bigcup_{b\in\mathbb{F}_{3^2}} \{b\} \times C_b$ is given by*

$$\{(0,0),(1,1),(1,2),(2,\gamma^6),(\gamma^2,\gamma^5),(\gamma^6,\gamma^7),(\gamma^2,\gamma),(\gamma^6,\gamma^3),(2,\gamma^2)\}$$

and by Corollary 0.16.1 is a $(81,9;8,17)$ partial geometric difference set in $\mathbb{F}_{3^2} \times \mathbb{F}_{3^2}$. By Theorem 0.3.1 this yields a partial geometric design with parameters $(81,9,9;0,8)$ whence, via Theorem 0.4.2, a directed strongly regular graph with parameters $(729,80,24,23,0)$.

Remark 0.16.1. *Interestingly, the partial geometric difference sets constructed in Theorem 0.16.3 are almost difference sets* [3] *and so correspond to planar 2-adesigns (see Section 0.18). Consequently these partial geometric difference sets must also satisfy the condition in Lemma 22 of [39], where Nowak et al. investigated when an almost difference set is partial geometric.*

In [39], partial geometric difference families in groups $G = \mathbb{Z}_n$ where $n = 4l$ for some positive integer l were constructed. We close this section by further generalizing this idea. The proof is a simple counting exercise, and so is omitted.

Theorem 0.16.4. *Let $G = \mathbb{Z}_2 \times \mathbb{Z}_n$ where $n = 4l$ for some positive integer l. Let $H = \langle 4 \rangle$ be the unique subgroup of $\mathbb{Z}_n$ of order l. Define $H + i = \{z + i \mid z \in H\} = \{x \in \mathbb{Z}_n \mid x \equiv i (mod\ 4)\}$ for $i = 0, 1, 2, 3$ (i.e. the cosets of H in $\mathbb{Z}_n$). Then both $\{0\} \times (H \cup (H + 1)) \cup \{1\} \times (H \cup (H + 3))$ and $\{1\} \times (H \cup (H + 1)) \cup \{0\} \times (H \cup (H + 3))$ are partial geometric difference sets in G with parameters $(8l, 4l; 6l^2, 10l^2)$.*

Example 0.16.4. *With $G = \mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $H = \langle 4 \rangle$ the unique subgroup of $\mathbb{Z}_{12}$ of order 3, by Theorem 0.16.4 we have that the set $\{0\} \times (H \cup (H + 1)) \cup \{1\} \times (H \cup (H + 3))$, which is given by*

$$\{(0,0), (0,1), (0,4), (0,5), (0,8), (0,9), (1,0), (1,3), (1,4), (1,7), (1,8), (1,11)\},$$

is a $(24, 12; 54, 90)$ partial geometric difference set. By Theorem 0.3.1 this yields a partial geometric design with parameters $(24, 12, 12; 54, 45)$ whence, via Theorem 0.4.2, a directed strongly regular graph with parameters $(288, 143, 67, 66, 54)$.

We next discuss some new partial geometric difference families.

0.17 New Partial Geometric Difference Families

We begin with the following construction.

Theorem 0.17.1. *Let $n = p^u$ where p is an odd prime and $u \geq 2$ is an integer. Let $S = \{0, 1, ..., p^{u-1} - 1\}$ and, for $l = 0, 1, ..., p^{u-1}$, define $S_l = (pl - 1)S = \{0, pl - 1, 2pl - 2, ..., (p^{u-1} - 1)pl - (p^{u-1} - 1)\}$. Then $\mathcal{S} = \{S_l \mid l = 1, 2, ..., p^{u-1}\}$ is a partial geometric difference family with parameters $(p^u, p^{u-1}, p^{u-1}; (p^{u-1} - 1)p^{u-1}p^{u-2}, p^u + (p^{u-1} - 1)p^{u-1}p^{u-2})$.*

Proof: We will use the following property, which is easily seen to hold:

The members $\pm(pl - 1), \pm(2pl - 2), ..., \pm(p^{u-1} - 1)pl - (p^{u-1} - 1)$ each appear in the multiset $\Delta(S_l)$ with multiplicities $p^{u-1} - 1, p^{u-1} - 2, ..., 1$ respectively. (0-13)

Also note that for $s \in S$ we have that $\pm s(pl - 1) \equiv \mp(p^{u-1} - s)(pl - 1) (\text{mod } p^{u-1})$ for each l, $l = 0, 1, ..., p^{u-1}$.

Claim: For each $s \in S$, the equation $s(pl-1) \equiv v(\text{mod } p^u)$ has p^{u-2} solutions (s,l) for $s,l \in \{0,1,...,p^{u-1}\}$.

Proof of Claim: Notice if $pl-1 \equiv v(\text{mod } p^u)$ we have $s(p(l+\omega)-1) \equiv v(\text{mod } p^u)$ if and only if

$$sv + sp\omega \equiv v(\text{mod } p^u). \tag{0-14}$$

We can see that (0-14) holds if and only if $s \equiv 1(\text{mod } p)$. We know that $(s,\omega) = (1,0)$ is a solution. Now set $s = 1+p$ and $\omega = pl'+1$ for some $l' \in \{0,...,p^{u-1}\}$. Then we have

$$\begin{aligned}(p+1)(pl-1)+(p+1)(pl'+1)p = pl-1 \quad &\Leftrightarrow \quad pv+(p^2l'+p+pl'+1)p = 0\\ &\Leftrightarrow \quad p(pl-1)+p^2(1+l')+p = 0\\ &\Leftrightarrow \quad p^2(l+l'+1) = 0\\ &\Leftrightarrow \quad l+l'+1 \equiv p(\text{mod } p^{u-1}).\end{aligned}$$

Thus we can choose $\omega = pl'+1$ where $l' \equiv -l-1(\text{mod } p^{u-1})$ and we have a solution. Since there are p^{u-2} such solutions, the claim is proved.

Thus we have that each element of $\mathbb{Z}_{p^u}$ not congruent to $0(\text{mod } p^{u-1})$ appears in S_l for p^{u-2} different values of l. Since 0 appears p^u times in the multiset $\bigsqcup_{l=1}^{p^{u-1}} \Delta(S_l)$, and by (0-13), we must have that if $x \in S_l$ for some l then

$$\begin{aligned}\beta = \sum_{y\in S_l}\sum_{l}\delta_{S_l}(x-y) &= p^u + \sum_{l}\sum_{y\in S_l, x\neq y} p^{u-2}p^{u-1}\\ &= p^u + (p^{u-1}-1)p^{u-2}p^{u-1}. \qquad \text{(since each } S_l \text{ contains } 0)\end{aligned}$$

Now notice that if we reduce the elements of S_l modulo p^{u-1} we get the set $S = S_0$. It follows then that for any S_l, and any $x \notin S_l$, the set $x - S_l$ contains exactly one member congruent to $0(\text{mod } p^{u-1})$. Then we have that if $x \notin S_l$ for all l, then

$$\begin{aligned}\alpha = \sum_{y\in S_l}\sum_{l}\delta_{S_l}(x-y) &= \sum_{l}\sum_{y\in S_l, x\not\equiv y(\text{mod } p^{u-1})} p^{u-2}p^{u-1}\\ &= (p^{u-1}-1)p^{u-2}p^{u-1}.\end{aligned}$$

□

Example 0.17.1. *Let $p = 5$ and $u = 2$ so that $n = 25$ and $S = \{0,1,2,3,4\} \subset \mathbb{Z}_{25}$. Then by Theorem 0.17.1 we have that $\mathcal{S} = \{S_l \mid l = 1,2,...,5\}$, which is given by*

$$\{\{0,4,8,12,16\},\{0,2,9,11,18\},\{0,3,6,14,17\},\{0,1,7,13,19\},\{0,21,22,23,24\}\},$$

is a $(25, 5, 5; 20, 45)$ *partial geometric difference family in* $\mathbb{Z}_{25}$*. By Theorem 0.3.1 this yields a partial geometric design with parameters* $(25, 5, 25; 20, 16)$ *whence, via Theorem 0.4.2, a directed strongly regular graph with parameters* $(625, 124, 44, 43, 20)$.

Our next two constructions further generalize Theorem 0.16.1.

Theorem 0.17.2. *Let* p *be a prime, and for each* $i \in \{0, 1, ..., p\}$ *let* $S_i = C_i \cup \{0\}$ *where* C_i *is the* i*th cyclotomic class of order* $p + 1$ *in* $\mathbb{F}_{p^2}$*. Let* $I \subset \{0, 1, ..., p\}$ *such that* $|I| = 2\kappa$ *for some positive integer* κ*. Say* $I = \{i_1, ..., i_{2\kappa}\}$*, and define* Θ_0 *to be the set of all pairs* $(i, j) \in I \times I$ *such that* $i \neq j$ *and each member of* I *appears in exactly one ordered pair. Let* m *be a positive, even integer. Define* $\Omega_l = l + \{0, 2, ..., m - 2\} \subset \mathbb{Z}_m$ *for* $l = 0, 1$*, and for each* $(i', j') \in \Theta_0$ *define* $S_{i'j'} = \Omega_0 \times S_{i'} \cup \Omega_1 \times S_{j'} \subset \mathbb{Z}_m \times \mathbb{F}_{p^2}$*. Then* $\mathcal{S} = \{S_{i'j'} \mid (i', j') \in \Theta_0\}$ *is a partial geometric difference family with parameters* $(mp^2, mp, \kappa; \kappa\frac{3}{4}m^2p, (\frac{m}{2})^2p(p + 3) + (\kappa - 1)\frac{3}{4}m^2p)$.

Proof: We have already established in Theorem 0.16.1 that if $(h, z) \in S_{i'j'}$ then

$$\sum_{(h',z') \in S_{i'j'}} \delta_{S_{i'j'}}((h, z) - (h', z')) = (\frac{m}{2})^2p(p + 3), \tag{0-15}$$

and if $(h, z) \notin S_{i'j'}$ then

$$\sum_{(h',z') \in S_{i'j'}} \delta_{S_{i'j'}}((h, z) - (h', z')) = \frac{3}{4}m^2p. \tag{0-16}$$

Now let $(h, z) \in S_{i'j'}$ for some $(i', j') \in \Theta_0$. Let $(i, j) \in \Theta_0$ such that $(i, j) \neq (i', j')$. Denote the number of occurrences of u in $\Delta(S_{ij})$ by n_u. Using Equation (0-11) we have

$$\sum_{(h',z') \in S_{i'j'}} \delta((h, z) - (h', z')) = 4(\frac{m}{2})^2p. \tag{0-17}$$

Then, using Equations (0-15), (0-16) and (0-17), we have

$$\beta = \sum_{(h,z) \in S_{i'j'}} \sum_{(i,j) \in \Theta_0} \delta_{S_{ij}}((h_1, z_1) - (h, z)) = (\frac{m}{2})^2p(p + 3) + (\kappa - 1)4(\frac{m}{2})^2p,$$

and if $(h, z) \notin S_{i'j'}$ we have

$$\alpha = \sum_{(h,z) \in S_{i'j'}} \sum_{(i,j) \in \Theta_0} \delta_{S_{ij}}((h_1, z_1) - (h, z)) = \frac{3}{4}m^2p + (\kappa - 1)4(\frac{m}{2})^2p.$$

□

Example 0.17.2. *Let $p = 5$, $m = 4$, $I = \{0, 1, 2, 3\}$, and $\Theta = \{(1, 0), (2, 3)\}$. Then Θ satisfies the condition in Theorem 0.17.2. Let γ be a generator of $\mathbb{F}_{5^2}^*$. Then $\mathcal{S} = \{S_{1,0}, S_{2,3}\}$, where*

$$S_{1,0} = \{(0,0), (0,\gamma), (0,\gamma^7), (0,\gamma^{13}), (0,\gamma^{19}), (2,0), (2,\gamma), (2,\gamma^7), (2,\gamma^{13}),$$
$$(2,\gamma^{19}), (1,0), (1,1), (1,2), (1,3), (1,4), (3,0), (3,1), (3,2), (3,3), (3,4)\},$$

and

$$S_{2,3} = \{(0,0), (0,\gamma^2)(0,\gamma^8), (0,\gamma^{14}), (0,\gamma^{20}), (2,0), (2,\gamma^2), (2,\gamma^8), (2,\gamma^{14}), (2,\gamma^{20}),$$
$$(1,0), (1,\gamma^3), (1,\gamma^9), (1,\gamma^{15}), (1,\gamma^{21}), (3,0), (3,\gamma^3), (3,\gamma^9), (3,\gamma^{15}), (3,\gamma^{21})\},$$

is a $(100, 20, 2; 140, 240)$ partial geometric difference family in $\mathbb{Z}_4 \times \mathbb{F}_{5^2}$. By Theorem 0.3.1 this yields a partial geometric design with parameters $(100, 20, 40; 140, 162)$ whence, via Theorem 0.4.2, a directed strongly regular graph with parameters $(2000, 799, 220, 219, 140)$.

The proofs of the following corollaries are omitted as they use simple counting principals similar to those used in the proof of Theorem 0.17.2.

Corollary 0.17.1. *Let p be a prime, and for each $i \in \{0, 1, ..., p\}$ let $S_i = C_i \cup \{0\}$ where C_i is the ith cyclotomic class of order $p+1$ in $\mathbb{F}_{p^2}$. Let $I \subset \{0, 1, ..., p\}$ such that $|I| = 2\kappa$ for some positive integer κ. Say $I = \{i_1, ..., i_{2\kappa}\}$, and define $\Theta_1 = \{(i_{2\kappa}, i_1), (i_1, i_2), (i_2, i_3), ..., (i_{2\kappa-1}, i_{2\kappa})\}$. Let m be a positive integer. Define $\Sigma_l = l + \{0, 2, ..., m-2\} \subset \mathbb{Z}_m$ for $l = 0, 1$, and for each $(i', j') \in \Theta_1$ define $S_{i'j'} = \Omega_0 \times S_{i'} \cup \Omega_1 \times S_{j'} \subset \mathbb{Z}_m \times \mathbb{F}_{p^2}$. Then $\mathcal{S} = \{S_{i'j'} \mid (i', j') \in \Theta_1\}$ is a partial geometric difference family with parameters $(mp^2, mp, 2\kappa; \frac{3}{4}m^2p + (2\kappa - 1)4(\frac{m}{2})^2p, (\frac{m}{2})^2p(p + 3) + (2\kappa - 1)4(\frac{m}{2})^2p)$.*

Corollary 0.17.2. *Let p be a prime, and for each $i \in \{0, 1, ..., p\}$ let $S_i = C_i \cup \{0\}$ where C_i is the ith cyclotomic class of order $p+1$ in $\mathbb{F}_{p^2}$. Let the integer κ and Θ_e, for $e = 0$ resp. 1, be defined as in Theorem 0.17.2 resp. Corollary 0.17.1. For each $(i', j') \in \Theta_e$ define $S^e_{i'j'} = \{0, 3\} \times S_{i'} \cup \{1, 4\} \times S_{j'} \subset \mathbb{Z}_6 \times \mathbb{F}_{p^2}$ for $e = 0, 1$, and $\mathcal{S}^e = \{S^e_{i'j'} \mid (i', j') \in \Theta_e\}$. Then $\mathcal{S}^0$ resp. $\mathcal{S}^1$ is a partial geometric difference family with parameters $(6p^2, 4p, \kappa; 8p + (\kappa - 1)12p, 20p + (\kappa - 1)12p)$ resp. $(6p^2, 4p, 2\kappa; 8p + (2\kappa - 1)12p, 20p + (2\kappa - 1)12p)$.*

We close this section with the following construction.

Theorem 0.17.3. *Let G be an Abelian group of odd composite order n. Let H be a proper, non-trivial subgroup of G of order m, and set $\kappa = \frac{n/m-1}{2}$. Suppose that $g_1, ..., g_\kappa \in G$ are such that $\{H \pm g_i \mid 1 \leq i \leq \kappa\}$ is a partition of $G \setminus H$. Then $\mathcal{S} = \{H \cup (H + g_i) \mid 1 \leq i \leq \kappa\}$ is a partial geometric difference family with parameters $(n, 2m, \kappa; 2(n-m)m, 3(n-m)m)$.*

Proof: If $g \in H \cup (H + g_{i'})$ for some fixed $i' \in \{1, ..., \kappa\}$ then

$$g - (H \cup (H + g_{i'})) = (H + g) \cup (H + (g - g_{i'})) = \begin{cases} (H + g_{i'}) \cup H, \text{ if } g \in H + g_{i'}, \\ H \cup (H - g_{i'}), \text{ otherwise.} \end{cases} \tag{0-18}$$

If $g \notin H \cup (H + g_{i'})$, then

$$g - (H \cup (H + g_{i'})) = (H + g) \cup (H + (g - g_{i'})) \tag{0-19}$$

where $H + g$ and $H + (g - g_{i'})$ are distinct members of $\{H \pm g_i \mid 1 \leq i \leq \kappa\}$. Also notice that, for fixed $i' \in \{1, ..., \kappa\}$, we have

$$\begin{aligned} \Delta(H \cup (H + g_{i'})) &= \underline{(H \cup (H + g_{i'}))(H \cup (H + g_{i'}))^{-1}} \\ &= 2\underline{HH^{-1}} + \underline{H(H + g_{i'})^{-1}} + \underline{(H + g_{i'})H^{-1}} \\ &= 2m\underline{H} + m\underline{(H - g_{i'})} + m\underline{(H + g_{i'})}. \end{aligned} \tag{0-20}$$

Let n_u denote the number of occurrences of u in $\Delta(\mathcal{S}) = \bigsqcup_{i=1}^{\kappa} \Delta(H \cup (H + g_i))$. Then, using (0-18) and (0-20), if $g \in H \cup (H + g_{i'})$ we have

$$\beta = \sum_{g' \in H \cup (H + g_{i'})} \sum_{i=1}^{\kappa} \delta_{H \cup (H + g_i)}(g - g') = 2\kappa|H| + m|H + g_i| + m|H - g_i| = 3(n-m)m,$$

and using (0-19) and (0-20), if $g \notin \mathcal{S}$ we have

$$\alpha = \sum_{g' \in H \cup (H + g_i)} \sum_{i=1}^{\kappa} \delta_{H \cup (H + g_i)}(g - g') = 2\kappa m^2 = 2(n-m)m.$$

□

Example 0.17.3. *Let $G = \mathbb{Z}_{15}$ and $H = \langle 3 \rangle \leq G$. Then by Theorem 0.17.3 we have that $\mathcal{S} = \{H \cup (H + 1), H \cup (H - 1)\}$ is a $(15, 10, 2; 100, 150)$ partial geometric difference family in G. By Theorem 0.3.1 this yields a partial geometric design with parameters $(15, 10, 20; 100, 40)$ whence, via Theorem 0.4.2, a directed strongly regular graph with parameters $(300, 199, 68, 67, 100)$.*

Table 0-3 **Parameters of partial geometric difference sets constructed in this paper.**

Reference	$(v, k; \alpha, \beta)$	Group	Information
Theorem 0.16.1	$(mp^2, mp; \frac{3}{4}m^2p, (\frac{m}{2})^2p(p+3))$	$\mathbb{Z}_m \times \mathbb{F}_{p^2}$	m even, p an odd prime
Theorem 0.16.2	$(6p^2, 4p; 8p, 20p)$	$\mathbb{Z}_6 \times \mathbb{F}_{p^2}$	p an odd prime
Theorem 0.16.3	$(n^2, n; n-1, 2n-1)^*$	$A \times B$ (generic)	A, B both Abelian groups of order n
Theorem 0.16.4	$(8l, 4l; 10l^2, 6l^2)$	$\mathbb{Z}_2 \times \mathbb{Z}_n$	$n = 4l$ for positive integer l

*: This partial geometric difference set is an almost difference set and corresponds to a planar 2-adesign (see Section 0.18).

Table 0-4 **Parameters of partial geometric difference families constructed in this paper.**

Reference	$(v, k, n; \alpha, \beta)$	Group	Information
Theorem 0.17.1	$(p^u, p^{u-1}, p^{u-1}; \alpha, \beta)$ $\alpha = (P^{u-1}-1)p^{u-1}p^{u-2}$ $\beta = p^u + (p^{u-1}-1)p^{u-1}p^{u-2}$	$\mathbb{Z}_{p^u}$	p an odd prime, $u \geq 2$ an integer
Theorem 0.17.2	$(mp^2, mp, \kappa; \kappa\frac{3}{4}m^2p, (\frac{m}{2})^2p(p+3) + (\kappa-1)\frac{3}{4}m^2p)$ $1 \leq \kappa \leq \frac{p+1}{2}$	$\mathbb{Z}_m \times \mathbb{F}_{p^2}$	m even, p an odd prime
Corollary 0.17.1	$(mp^2, mp, 2\kappa; \alpha, \beta)$ $\alpha = \frac{3}{4}m^2p + (2\kappa-1)4(\frac{m}{2})^2p$ $\beta = (\frac{m}{2})^2p(p+3) + (2\kappa-1)4(\frac{m}{2})^2p$ $1 \leq \kappa \leq \frac{p+1}{2}$	$\mathbb{Z}_m \times \mathbb{F}_{p^2}$	m even, p an odd prime
Corollary 0.17.2	$(6p^2, 4p, \kappa; 8p + (\kappa-1)12p, 20p + (\kappa-1)12p)$ $1 \leq \kappa \leq \frac{p+1}{2}$	$\mathbb{Z}_6 \times \mathbb{F}_{p^2}$	p an odd prime
Corollary 0.17.2	$(6p^2, 4p, 2\kappa; 8p + (2\kappa-1)12p, 20p + (2\kappa-1)12p)$ $1 \leq \kappa \leq \frac{p+1}{2}$	$\mathbb{Z}_6 \times \mathbb{F}_{p^2}$	p an odd prime
Theorem 0.17.3	$(n, 2m, \kappa; 2(n-m)m, 3(n-m)m)$ $\kappa = \frac{n/m-1}{2}$	G (generic)	G Abelian of odd, composite order n with $m \mid n$

The following table accounts for the directed strongly regular graphs with less than 110 vertices constructed in this paper. We provide the parameters of the directed strongly regular graphs, the theorem in this paper by which it is constructed, as well as the references of other works in which the parameters have previously appeared.

Table 0-5 **Parameters of directed strongly regular graphs with less than 110 vertices constructed in this paper.**

(v,k,t,λ,μ)	Ref. in this paper	Information	Param. appear in
$(27,8,4,3,2)$	Corollary 0.16.1	$p=3, m=1, f(x)=x^2$	[2], [26]
$(32,15,9,8,6)$	Theorem 0.16.4	$l=1$	[25]
$(48,31,23,22,16)$	Theorem 0.17.3	$G=\mathbb{Z}_6, H=\langle 3\rangle$	[25], [26], [44]
$(81,26,14,13,6)$	Theorem 0.17.1	$p=3, u=2$	[25]
$(108,35,17,16,9)$	Theorem 0.16.1	$p=3, m=2$	[26], [44]

0.18 Partial Geometric Designs, Adesigns, and Their Links

We first discuss an important connection between partial geometric designs and tactical configurations that have exactly *two* indices, i.e., tactical configurations $(V,\mathcal{B})$ where there are integers $\mu_1 \neq \mu_2$ such that for any pair of distinct points $x, y \in V$, $r_{xy} \in \{\mu_1, \mu_2\}$. If A is the $v \times b$ incidence matrix of a tactical configuration $(V,\mathcal{B})$ with v points, b blocks, and the two indices $\mu_1 \neq \mu_2$, then we will denote by A_1 the symmetric matrix whose (i,j)th entry is 1 if the points corresponding to the ith and jth rows of A are contained in exactly μ_1 blocks, and is 0 otherwise. We will need the following lemma.

Lemma 0.18.1. [37] *An incidence structure $(V,\mathcal{B})$ is a partial geometric design with parameters $(v,k,r;\alpha',\beta')$ if and only if its incidence matrix A satisfies*

$$AJ = rJ, JA = kJ \text{ and } AA^TA = n'A + \alpha' J,$$

where $n' = r + k + \beta' - \alpha' - 1$.

Suppose $(V,\mathcal{B})$ is a partial geometric design with parameters $(v,k,r;\alpha',\beta')$ and the two indices $\mu_1 \neq \mu_2$. Let A be the incidence matrix of $(V,\mathcal{B})$. It is easy to see that A satisfies

$$AA^T = rI + \mu_1 A_1 + \mu_2(J - A_1 - I). \tag{0-21}$$

Since $(V, \mathcal{B})$ is partial geometric, by Lemma 0.18.1 we have that A also satisfies

$$n'A + \alpha' J = AA^T A = (r - \mu_2)A + (\mu_1 - \mu_2)A_1 A + \mu_2 kJ. \tag{0-22}$$

Then, using (0-21) and (0-22), we must have that $A_1 A = \nu A + \zeta(J - A)$ for some integers ν and ζ. Moreover we must have $n' + \alpha' = r - \mu_2 + \nu$ and $\alpha' = \zeta + \mu_2 k$. This means that, for each pair $(x, b) \in V \times \mathcal{B}$, we have

$$|\{y \in b \mid y \neq x, r_{xy} = \mu_1\}| = \begin{cases} \nu & (= n' + \alpha' - r + \mu_2), \text{ if } x \in b, \\ \zeta & (= \alpha' - \mu_2 k), \text{ otherwise.} \end{cases} \tag{0-23}$$

Note that condition (0-23) is necessary and sufficient.

Now set $\sigma = r - \mu_2$, $\phi = \mu_1 - \mu_2$ and $\psi = \nu - \zeta$. Then we can write $AA^T = \sigma I + \phi A_1 + \mu_2 J$ and $A_1 A = \psi A + \zeta J$. By Lemma 0.18.1, and since A_1 is symmetric, we have

$$krJ = AA^T J = \psi A_1 J + \sigma J + \mu_2 kJ = JAA^T.$$

Then, after some simple arithmetic, we can get

$$A_1 J = JA_1 = \kappa J \tag{0-24}$$

where $\kappa = \frac{(k-1)r + \mu_2(1-v)}{\mu_1 - \mu_2}$. Now set $\epsilon = \zeta r - \mu_2(\kappa - \psi)$. Then we have

$$\begin{aligned} (\psi A + \zeta J)A^T = A_1 AA^T = \phi A_1^2 + \sigma A_1 + \mu_2 \kappa J \quad &\Leftrightarrow \quad \phi A_1^2 + \sigma A_1 - \psi\phi A_1 + \psi\sigma I = \epsilon J \\ &\Leftrightarrow \quad A_1^2 = k'I + aA_1 + b(J - I - A_1), \end{aligned} \tag{0-25}$$

where $k' = \kappa = \frac{\epsilon - \psi\sigma}{\phi}$, $a = \frac{\epsilon + \psi\phi - \sigma}{\phi}$ and $b = \frac{\epsilon}{\phi}$ are integers (note that $k' = \kappa$ follows from (0-24)). From (0-24) and (0-25) it is clear that A_1 is the adjacency matrix of a strongly regular graph with parameters (v, k', a, b) (see Subsection 0.4). We have thus shown the following.

Lemma 0.18.2. *A tactical configuration with the two indices $\mu_1 \neq \mu_2$ and incidence matrix A is partial geometric with parameters $(v, k, r; \alpha', \beta')$ if and only if there are integers ν and ζ such that for each pair $(x, b) \in V \times \mathcal{B}$,*

$$|\{y \in b \mid y \neq x, r_{xy} = \mu_1\}| = \begin{cases} \nu & (= n' + \alpha' - r + \mu_2), \textit{ if } x \in b, \\ \zeta & (= \alpha' - \mu_2 k), \textit{ otherwise}, \end{cases}$$

and A_1 is the adjacency matrix of a strongly regular graph with parameters (v, k', a, b) where $k' = \frac{\epsilon - \psi\sigma}{\phi}$, $a = \frac{\epsilon + \psi\phi - \sigma}{\phi}$ and $b = \frac{\epsilon}{\phi}$. Moreover, $k' = \frac{(k-1)r + \mu_2(1-v)}{\mu_1 - \mu_2}$.

It is interesting that Condition (0-23), when combined with (0-21), leads to the strongly regular graph described by (0-25). We can see that Lemma 0.18.2 describes a special class of block designs that have two indices. We now discuss a particular subclass of these block designs.

A tactical configuration $(V, \mathcal{B})$ with the two indices μ_1 and μ_2 such that $\mu_1 - \mu_2 = 1$ is called a 2-*adesign*. Adesigns were were recently introduced in [21], and reported on in [24] and [35], where several constructions are given, and codes generated by the incidence matrices are computed.

Theorem 0.18.1. *A 2-(v, k, λ) adesign with incidence matrix A is partial geometric with parameters $(v, k, r; \alpha', \beta')$ if and only if there are integers ν and ζ such that for each pair $(x, b) \in V \times \mathcal{B}$,*

$$|\{y \in b \mid y \neq x, r_{xy} = \mu_1\}| = \begin{cases} \nu & (= n' + \alpha' - r + \lambda), \text{ if } x \in b, \\ \zeta & (= \alpha' - \lambda k), \text{ otherwise}, \end{cases}$$

and A_1 is the adjacency matrix of a strongly regular graph with parameters (v, k', a, b) where $k' = \epsilon - \psi\sigma, a = \epsilon + \psi - \sigma$ and $b = \epsilon$. Moreover, the following relations hold: $\sigma = r - \lambda, \psi = n' - r + \lambda(k + 1), \epsilon = \lambda^2 v + \lambda(k + r - 2kr + \beta' - \alpha' - 1) + \alpha' r$ and $k' = (k - 1)r + \lambda(1 - v)$.

We can see that Theorem 0.18.1 describes a special class of 2-adesigns. There seem to be even fewer examples of these, and the few examples we can find have long since been discovered.

Example 0.18.1. *Partial geometries in which not every pair of points is contained in a line is one obvious example. It is clear that partial geometries satisfy the condition given in Lemma 0.18.1, and that we will have every pair of points contained either in one line, or in no line [7]. Partial geometries have extensive applications in combinatorics and information theory.*

Example 0.18.2. *Let $(V, \mathcal{B})$ be a quasi-symmetric design with intersection numbers s_1 and s_2 such that $s_2 - s_1 = 1$. Several families of such quasi-symmetric designs are known to exist* [45]. *It is well-known that the dual of any balanced incomplete block design is a partial geometric design* [41]. *Then the dual $(V, \mathcal{B})^{\perp}$ of $(V, \mathcal{B})$ is a partial geometric 2-adesign.*

Example 0.18.3. *Let p be an odd prime. Let D_i^{p+1} denote the ith cyclotomic class or order $p + 1$ in $\mathbb{F}_{p^2}$. It was shown in* [39] *that $(\mathbb{F}_{p^2}, Dev(D_i^{p+1}))$ is a partial geometric design. It is easy to see*

that $(\mathbb{F}_{p^2}, Dev(D_i^{p+1}))$ *has the two indices* $\mu_1 = 1$ *and* $\mu_2 = 0$ *(see* [38]*). Then* $(\mathbb{F}_{p^2}, Dev(D_i^{p+1}))$ *is a symmetric partial geometric* 2*-adesign.*

Example 0.18.4. *Let* C *be the partial geometric difference set from Theorem 0.16.3 in the Abelian group* $A \times B$ *of order* n^2*. Then* $(A \times B, Dev(C))$ *is a partial geometric design, and it was shown in* [3] *that* $(A \times B, Dev(C))$ *has the two indices* $\mu_1 = 1$ *and* $\mu_2 = 0$*. Then* $(A \times B, Dev(C))$ *is a symmetric partial geometric* 2*-adesign.*

0.19 Concluding Remarks

We have constructed several families of partial geometric difference sets and partial geometric difference families whose parameters are recorded in Table 0-3 and Table 0-4 respectively. These families have new parameters and so give directed strongly regular graphs with new parameters. We discussed some links between partially balanced designs, 2-adesigns, and partial geometric designs and made an investigation into when a 2-adesign is partial geometric. The condition noted in Lemma 0.18.2 seems surprisingly strong, and describes a special class of partial geometric designs that correspond (via (0-25)) to strongly regular graphs. The condition noted in Theorem 0.18.1 is also strong and describes a special class of 2-adesigns.

參考文獻

[1] G. E. Andrews. *Number Theory*, pages 128–132. W. B. Saunders Company, Philadelphia, Pa., 1971.

[2] A. Araluze, K. Kutnar, L. Martinez, and D. Marusic. Edge connectivity in difference graphs and some new contructions of partial sum families. *European Journal of Combinatorics*, 32:352–360, 2011.

[3] K. T. Arasu, C. Ding, P. V. T. Helleseth, Kumar, and H. M. Martinsen. Almost difference sets and their sequences with optimal autocorrelation. *IEEE Trans. Inform. Theory*, 47:2934–2943, 2001.

[4] L. D. Baumert and W. H. Hills. Uniform cyclotomy. *Journal of Number Theory*, 14:67–82, 1982.

[5] R. C. Bose. On the construction of balanced incomplete block designs. *Annals of Eugenics*, (9):358–399, 1939.

[6] R. C. Bose. On some new series of balanced incomplete block designs. *Bull. Calcutta Math. Soc.*, (34):17–31, 1942.

[7] R. C. Bose. Strongly regular graphs, partial geometries, and partially balanced deisgns. *Pacific Journal of Mathematics*, 13:389–419, 1963.

[8] R. C. Bose and S. S. Shrikhande. Edge regular multigraphs and partial geometric designs with an application to the embedding of quasi-residual designs. *Colloquio Internazionale sulle Teorie Combinatorie*, 1:49–81, 1976.

[9] A. E. Brouwer, O. Olmez, and S. Y. Song. Directed strongly regular graphs from $1\frac{1}{2}$-designs. *European Journal of Combinatorics*, 33(6):1174–1177, 2012.

[10] R. Calderbank and W.M. Kantor. The geomertry of two-weight codes. *Bull. London Math. Soc.*, 18:97–122, 1986.

[11] Z. Chai, R. Feng, and L. Zeng. Constructions of $1\frac{1}{2}$ designs from symplectic geometry over finite fields. *Acta mathematica Sinica, English Series*, 31(9).

[12] C. J. Colbourn and J. Dintiz (Eds.). *CRC Handbook of Combinatorial Designs*. CRC Press, Boca Raton, 1996.

[13] T. W. Cusick, C. Ding, and A. Renvall. *Stream Ciphers and Number Theory*. North-Holland, 1998.

[14] A. Davis. Almost difference sets and reversible difference sets. *Arch. Math.*, (59):595–602, 1992.

[15] P. Delsarte. An algebraic approach to association schemes of coding theory. *Phillips Res. Rep.*, (10), 1973.

[16] P. Dembowski. *Finite geometries*. Springer-Verlag, New York, 1968.

[17] L. E. Dickson. Cyclotomy, higher congruences and Waring's problem. *Amer. J. Math.*, 57:391–424, 1935.

[18] C. Ding. The differential cryptanalysis and design of the natural stream ciphers. *Proc. of FSE'93, LNCS 809 (Springer-Verlag)*, pages 101–115, 1994.

[19] C. Ding. Cyclic codes from the two-prime sequences. *IEEE Trans. Inform. Theory*, 58(6):3883–3890, 2012.

[20] C. Ding. Cyclic codes from cyclotomic sequences of order four. *Finite Fields and Their Applications*, 23:8–34, 2013.

[21] C. Ding. *Codes from Difference Sets*, page 75. World Scientific, 2015.

[22] 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.

[23] C. Ding, A. Pott, and Q. Wang. Constructions of almost difference sets from finite fields. *Des. Codes Cryptogr.*, 72:581–592, 2014.

[24] C. Ding and J. Yin. Constructions of almost difference families. *Discrete Mathematics*, (308):4941–4954, 2008.

[25] A. Duval. A directed graph version of strongly regular graphs. *Journal of Combinatorial Theorey, (A)*, 47:71–100, 1988.

[26] F. Fiedler, M. Klin, and C. Pech. Directed strongly regular graphs as elements of coherent algebras. *General Algebra and Discrete Mathematics: proceedings of the Conference on General Algebra and Discrete Mathematics, Postdam 1998*, pages 69–87, 1999.

[27] R. A. Fisher. An examination of the different possible solutions of a problem in incomplete blocks. *Annals of Eugenics*, 10:52–75, 1940.

[28] R. A. Fisher. An examination of the different possible solutions of a problem in incomplete blocks. *Annals of Eugenics*, 10:52–75, 1940.

[29] M. Grassl. Tables for linear codes. *Online at http://www.codetables.de*.

[30] J. W. P. Hirschfeld. *Projective geometries over finite feilds*. Oxford University Press, New York, 2nd edition, 1998.

[31] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.

[32] M. Hall Jr. A survey of difference sets. *Proc. AMS*, 7:975–986, 1956.

[33] M. Klin, A. Munemasa, M. Muzychuk, and P. H. Zieschang. Directed strongly regular graphs obtained from coherent algebras. *Linear Algebra and its Applications*, 377(15):83–109, 2004.

[34] J. Michel. New partial geometric difference sets and partial geometric difference families. *Acta Math. Sinica*, To appear.

[35] J. Michel and B. Ding. A generalization of combinatorial designs related to almost difference sets. *Des. Codes and Cryptogr.*, pages 1–19, 2016.

[36] E. H. Moore and H. S. Pollatsek. *Difference Sets: Connecting Algebra, Combinatorics, and Geometry*. American Mathematical Society, 2013.

[37] A. Neumaier. $t\frac{1}{2}$-designs. *Journal of Combinatorial Theory, (A)*, 78:226–248, 1980.

[38] K. Nowak. A survey on almost difference sets. *arXiv:1409.0114v1*, 2014.

[39] K. Nowak, O. Olmez, and S. Y. Song. Partial geometric difference families. *Journal of Combinatorial Designs*, pages 1–20, 2014.

[40] W. Ogata, K. Kurosawa, D. R. Stinson, and H. Saido. New combinatorial designs and their applications to authentication codes and secret sharing schemes. *Discrete Math.*, 279:384–405, 2004.

[41] O. Olmez. *On Highly Regular Digraphs*. PhD thesis, Iowa State University, 2012.

[42] O. Olmez. Symmetric $1\frac{1}{2}$-deisgns and $1\frac{1}{2}$-difference sets. *Journal of Combinatorial Designs*, 22(6):252–268, 2013.

[43] O. Olmez. Plateaued functions and one-and-half difference sets. *Des. Codes and Cryptogr.*, pages 1–13, 2014.

[44] O. Olmez and S. Y. Song. Some families of directed strongly regular graphs obtained from certain finite incidence structures. *Graphs and Combinatorics*, 30(6):1529–1549, 2014.

[45] R. M. Pawale. Quasi-symmetric designs with fixed difference of block intersection numbers. *Journal of Combinatorial Designs*, 15(1):49–60, 2007.

[46] E. M. Rains. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory*, 44(1):134–139, 1998.

[47] D. R. Stinson. *Combinatorial Designs: Constructions and Analysis*. SpringerVerlag, 2003.

[48] X. H. Tang and G. Gong. New constructions of binary sequences with optimal autocorrelation magnitude/value. *IEEE Trans. Inform. Theory*, 56(3):1278–1286, 2010.

[49] X. Wang and J. Wang. A note on cyclic almost differnce families. *Discrete Mathematics*, 311(8–9):628–633, 2011.

[50] A. L. Whiteman. The cyclotomic numbers of order ten. *Acta Arith.*, 10:95–111, 1960.

[51] F. Yates. *The design and analysis of factorial experiments*. Imperial Bureau of Soil Science, 1937.

[52] N. Y. Yu and G. Gong. New binary sequences with optimal autocorrelation. *IEEE Trans. Inform. Theory*, 54(10):4771–4779, 2008.

[53] L. Zeng, Z. Chai, and R. Feng. Full automorphism group of the generalized symplectic graph. *Sci. China Math.*, 56(7):1509–1520, 2013.

[54] Y. Zhang, J. G. Lei, and S. P. Zhang. A new family of almost difference sets and some necessary conditions. *IEEE Trans. Inform. Theory*, 52(5):2052–2061, 2006.

Publications

As First Author:

1. *A Note on Directed Strongly Regular Graphs*, Graphs and Combinatorics, Springer, Accepted and to appear 2016.

2. *Experimental Constructions of Binary Matrices with Good peak-Sidelobe Distances*, Journal of Vacuum Science and Technology B, Accepted and to appear 2016.

3. *A Generalization of Combinatorial Designs and Related Codes*, Designs, Codes and Cryptography, Springer, pp 1-19, 2016.

4. *New Partial Geometric Difference Sets and Partial Geometric Difference Families*, Acta Mathematica Sinica, English Series, Springer, Accepted and to appear, 2016.

Joint Work:

1. *On the existence of certain optimal self-dual codes with lengths between 74 and 116*, Electronic Journal of Combinatorics, pp 1-25, 2015.