# A NEW CLASS OF DESIGNS AND SINGLY OR DOUBLY EQUIVALENT DESIGNS

BY

MO LIANG

A Thesis
Submitted to the Faculty of Graduate Studies
in Partial Fulfillment of the Requirements
for the Degree of

## DOCTOR OF PHILOSOPHY

Department of Mathematics
University of Manitoba
Winnipeg, Manitoba
Canada

0-612-53064-7

THE UNIVERSITY OF MANITOBA

FACULTY OF GRADUATE STUDIES

*****

COPYRIGHT PERMISSION PAGE

# A New Class of Designs and Singly or Doubly Equivalent Designs

BY

Mo Liang

A Thesis/Practicum submitted to the Faculty of Graduate Studies of The University of Manitoba in partial fulfillment of the requirements of the degree

of

Doctor of Philosophy

# Acknowledgements

I am deeply indebted to my advisor Dr. N. S. Mendelsohn for having supervised me in my Master and PhD programs successively. He introduced me to this topic of research. His excellent guidance has been invaluable and is gratefully acknowledged.

I would also like to specially thank the other members of my Advisory Committee: Professor Michael Doob and Professor John van Rees. They have taken the time and trouble to carefully read this thesis and provided many valuable suggestions. I would also wish to thank in particular Professor Lynn Batten and Professor R. Padmanabhan for being kindly helpful and giving me encouragement for all those years in my programs at University of Manitoba. A special thanks to Dr. J. A. Gerhard for his great and continuous help. Many thanks also to the General Office of the Department of Mathematics as well as my fellow graduate students who have offered me different kinds of valuable help: Zhang Yong, Zhang Xuebin, Yang Xiao, Iraghi Moghaddam. I give sincere thanks to Barry Wolk, Dr. C. R. Platt, Michelle Davidson, Michael Potter, Michael Newman etc, for kindly answering my English or computer questions.

I would like to express my deepest appreciation and memory to my very hard-working aunt Zhang Sufen who kindly took care of me when I was growing up. Unfortunately, she passed away on December 31, 1996 in China at the age 88 while I was here in Canada. Finally, I wish to express my most sincere gratitude to my parents for their invaluable guidance, support and encouragement.

# Abstract

We are already familiar with $(v, k, \lambda)$-difference sets and $(v, k, \lambda)$-designs. In this thesis, we will introduce a new class of difference sets and designs: $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-difference sets and $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-designs. We will also introduce the concepts of singly equivalent designs and doubly equivalent designs.

In Chapter 2, we will discuss some necessary conditions and nonexistence theorems.

In Chapter 3, we will first discuss the necessary and sufficient conditions for a $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-designs to be a singly equivalent design. We will prove that a $\lambda_2$-equivalent $(v, k, [\lambda_1, \lambda_2]: t)$-difference set is a $(\alpha, t+1, k, \lambda_2, \lambda_1)$-DDS. We will show that a 0-equivalent $(n^2-1, n, [1, 0])$--design can be embedded into an affine plane. We will also prove that for a 0-equivalent $(v, k, [\lambda, 0]: t)$-design if $t \geq 2$ then the point 0 is missing from at least one parallel class. Define $u$ to be the number of parallel classes missing the point 0. We have obtained that up to isomorphism $\{0, 1\}$ mod 4 is the only 0-equivalent $(v, k, [\lambda, 0]: t)$-design with $u = 0$. We can attain a "standard" difference set from a 0-equivalent $(v, k, [\lambda, 0]: t)$-design with $u > 1$. We will also prove that we can add some points to a base set of a 0-equivalent $(v, k, [\lambda, 0]: t)$-design with $u = 1$ and get a set which generates a $(t+1)$-

-equivalent $(v, k+t+1, [\lambda+2, t+1]; t)$-design or a $(v, k+t+1, \lambda+2)$-design.

In Chapter 4, we will discuss doubly equivalent designs as well as the notion of super classes. We will describe the structure of super classes and discuss properties of doubly equivalent designs. We will extend results of singly equivalent designs to doubly equivalent designs.

In Chapter 5, we will give an example to construct a $(v, k, [\lambda_1, \lambda_2, \lambda_3])$--design. Some more general necessary conditions and existence theorems than those in Elliott and Butson [12], Ryser [35], Wei, Gao and Yang [37] and/or Theorem 2.44 in Chapter 2 will be given. We will also show how to construct difference sets from $(v, k, [\lambda, 0])$-difference sets.

Many other results will be also given.

We will include the tables of singly equivalent difference sets obtained by computers as appendixes. We will also include a $C^{++}$ program to search $(v, k, [\lambda_1, \lambda_2])$-difference sets.

# Contents

# Chapter 1

# Old Designs

In this Chapter, first we will quote some definitions and results of "standard" designs. In Chapter 2, we will define a new class of designs and try to generalize the results on normal designs to our new designs. For more details about the discussion of this part, one may check M. Hall [13]. In the second part of this Chapter, we will review some existing papers on partial difference sets, relative difference sets and near difference sets.

**Definition 1.1.** *A* $(v, b, r, k, \lambda)$***-design*** *is an arrangement of $v$ distinct objects $a_1, a_2, \ldots, a_v$ into $b$ blocks $B_1, B_2, \ldots, B_b$ such that each block contains exactly $k$ distinct objects, each object occurs in exactly $r$ different blocks, and every pair of distinct objects $a_i, a_j$ occurs together in exactly $\lambda$ blocks.*

**Theorem 1.2.** *For a $(v, b, r, k, \lambda)$-design,*

$$bk = vr, \tag{1.1}$$

*and*

$$r(k-1) = \lambda(v-1). \tag{1.2}$$

**Definition 1.3.** *The* ***incidence matrix*** *of a* $(v, b, r, k, \lambda)$*-design is a* $v \times b$ *matrix* $A = [a_{ij}]$ *with*

$$a_{ij} = \begin{cases} 1 & \text{if } a_i \in B_j \\ 0 & \text{if } a_i \notin B_j. \end{cases}$$

*where* $a_1, \ldots, a_v$ *are the objects and* $B_1, \ldots, B_b$ *are the blocks.*

**Definition 1.4.** *A* $(v, b, r, k, \lambda)$*-design is called a* $\boldsymbol{(v, k, \lambda)}$***-design*** *if* $v = b$ *(and thus* $k = r$*).*

**Theorem 1.5.** *Let* $A$ *be the incidence matrix of a* $(v, k, \lambda)$*-design. Then*

$$AA^T = B = (k - \lambda)I + \lambda J,$$

$$A^T A = B = (k - \lambda)I + \lambda J,$$

$$JA = AJ = kJ,$$

*where* $J$ *is the* $v \times v$ *matrix of all* 1*'s.*

**Theorem 1.6.** *If a* $(v, k, \lambda)$*-design exists, letting* $n = k - \lambda$*, then:*
*(1) if* $v$ *is even, then* $n$ *is a square;*
*(2) if* $v$ *is odd,* $z^2 = nx^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$ *has a solution in integers* $x, y, z$ *not all zero.*

There are many types of constructions of $(v, b, r, k, \lambda)$-designs and $(v, k, \lambda)$--designs ([13] and [9]). One of the most interesting generalizations occurs when the number $k$ is replaced by a set $\{k_1, k_2, k_3, \ldots, k_m\}$ of distinct numbers. The corresponding designs are referred to as pairwise balanced designs or sometimes as linear spaces.

These designs have been explored by many but especially by H. Hanani [14] and R.M. Wilson [38, 39, 40]. The ultimate result was Wilson's Asymptotic Theorem.

In the present thesis instead of replacing $k$ by $\{k_1, k_2, k_3, \dots, k_m\}$, we replace $\lambda$ by $\{\lambda_1, \lambda_2, \dots, \lambda_m\}$, and we study these designs which we call $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$-designs and use them to produce other designs.

$(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$-designs with $m \geq 3$ have very rarely been studied in the past. In 1982, J. Sumner and A. T. Butson [36] introduced a concept of a very special difference set with different values of $\lambda$'s which was called a generalized relative difference set. However, no properties of generalized relative difference sets were developed in that paper. In 1992, J. Y. Xu [41] studied relative difference sets in a finite group $G = G_1 \times G_2$. Under other names, partial difference sets, relative difference sets or near difference sets. $(v, k, [\lambda, \mu])$-designs have been studied. These designs come from strongly regular graphs, quadratic residues of $GF(q)$ ($p \equiv 1 \bmod 4$), and $(v, k, [\lambda, 0])$--designs. This work appears in D. Jungnickel [18], S. L. Ma [25, 26, 27], C. Koukouvinos and A. L. Whiteman [21, 22], and P. A. Leonard [24].

The concept of a relative difference set was introduced by A. T. Butson [7] in 1963. D. Jungnickel [18] has considered divisible designs, so called because of their role as the automorphism group of cyclic (group) divisible designs, see [9].

**Definition 1.7.** *Given a group $G$ of order $mn$ containing a normal subgroup $N$ of order $n$, a* ***divisible difference set****, denoted by* $\boldsymbol{(m, n, k, \lambda_1, \lambda_2)}$**-**-***DDS****, is a $k$-subset of $G$ such that the list of differences $d - d'$ with $d \neq d'$, $d, d' \in D$, covers every element in $N \backslash \{0\}$ exactly $\lambda_1$ times and every element* *in $G \backslash N$ exactly $\lambda_2$ times, where $m > 1$.*

*If $\lambda_1 = 0$, then the divisible difference set $D$ is referred as a* ***relative difference set*** *(of $G$ relative to $N$) and is denoted by* $\boldsymbol{(m, n, k, \lambda)}$*-**RDS**, where $\lambda = \lambda_2$.*

In 1966, J. E. H. Elliott and A. T. Butson [12] studied relative difference sets. They gave some existence theorems and multiplier theorems for relative difference sets, and also showed how to construct some relative difference sets. In 1970, S. E. Payne [31] gave a nonexistence theorem for relative difference sets. In 1974, F. Piper [32] studied relative difference sets of a quasiregular collineation group. In 1989, D. Jungnickel [19] gave a construction of a family of relative difference sets with special parameters. In 1995, K. T. Arasu, D. Jungnickel, S. L. Ma and A. Pott investigated the existence of relative $(m, 2, k, \lambda)$-RDS's of a group $H \times N$ relative to $N$. In 1996, D. K. Ray-Chaudhuri and Q. Xiang [33], and Y. Q. Chen, D. K. Ray-Chaudhuri and Q. Xiang [8] studied the constructions of partial difference sets and relative difference sets using Galois rings. In 1996, C. Koukouvinos and A. L. Whiteman [22] gave more constructions of relative difference sets.

In 1973, H. J. Ryser [35] introduced the concept of a near difference set of type 1.

**Definition 1.8.** *Let $v \geq 4$ be an even integer, and $k$, $\lambda$ positive integers. Suppose that $D = \{a_1, a_2, \dots, a_k\}$ is a set of $k$ residues modulo $v$ with the property that for any residue $a \not\equiv 0, \frac{v}{2}$ (mod $v$), the congruence equation*

$$a_i - a_j \equiv a \ (mod\ v), \ a_i, a_j \in D$$

*has exactly $\lambda$ solution pairs $(a_i, a_j)$ and no solution pair for the residue $a \equiv \frac{v}{2}$*

*(mod $v$). Then $D$ is is called a* $(\boldsymbol{v}, \boldsymbol{k}, \boldsymbol{\lambda})$***-near difference set of type*** 1.

Actually, a $(v, k, \lambda)$-near different set of type 1 is a $(m, n, k, \lambda)$-RDS with $m = \frac{v}{2}$, $n = 2$. Although the study of relative difference sets appeared much earlier, Ryser did not point out the relationship between relative difference sets and near difference sets of type 1. In 1993, W. D. Wei, S. Gao and B. Yang [37] gave some nonexistence theorems, uniqueness theorems and constructions of some near difference sets of type 1. In 1995, C. Koukouvinos and A. L. Whiteman [21] studied near difference sets of another type, giving some nonexistence theorems and showing how to construct some near difference sets.

The present thesis mainly studies designs with a relationship we call $\lambda$--equivalence. We also introduce the parameter $u$. To the best of our knowledge, our approach of considering $\lambda$-equivalence classes and introducing the parameter $u$ are new. We also extend some results of relative difference sets and near difference sets of type 1 to our difference sets.

# Chapter 2

# Generalized Designs

In this Chapter, we will define a new class of designs and discuss some of its properties.

## 2.1 $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-designs

**Definition 2.1.** *A* $(\boldsymbol{v}, \boldsymbol{b}, \boldsymbol{r}, \boldsymbol{k}, [\boldsymbol{\lambda_1}, \boldsymbol{\lambda_2}, \ldots, \boldsymbol{\lambda_m}])$***-design*** *is an arrangement of $v$ distinct objects $a_1, a_2, \ldots, a_v$ into $b$ blocks $B_1, B_2, \ldots B_b$ such that each block contains exactly $k$ distinct objects, each object occurs in exactly $r$ different blocks, and every pair of distinct objects $a_i, a_j$ occurs together in exactly $\lambda_1, \lambda_2, \ldots,$ or $\lambda_m$ blocks, while for each $\lambda_s$ $(s = 1, 2, \ldots, m)$, there exists at least one pair $a_i, a_j$ $(i \neq j)$ appearing together in exactly $\lambda_s$ blocks.*

**Theorem 2.2.** *For a $(v, b, r, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-design,*

$$bk = vr \tag{2.1}$$

*Proof.* Since each of the $b$ blocks contains exactly $k$ distinct objects and since each of the $v$ objects occurs in exactly $r$ different blocks, counting the total number of incidences, we obtain that $bk = vr$. □

**Definition 2.3.** *The **incidence matrix** of a $(v, b, r, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-design is a $v \times b$ matrix $A = [a_{ij}]$ with*

$$a_{ij} = \begin{cases} 1 & \text{if } a_i \in B_j \\ 0 & \text{if } a_i \notin B_j. \end{cases}$$

*where $a_1, \ldots, a_v$ are the objects and $B_1, \ldots, B_b$ are the blocks.*

**Definition 2.4.** *A $(v, b, r, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-design is called a $(\boldsymbol{v}, \boldsymbol{k}, [\boldsymbol{\lambda_1}, \boldsymbol{\lambda_2}, \ldots, \boldsymbol{\lambda_m}])$**-design** if $v$=$b$ (and thus $k$=$r$).*

We now extend the third result in Theorem 1.5 to

**Theorem 2.5.** *Let $A$ be the incidence matrix of a $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-design. Then*

$$JA = AJ = kJ,$$

*where $J$ is the $v \times v$ matrix of all 1's.*

*Proof.* Let $JA = [b_{ij}]$ and $AJ = [c_{ij}]$, then

$$b_{ij} = \text{the number of objects contained in the block } B_j,$$

and

$$c_{ij} = \text{the number of blocks containing the object } a_i.$$

So,

$$b_{ij} = c_{ij} = k.$$

Therefore,

$$JA = AJ = kJ.$$

□

**Definition 2.6.** *Let $S = \{a_1, a_2, a_3, \ldots, a_k\}$ be a set of $k$ distinct residues mod $v$. We say that $S$ is a* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$***-difference set*** *if*

*(1) For each $d \not\equiv 0$ (mod $v$) there are exactly $\lambda_1, \lambda_2, \ldots$ or $\lambda_m$ ordered pairs $(a_i, a_j)$, where $a_i, a_j \in S$, such that $a_i - a_j \equiv d$ (mod $v$).*

*(2) For each $\lambda_s$ $(s = 1, 2, \ldots, m)$, there exists at least one $d \not\equiv 0$ (mod $v$) such that there are exactly $\lambda_s$ ordered pairs $(a_i, a_j)$, where $a_i, a_j \in S$, satisfying $a_i - a_j \equiv d$ (mod $v$).*

Thus the definition of a $(v, k, [\lambda_1, \lambda_2, \ldots \lambda_m])$-difference set generalizes the notion of a divisible difference set of $\mathbf{Z}_v$ in two ways: by relaxing the subgroup condition and by allowing an arbitrary number of $\lambda$s. Example 3.2 in Chapter 3 is an example that a $(15, 4, [1, 0] : 2)$-difference set is not a divisible difference set nor a relative difference set.

**Example 2.7.** $\{0, 1, 2, 5, 10\}$ *mod* 12 *is a* $(12, 5, [2, 0])$*-difference set since the multiset of its differences is*

$$\begin{array}{llll}
\pm 1 & \pm 2 & \pm 5 & \pm 10 \\
\pm 1 & \pm 4 & \pm 9 & \\
\pm 3 & \pm 8 & & \\
\pm 5, & & &
\end{array}$$

*and* $\pm 10 \equiv \mp 2$ *(mod* 12*),* $\pm 9 \equiv \mp 3$ *(mod* 12*) and so on.* 6 *is missing from the multiset of its differences.*

**Theorem 2.8.** *Let* $S = \{a_1, a_2, a_3, \ldots, a_k\}$ *be a* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$*-difference set and* $B_i$ *be the sets:* $\{a_1 + i, a_2 + i, a_3 + i, \ldots, a_k + i\}$ *mod* $v$, $i = 0, \ldots, v-1$. *If* $j < i$ *and* $1 \leq e \leq m$, *then the following three statements are equivalent to each other:*

*(1)* $i - j$ *appears as a difference* $\lambda_e$ *times in* $S$*;*

*(2)* $B_i$ *and* $B_j$ *have* $\lambda_e$ *objects in common;*

*(3)* $i$ *and* $j$ *appear together in* $\lambda_e$ *blocks.*

*Proof.* The difference of two objects $a_r$ and $a_s$ in $S$ is $i-j$ if and only if they contribute one common object to the two blocks $B_i$ and $B_j$. So, (1) and (2) are equivalent.

Every appearance of $i-j$ as a difference in $S$ contributes one appearance of pair $i, j$ together in a block and vice versa. So, (1) and (3) are equivalent. □

**Corollary 2.9.** *For a* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$*-difference set.* $\lambda_i \leq k$ *for* $i = 1, 2, \ldots, m$.

*Proof.* Two sets $B_i$ and $B_j$ cannot have more that $k$ objects in common. So, by Theorem 2.8, the conclusion is true. □

**Theorem 2.10.** $S = \{a_1, a_2, a_3, \ldots, a_k\}$ *is a* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$*-difference set if and only if the sets* $B_i$*:* $\{a_1 + i, a_2 + i, a_3 + i, \ldots, a_k + i\}$ *mod* $v$, $i = 0, \ldots, v-1$ *are a* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$*-design.*

*Proof.* Using the fact that statements (1) and (3) of Theorem 2.8 are equivalent, it is not hard to prove this theorem. □

**Definition 2.11.** *Under the assumption of Theorem 2.10, the design in Theorem 2.10 is called the* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$***-design generated by the*** $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$***-difference set*** $S$ *and* $S$ *is called a* ***base set*** *of the design.*

From now on, we just discuss $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-designs generated by $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-difference sets. Therefore, whenever we mention a $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-design, it always means a design generated by a $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-difference set except when we specify otherwise.

The following Definition generalizes the Definition on p 147 of M. Hall [13].

**Definition 2.12.** *Two designs* $D$ *and* $D'$ *are said to be* ***isomorphic*** *if there is a one-to-one mapping* $\phi$ *of objects and blocks of* $D$ *onto those of* $D'$ *satisfying that if* $x_i$ *is an object,* $B_j$ *is a block of* $D$.

$$\phi : x_i \to x'_i = \phi(x_i), \text{ an object of } D',$$

$$\phi : B_j \to B'_j = \phi(B_j), \text{ a block of } D',$$

*then* $x_i \in B_j$ *if and only if* $\phi(x_i) \in \phi(B_j)$.

**Definition 2.13.** *Two difference sets are called* ***isomorphic*** *if they generate isomorphic designs. We use* $\boldsymbol{S \simeq T}$ *to denote that difference sets* $S$ *and* $T$ *are isomorphic.*

**Theorem 2.14.** *If* $S = \{a_1, a_2, a_3, \ldots, a_k\}$ *is a* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_{m-1}, 0])$*-difference set, then* $T = \{a \cdot a_1, a \cdot a_2, a \cdot a_3, \ldots, a \cdot a_k\}$*, where* $a$ *is a positive integer, is an* $(a \cdot v, k, [\lambda_1, \lambda_2, \ldots, \lambda_{m-1}, 0])$*-difference set.*

*Proof.* This theorem follows from the fact that when $a \neq 0$ we have $a \cdot \alpha \equiv a \cdot \beta$ (mod $a \cdot v$) if and only if $\alpha \equiv \beta$ (mod $v$), where $\alpha$, $\beta$ are integers. □

**Definition 2.15.** *Under the assumption of Theorem 2.14, we call the difference set $T$ in Theorem 2.14 a* ***multiple*** *of $S$.*

We extend the results on pp 134-135 in H. J. Ryser [34] to

**Theorem 2.16.** *If $S = \{a_1, a_2, a_3, \ldots, a_k\}$ is a $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$--difference set, then $T = \{a \cdot a_1 + b, a \cdot a_2 + b, a \cdot a_3 + b, \ldots, a \cdot a_k + b\}$ (mod $v$), where $a$, $b$ are integers and $(a, v) = 1$, is also a $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-difference set and $S \simeq T$.*

*Proof.* The first result can be derived from the fact that when $(a, v) = 1$ we have $a \cdot \alpha \equiv a \cdot \beta$ (mod $v$) if and only if $\alpha \equiv \beta$ (mod $v$), where $\alpha$, $\beta$ are integers. It is easy to show that $S \simeq T$. □

By this theorem, normally we just consider the case of $a_1 = 0$.

## 2.2 Nonexistence Theorems

**Definition 2.17.** *Let $D = \{a_1, a_2, a_3, \ldots, a_k\}$ be a set of $k$ distinct residues mod $v$. We say that $D$ is a* **$\lambda$-difference set** *if any difference $a_i - a_j$ appears $\lambda$ or 0 times.*

**Example 2.18.** $S_1 = \{0, 1, 2, 5\}$ *mod 7 is a 2-difference set since the multiset of differences is*

$$\begin{array}{lll} \pm 1 & \pm 2 & \pm 5 \\ \pm 1 & \pm 4 & \\ \pm 3, & & \end{array}$$

*and* $\pm 5 \equiv \mp 2 \pmod 7$, $\pm 4 \equiv \mp 3 \pmod 7$ *and so on.*

**Theorem 2.19.** *If* $S = \{a_1, a_2, a_3, ..., a_k\}$ *mod* $v$ *is a* $\lambda$*-difference set, then* $T = \{a \cdot a_1, a \cdot a_2, a \cdot a_3, ..., a \cdot a_k\}$ *mod* $a \cdot v$*, where* $a$ *is a positive integer, is also a* $\lambda$*-difference set.*

*Proof.* This theorem follows from the fact that when $a \neq 0$ we have $a \cdot \alpha \equiv a \cdot \beta \pmod{a \cdot v}$ if and only if $\alpha \equiv \beta \pmod v$, where $\alpha$, $\beta$ are integers. □

**Definition 2.20.** *Under the assumption of Theorem 2.19, we call the difference set* $T$ *in Theorem 2.19 a* ***multiple*** *of* $S$.

**Theorem 2.21.** *If* $S = \{a_1, a_2, a_3, ..., a_k\}$ *mod* $v$ *be a* $\lambda$*-difference set, then* $T = \{a \cdot a_1 + b, a \cdot a_2 + b, a \cdot a_3 + b, ..., a \cdot a_k + b\}$ *mod* $v$*, where* $a$, $b$ *are integers and* $(a, v) = 1$*, is also a* $\lambda$*-difference set, and* $T$ *is isomorphic to* $S$.

*Proof.* This theorem can be derived from the fact that when $(a, v) = 1$ we have $a \cdot \alpha \equiv a \cdot \beta \pmod v$ if and only if $\alpha \equiv \beta \pmod v$, where $\alpha$, $\beta$ are integers. □

By this theorem, normally we just consider the case of $a_1 = 0$.

**Example 2.22.** $T_1 = \{0, 1, 3, 6\}$ *mod 7 and* $T_2 = \{0, 2, 3, 4\}$ *mod 7 are 2-difference sets.*

From $S_1$ in Example 2.18, by Theorem 2.21, let $a = 3$ and $b = 0$, we obtain $T_1$. From $S_1$, let $a = 2$ and $b = 0$, we obtain $T_2$.

**Example 2.23.** *$T_3 = \{0, 1, 2, 4\}$ mod 7 is a 2-difference set.*

From $S_1$, by Theorem 2.21, let $a = -1$ and $b = 2$, we obtain $T_3$.

**Corollary 2.24.** *If $S = \{a_1, a_2, a_3, ..., a_k\}$ mod $v$ is a $\lambda$-difference set, then $T = \{v - a_1, v - a_2, v - a_3, ..., v - a_k\}$ mod $v$ is also a $\lambda$-difference set.*

*Proof.* By Theorem 2.21, let $a = -1$ and $b = 0$, we get that

$$T = \{v - a_1, v - a_2, v - a_3, ..., v - a_k\} \text{ mod } v$$

is a $\lambda$-difference set. □

**Example 2.25.** *$T_4 = \{0, 1, 4, 6\}$ mod 7 is a 2-difference set.*

Applying Corollary 2.24 on $T_1$, we get $T_4$.

**Theorem 2.26.** *For $k = 4$, up to the multiple and isomorphism, there is just one 2-difference set, which is $S_1$ as shown in Example 2.18.*

*Proof.* Let $S = \{0, a, b, c\}$ mod $v$ be a 2-difference set. By relabeling elements and Corollary 2.24, we can assume, without loss of generality, that $0 < a < b < c$ and $b \leq \lfloor \frac{v}{2} \rfloor$, where $\lfloor \frac{v}{2} \rfloor$ is the largest integer which is not greater than $\frac{v}{2}$. Since there is a difference $a$ coming from $a - 0$, the second difference $a$ might come from $\pm(b - 0)$, $\pm(c - 0)$, $\pm(b - a)$, $\pm(c - a)$, or $\pm(c - b)$. This leads to five cases:

Case I. The second difference $a$ comes from $\pm(b - 0) = \pm b$. Obviously, this is impossible since first $a \neq b$ and second $a \not\equiv -b$ (mod $v$) because $0 < a + b < v$.

Case II. The second difference $a$ comes from $\pm(c-0)=\pm c$. Since $a<c$ so we have $a+c=v$ and the 2-difference set should be $S=\{0,a,b,v-a\}$ mod $v$. The multiset of its differences is

$$\begin{array}{lll} \pm a & \pm b & \pm(v-a) \\ \pm(b-a) & \pm(v-2a) & \\ \pm(v-a-b). & & \end{array}$$

The second difference $b$ might come from $\pm(b-a)$, $\pm(v-2a)$, or $\pm(v-a-b)$ and this leads to three sub-cases:

(1) It comes from $\pm(b-a)$. Then since $a\neq 0$ we have $b+(b-a)=v$. It follows that $b=\frac{v+a}{2}>\frac{v}{2}$, which contradicts $b\leq\lfloor\frac{v}{2}\rfloor$.

(2) It comes from $\pm(v-2a)$. If $b=v-2a$, then $v-a-b=a$, which means $a$ appears more than two times in the multiset of differences, and so this leads to a contradiction. If $b+(v-2a)=v$, then $b=2a$. Thus $a$ also appears more than two times in the multiset of differences, which is impossible.

(3) It comes from $\pm(v-a-b)$. If $b=v-a-b$, then $2b=v-a$. We have $b=\frac{v-a}{2}$. Now considering the remaining difference, $b-a=\pm(v-2a)$, we have $b-a=\frac{v-3a}{2}=v-2a$ or $\frac{v-3a}{2}+(v-2a)=v$. For the former, we get $v-3a=2v-4a$. Thus $v=a$; impossible. For the latter, we have $v-3a=4a$. So $v=7a$ and $b=\frac{v-a}{2}=3a$. Therefore, $S=\{0,a,3a,6a\}$ mod $7a$, which is a multiple of $T_1$.

Case III. The second difference $a$ comes from $\pm(b-a)$. Since $a+(b-a)=b\neq v$, we have $a=b-a$, i.e., $b=2a$. So the 2-difference set is

$S = \{0, a, 2a, c\}$ mod $v$. The multiset of difference is

$$\begin{array}{lll} \pm a & \pm 2a & \pm c \\ \pm a & \pm(c-a) & \\ \pm(c-2a). & & \end{array}$$

The second difference $c$ might come from $\pm 2a$, $\pm(c-a)$, or $\pm(c-2a)$ and this leads to three sub-cases:

(1) It comes from $\pm 2a$. Since $c > 2a = b$, we have $c + 2a = v$. It follows that $c - a = v - 3a$ and $c - 2a = v - 4a$. So, $(v - 3a) + (v - 4a) = v$. This leads $v = 7a$ and $c = 5a$. Thus $S = \{0, a, 2a, 5a\}$ mod $7a$, which is a multiple of $S_1$.

(2) It comes from $\pm(c - a)$. If $c = c - a$, then $a = 0$: impossible. If $c + (c - a) = v$, then $2c = v + a$. Thus $c = \frac{v+a}{2}$. We have $c - 2a = \frac{v+a}{2} - 2a =$ $= \frac{v-3a}{2} = 2a$ or $\frac{v-3a}{2} + 2a = v$. If $\frac{v-3a}{2} = 2a$, then $v - 3a = 4a$, so $v = 7a$ and $c = 4a$. We get $S = \{0, a, 2a, 4a\}$ mod $7a$, which is a multiple of $T_3$. If $\frac{v-3a}{2} + 2a = v$, then $v - 3a + 4a = 2v$. So, $v = a$: contradiction.

(3) It comes from $\pm(c - 2a)$. If $c = c - 2a$, then $a = 0$: impossible. If $c + (c - 2a) = v$, then $2c = v + 2a$. Thus $c = \frac{v+2a}{2}$. We have $c - a = \frac{v+2a}{2} - a =$ $= \frac{v}{2} = 2a$ or $\frac{v}{2} + 2a = v$. In both cases, we have $v = 4a$. So $c = \frac{v+2a}{2} = 3a$. We have $S = \{0, a, 2a, 3a\}$ mod $4a$, which is not a 2-difference set since $a$ appears more than two times in the multiset of differences.

Case IV. The second difference $a$ comes from $\pm(c - a)$. We have $a + (c - a) = c \neq v$. So, $a = c - a$, i.e., $c = 2a$. The 2-difference set should be $S = \{0, a, b, 2a\}$ mod $v$. The multiset of differences is

$$\begin{array}{lll} \pm a & \pm b & \pm 2a \\ \pm(b-a) & \pm a & \\ \pm(2a-b). & & \end{array}$$

The second difference $b$ might come from $\pm 2a$, $\pm(b-a)$, or $\pm(2a-b)$ and this leads to three sub-cases:

(1) It comes from $\pm 2a$. The only possibility is $b+2a = v$ since $b < 2a = c$. Thus $b = v - 2a$. $b - a = v - 3a$ and $2a - b = 2a - (v - 2a) = 4a - v$. So, $(v - 3a) + (4a - v) = v$ or $v - 3a = 4a - v$. If $(v - 3a) + (4a - v) = v$, then $a = v$: impossible. If $v - 3a = 4a - v$, then $2v = 7a$. Let $a = 2d$, where $d$ is a positive integer. Then $v = 7d$. Thus $b = 3d$ and $c = 4d$. And $S = \{0, 2d, 3d, 4d\}$ mod $7d$, which is a multiple of $T_2$.

(2) It comes from $\pm(b - a)$. The only possibility is $b + (b - a) = v$ since $b \neq b - a$. So $2b = v + a$. It follows that $b = \frac{v+a}{2} > \frac{v}{2}$, which is impossible since $b \leq \lfloor \frac{v}{2} \rfloor$.

(3) It comes from $\pm(2a - b)$. This will cause $a = b$ or $v = 2a = c$. Both are impossible.

Case V. The second difference $a$ comes from $\pm(c-b)$. Since $0 < c-b+a <$ $< c < v$, we have $c-b+a \neq v$. So, $a = c-b$, i.e., $c = a+b$. The 2-difference set is $S = \{0, a, b, a+b\}$ mod $v$. The multiset of differences is

$$\begin{array}{lll} \pm a & \pm b & \pm(a+b) \\ \pm(b-a) & \pm b & \\ \pm a. & & \end{array}$$

So, $(b - a) + (b + a) = v$. Thus $v = 2b$. Since $-b \equiv b \pmod{2b}$, $b$ in fact appears at least four times as a difference, which leads to a contradiction.

This finishes our proof. □

Since $S_1$ in Example 2.18 does not miss any nonzero residue as a difference, it is not a $(v, 4, [2, 0])$-difference set. We have:

**Corollary 2.27.** *There does not exist any* $(v, 4, [2, 0])$*-difference set* $S = \{0, a, b, c\}$ *mod* $v$, *if* $(a, b, c, v) = 1$.

Similarly, but more easily, we can prove:

**Theorem 2.28.** *There does not exist any* $(v, 3, [2, 0])$*-difference set* $S = \{0, a, b\}$ *mod* $v$, *if* $(a, b, v) = 1$.

## 2.3 $(v, k, [\lambda_1, \lambda_2]; t)$-designs

**Definition 2.29.** *A* $(v, k, [\lambda, 0])$*-difference set* $S$ *is called a* $\boldsymbol{(v, k, [\lambda, 0]; t)}$***-difference set*** *if there are exactly* $t$ *distinct nonzero residues* $d_1, d_2, \ldots, d_t$ *mod* $v$ *such that there are no ordered pairs* $(a_i, a_j)$, $a_i, a_j \in S$, *satisfying* $a_i - a_j \equiv d_1, d_2, \ldots,$ *or* $d_t \pmod v$. *The design generated by a* $(v, k, [\lambda, 0]; t)$*-difference set is called* $\boldsymbol{(v, k, [\lambda, 0]; t)}$***-design***.

Therefore, in a $(v, k, [\lambda, 0]; t)$-difference set, there are exactly $t$ distinct nonzero residues missing from the multiset of its differences while each of the other nonzero residues appears as a difference exactly $\lambda$ times. $t + 1$ corresponds to the parameter $n$ in a $(m, n, k, \lambda_1, \lambda_2)$-DDS.

**Example 2.30.** *The difference set in Example 2.7 is a* $(12, 5, [2, 0]; 1)$-

*-difference set. It generates a* $(12, 5, [2, 0]; 1)$*-design:*

| | | | | |
|---|---|---|---|---|
| 0, | 1, | 2, | 5, | 10 |
| 1, | 2, | 3, | 6, | 11 |
| 2, | 3, | 4, | 7, | 0 |
| 3, | 4, | 5, | 8, | 1 |
| 4, | 5, | 6, | 9, | 2 |
| 5, | 6, | 7, | 10, | 3 |
| 6, | 7, | 8, | 11, | 4 |
| 7, | 8, | 9, | 0, | 5 |
| 8, | 9, | 10, | 1, | 6 |
| 9, | 10, | 11, | 2, | 7 |
| 10, | 11, | 0, | 3, | 8 |
| 11, | 0, | 1, | 4, | 9. |

*In this design, every pair of distinct residues whose difference is* 6 *does not appear together in any block, while all other pairs of distinct residues appear together twice.*

The following Theorem generalizes the results in Elliott and Butson [12], Ryser [35], Koukouvinos and Whiteman [21], and Wei, Gao and Yang [37].

**Theorem 2.31.** *A* $(v, k, [\lambda, 0]; t)$*-design has*

$$\lambda(v - 1 - t) = k(k - 1). \tag{2.2}$$

*Proof.* We count the occurrences of differences of all two distinct objects $a_i$, $a_j$ of a base set of the $(v, k, [\lambda, 0]; t)$-design in two ways:

(1) There are $v - 1 - t$ nonzero residues appearing as differences exactly $\lambda$ times while the other $t$ nonzero residues do not appear:

(2) $k$ objects generate $k(k-1)$ differences. □

**Lemma 2.32.** *If a $(v, k, [\lambda, 0]; t)$-difference set exists and $t$ is odd, then $v$ is even and $\frac{v}{2}$ is a missing difference.*

*Proof.* If a nonzero residue $d$ is missing from the multiset of differences of the $(v, k, [\lambda, 0]; t)$-difference set, then $v - d$ is also missing. Since $t$ is odd, there must exist a missing difference $d$ such that $d = v - d$. So, $v = 2d$ is even and $\frac{v}{2}$ is a missing difference. □

We note that Lemma 2.32 implies that when $t = 1$ a $(v, k, [\lambda, 0]; 1)$--difference set is exactly a near difference set of type 1 of Ryser [35], and thus a $(\frac{v}{2}, 2, k, \lambda)$-RDS. The following Lemma appears in Ryser [35], but in fact it is a special case of a result of Elliot and Butson [12].

**Lemma 2.33.** *Let $A$ be the incidence matrix of a $(v, k, [\lambda, 0]; 1)$-design, then*

$$AA^T = \begin{bmatrix} k & \lambda & \cdots & \lambda & 0 & \lambda & \cdots & \lambda \\ \lambda & k & \cdots & \lambda & \lambda & 0 & \cdots & \lambda \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \lambda & \ddots & \ddots & k & \lambda & \lambda & \ddots & 0 \\ 0 & \ddots & \ddots & \lambda & k & \lambda & \ddots & \lambda \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \vdots \\ \lambda & \cdots & \cdots & \lambda & \lambda & \lambda & \ddots & \lambda \\ \lambda & \cdots & \cdots & 0 & \lambda & \lambda & \cdots & k \end{bmatrix}.$$

*Proof.* Let $B = AA^T = (b_{ij})_{v\times v}$. Then $b_{ij}$ is the inner product of the $i$-th row of $A$ with the $j$-th row of $A$. It follows that $b_{ii}$ counts the number of 1's in the $i$-th row of $A$. So, $b_{ii} = k$. If $i \neq j$, then $b_{ij}$ counts the number of blocks containing both $a_i$ and $a_j$ ($a_i = i - 1$, $a_j = j - 1$). By Lemma 2.32, $\frac{v}{2}$ is the missing difference. Thus, by Theorem 2.8, we have

$$\text{when } i \neq j,\ b_{ij} = \begin{cases} 0 & \text{if } |i-j| = \frac{v}{2} \\ \lambda & \text{otherwise.} \end{cases}$$

and this finishes the proof. □

**Definition 2.34.** *A $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$-difference set $S$ is called a* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m]; t_1, t_2, \dots, t_m)$***-difference set*** *if for each $i$ ($i = 1, 2, \dots, m$) there are exactly $t_i$ nonzero residues appearing exactly $\lambda_i$ times in the multiset of differences of $S$. The $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$-design generated by a $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m]; t_1, t_2, \dots, t_m)$-difference set is called a* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m]; t_1, t_2, \dots, t_m)$***-design.*** *In addition, a* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m]; t)$***-difference set*** *is defined to be a $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m]; t_1, t_2, \dots, t_m)$-difference set with $t_m = t$. A* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m]; t)$***-design*** *can be defined similarly.*

**Example 2.35.** *$\{0, 1, 2, 5, 7\}$ mod 10 is a $(10, 5, [2, 4]; 8, 1)$-difference set. The multiset of its differences is*

$$\begin{array}{llll} \pm1 & \pm2 & \pm5 & \pm7 \\ \pm1 & \pm4 & \pm6 & \\ \pm3 & \pm5 & & \\ \pm2, & & & \end{array}$$

*and note that $\pm7 \equiv \mp3$ (mod 10), $\pm6 \equiv \mp4$ (mod 10) and $-5 \equiv 5$ (mod 10). We have that 5 appears four times as a difference while all other nonzero residues appear twice as differences. This difference set generates a*

$(10, 5, [2, 4]; 8, 1)$-*design:*

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

We now generalize Theorem 2.31 in this thesis. Equation 2.1 of Elliot and Butson [12] and Lemma 2.5 of Jungnickel [18].

**Theorem 2.36.** *A* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m]; t_1, t_2, \ldots, t_m)$*-design has*

$$t_1 + t_2 + \cdots + t_m = v - 1, \tag{2.3}$$

*and*

$$\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_m t_m = k(k-1). \tag{2.4}$$

*Proof.* Counting the total number of nonzero residues, we obtain the first equality. To get the second one, we count the occurrences of differences of all two distinct objects $a_i$, $a_j$ in a base set $S$ of the $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m]; t_1, t_2, \ldots, t_m)$-design in two ways:

(1) For each $i$ $(i = 1, 2, \ldots, m)$ there are exactly $t_i$ nonzero residues appearing exactly $\lambda_i$ times in the multiset of differences of $S$. So the total is $\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_m t_m$;

(2) $k$ objects generate $k(k-1)$ differences. □

**Lemma 2.37.** *Let $A$ be the incidence matrix of a $(v, k, [\lambda_1, \lambda_2]; 1)$-design, then $v$ is even and*

$$AA^T = \begin{bmatrix} k & \lambda_1 & \cdots & \lambda_1 & \lambda_2 & \lambda_1 & \cdots & \lambda_1 \\ \lambda_1 & k & \cdots & \lambda_1 & \lambda_1 & \lambda_2 & \cdots & \lambda_1 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \lambda_1 & \ddots & \ddots & k & \lambda_1 & \lambda_1 & \ddots & \lambda_2 \\ \lambda_2 & \ddots & \ddots & \lambda_1 & k & \lambda_1 & \ddots & \lambda_1 \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \vdots \\ \lambda_1 & \cdots & \cdots & \lambda_1 & \lambda_1 & \lambda_1 & \ddots & \lambda_1 \\ \lambda_1 & \cdots & \cdots & \lambda_2 & \lambda_1 & \lambda_1 & \cdots & k \end{bmatrix}.$$

*Proof.* The proof of this Lemma is similar to the proofs of Lemma 2.32 and Lemma 2.33. □

**Lemma 2.38.** *(p 129, [13]) For $v \times v$ matrices $I$ and $J$, we have*

$$det\left[(r-\lambda)I + \lambda J\right] = (r-\lambda)^{v-1}(v\lambda - \lambda + r). \qquad (2.5)$$

**Lemma 2.39.** *(p 164, [16]) If $M$, $N$, $O$ and $P$ are $n \times n$ matrices which commute in pairs, then*

$$det \begin{bmatrix} M & N \\ O & P \end{bmatrix} = det(MP - NO).$$

**Lemma 2.40.** *If $M$ is an $n \times n$ matrix and all eigenvalues of $M$ are $\lambda_1, \lambda_2, \ldots, \lambda_n$, then all eigenvalues of the matrix $M + aI$ are $\lambda_1 + a, \lambda_2 + a, \ldots, \lambda_n + a$, where $a$ is a real number and $I$ is the $n \times n$ identity matrix.*

*Proof.* In the characteristic polynomial of $M$

$$det(\lambda I - M) = \prod_{i=1}^{n}(\lambda - \lambda_i),$$

replacing $\lambda$ by $\lambda - a$, we get the result. □

**Lemma 2.41.** *(p 237, [30]) Let $M$ be an $m \times m$ matrix and $N$ be an $n \times n$ matrix. If all eigenvalues of $M$ are $\lambda_1, \lambda_2, \ldots, \lambda_m$ and all eigenvalues of $N$ are $\mu_1, \mu_2, \ldots, \mu_n$, then all $mn$ eigenvalues of the Kronecker product $M \times N$ are $\lambda_i\mu_j$, where $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$.*

**Lemma 2.42.** *Let*

$$M = \begin{bmatrix} \lambda_2 & \lambda_1 & \cdots & \lambda_1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_1 \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_1 & \lambda_1 & \cdots & \lambda_2 \end{bmatrix}$$

*be an $n \times n$ matrix. Then all eigenvalues of $M$ are $\lambda_2 - \lambda_1$ ($(n-1)$-multiplicity) and $\lambda_2 + (n-1)\lambda_1$.*

*Proof.* We can get this from Lemma 2.38. □

We extend (10.2.2) on p 129 of M. Hall [13] and (2.7) on p 103 of H. J. Ryser [34] to

**Lemma 2.43.** *Let $A$ be the incidence matrix of a $(v, k, [\lambda_1, \lambda_2]; 1)$-design and $B = AA^T$, then*

$$det(B) = [(v-2)\lambda_1 + \lambda_2 + k]\,(k - \lambda_2)^{\frac{v}{2}}(k - 2\lambda_1 + \lambda_2)^{\frac{v}{2}-1}, \tag{2.6}$$

*where $v \geq 4$.*

*Proof 1.* In $det(B)$, we first add all other rows to the first row and factor $[(v-2)\lambda_1+\lambda_2+k]$ out, then subtract $\lambda_1$ times the first row from each of the other rows. This gives that

$$
\begin{aligned}
& det(B) \\
= & [(v-2)\lambda_1+\lambda_2+k]\cdot \\
& \cdot\begin{vmatrix}
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\
0 & k-\lambda_1 & \cdots & 0 & 0 & \lambda_2-\lambda_1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & \ddots & \ddots & k-\lambda_1 & 0 & 0 & \ddots & \lambda_2-\lambda_1 \\
\lambda_2-\lambda_1 & \ddots & \ddots & 0 & k-\lambda_1 & 0 & \ddots & 0 \\
\vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \vdots \\
0 & \cdots & \cdots & 0 & 0 & 0 & \ddots & 0 \\
0 & \cdots & \cdots & \lambda_2-\lambda_1 & 0 & 0 & \cdots & k-\lambda_1
\end{vmatrix}.
\end{aligned}
$$

Then, add $\frac{\lambda_1-\lambda_2}{k-\lambda_1}$ times the $(\frac{v}{2}+1)$-th column to the first column and add $\frac{\lambda_1-\lambda_2}{k-\lambda_1}$ times the 2nd row, 3rd row, ..., $\frac{v}{2}$-th row to the $(\frac{v}{2}+2)$-th row, $(\frac{v}{2}+3)$-th row, ..., $v$-th row respectively. Let $d=\frac{(k-\lambda_2)(k-2\lambda_1+\lambda_2)}{k-\lambda_1}$, then we have

$$
\begin{aligned}
det(B) &= [(v-2)\lambda_1+\lambda_2+k]\cdot \\
&\cdot\begin{vmatrix}
\frac{k-\lambda_2}{k-\lambda_1} & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\
0 & k-\lambda_1 & \cdots & 0 & 0 & \lambda_2-\lambda_1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & \ddots & \ddots & k-\lambda_1 & 0 & 0 & \ddots & \lambda_2-\lambda_1 \\
0 & \ddots & \ddots & 0 & k-\lambda_1 & 0 & \ddots & 0 \\
\vdots & \ddots & \ddots & \ddots & 0 & d & \ddots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \cdots & \ddots & \vdots \\
0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & d
\end{vmatrix} \\
&= [(v-2)\lambda_1+\lambda_2+k]\,\frac{k-\lambda_2}{k-\lambda_1}(k-\lambda_1)^{\frac{v}{2}}\left[\frac{(k-\lambda_2)(k-2\lambda_1+\lambda_2)}{k-\lambda_1}\right]^{\frac{v}{2}-1} \\
&= [(v-2)\lambda_1+\lambda_2+k]\,(k-\lambda_2)^{\frac{v}{2}}(k-2\lambda_1+\lambda_2)^{\frac{v}{2}-1}.
\end{aligned}
$$

□

*Proof 2.* Let $M$, $N$, $O$ and $P$ be $\frac{v}{2}\times\frac{v}{2}$ matrices and let

$$
M=P=\begin{bmatrix}
k & \lambda_1 & \cdots & \lambda_1 \\
\lambda_1 & k & \cdots & \lambda_1 \\
\vdots & \ddots & \ddots & \vdots \\
\lambda_1 & \lambda_1 & \cdots & k
\end{bmatrix}
$$

and

$$
N=O=\begin{bmatrix}
\lambda_2 & \lambda_1 & \cdots & \lambda_1 \\
\lambda_1 & \lambda_2 & \cdots & \lambda_1 \\
\vdots & \ddots & \ddots & \vdots \\
\lambda_1 & \lambda_1 & \cdots & \lambda_2
\end{bmatrix}.
$$

Using Lemmas 2.38 and 2.39, we can evaluate $det(B)$ in a different way and get the same result. □

*Proof 3.* Let $n = \frac{v}{2}$. Then

$$B-(k-\lambda_2)I = \begin{bmatrix} \lambda_2 & \lambda_1 & \cdots & \lambda_1 & \lambda_2 & \lambda_1 & \cdots & \lambda_1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_1 & \lambda_1 & \lambda_2 & \cdots & \lambda_1 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \lambda_1 & \ddots & \ddots & \lambda_2 & \lambda_1 & \lambda_1 & \ddots & \lambda_2 \\ \lambda_2 & \ddots & \ddots & \lambda_1 & \lambda_2 & \lambda_1 & \ddots & \lambda_1 \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \vdots \\ \lambda_1 & \cdots & \cdots & \lambda_1 & \lambda_1 & \lambda_1 & \ddots & \lambda_1 \\ \lambda_1 & \cdots & \cdots & \lambda_2 & \lambda_1 & \lambda_1 & \cdots & \lambda_2 \end{bmatrix} = M \times J_{2\times 2},$$

where

$$M = \begin{bmatrix} \lambda_2 & \lambda_1 & \cdots & \lambda_1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_1 \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_1 & \lambda_1 & \cdots & \lambda_2 \end{bmatrix}$$

is an $n \times n$ matrix. By Lemmas 2.41 and 2.42, since $J_{2\times 2}$ has two eigenvalues 2 and 0, we have that $B-(k-\lambda_2)I$ has eigenvalues $2(\lambda_2-\lambda_1)$ ($(n-1)$-multiplicity), $2[\lambda_2+(n-1)\lambda_1]$, and 0 ($n$-multiplicity). Thus, by Lemma 2.40, the matrix $B = M \times J_{2\times 2}+(k-\lambda_2)I$ has eigenvalues $2(\lambda_2-\lambda_1)+$ $+(k-\lambda_2) = k-2\lambda_1+\lambda_2$ ($(n-1)$-multiplicity), $2[\lambda_2+(n-1)\lambda_1]+(k-\lambda_2) =$ $=(2n-2)\lambda_1+\lambda_2+k$, and $0+(k-\lambda_2) = k-\lambda_2$ ($n$-multiplicity). Since the determinant of a square matrix equals the product of all its eigenvalues, we get $det(B)$. □

The following Theorem is more general than the first part of Theorem 2.1 in Ryser [35], Parts (i) and (ii) of Theorem 3.1 in Wei, Gao and Yang [37] and a special case of Theorem 2.3 in Elliot and Butson [12]. We will show, in Theorem 5.4, that a similar result holds in the general case.

**Theorem 2.44.** *Assume that there exists a $(v, k, [\lambda_1, \lambda_2]; 1)$-design, then:*

*(1) if $v \equiv 0 \pmod 4$, then $k - 2\lambda_1 + \lambda_2$ is a square;*

*(2) if $v \equiv 2 \pmod 4$, then $k - \lambda_2$ is a square.*

*Proof.* Let $B = AA^T$, so $det(B) = det(A)det(A^T) = det(A)^2$. Thus $det(B) = [(v-2)\lambda_1 + \lambda_2 + k](k-\lambda_2)^{\frac{v}{2}}(k-2\lambda_1+\lambda_2)^{\frac{v}{2}-1}$ should be a square. By (2.3), $(v, k, [\lambda_1, \lambda_2]; 1)$-design is a $(v, k, [\lambda_1, \lambda_2]; v-2, 1)$-design. Hence by (2.4), we have that $(v-2)\lambda_1 + \lambda_2 + k = k(k-1) + k = k^2$. If $v \equiv 0 \pmod 4$, then $\frac{v}{2}$ is even. Thus $(k-\lambda_2)^{\frac{v}{2}}$ is a square. So, $(k-2\lambda_1+\lambda_2)^{\frac{v}{2}-1}$ should be a square. Since $\frac{v}{2} - 1$ is odd, we have $k - 2\lambda_1 + \lambda_2$ is a square. If $v \equiv 2 \pmod 4$, then $\frac{v}{2} - 1$ is even. So, $(k - 2\lambda_1 + \lambda_2)^{\frac{v}{2}-1}$ is a square. This implies that $(k - \lambda_2)^{\frac{v}{2}}$ is a square. Since $\frac{v}{2}$ is odd, $k - \lambda_2$ must be a square. $\square$

# Chapter 3

# Singly Equivalent Designs

In this Chapter, we will introduce the concept of $\lambda$-equivalent designs. We will prove that a 0-equivalent $(n^2 - 1, n, [1, 0])$-design can be embedded into an affine plane. We will also prove that for a 0-equivalent $(v, k, [\lambda, 0]: t)$--design if $t \geq 2$ then the point 0 must miss at least one parallel class. Define $u$ to be the number of parallel classes missing the point 0. Then we can obtain a standard difference set from a 0-equivalent $(v, k, [\lambda, 0]: t)$-design with $u > 1$ (Theorem 3.32). We will also prove that we can add some points to a base set of a 0-equivalent $(v, k, [\lambda, 0]: t)$-design with $u = 1$ and get a set which generates a $(t+1)$-equivalent $(v, k+t+1, [\lambda+2, t+1]: t)$-design or a $(v, k+t+1, \lambda+2)$-design.

## 3.1 Basic Concepts

**Definition 3.1.** *In a* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$*-difference set* $S = \{a_1, a_2, a_3, \ldots, a_k\}$, *the set* $B_i = \{a_1 + i, a_2 + i, a_3 + i, \ldots, a_k + i\}$ *mod*

*$v$ is also denoted by $\boldsymbol{l_i}$ or $[\boldsymbol{i}]$ and is called a **line** in the design generated by $S$ while an object $i$ in the design is also called a **point**, where $i = 0, \ldots, v-1$. If two lines $l_i$ and $l_j$ are the same or intersect in $\lambda_r$ $(1 \leq r \leq m)$ points, then $l_i$ and $l_j$ are called **$\lambda_r$-intersecting**. If $l_i$ and $l_j$ are 0-intersecting, then $l_i$ and $l_j$ are called **parallel** and we denote this by $\boldsymbol{l_i} \parallel \boldsymbol{l_j}$.*

Obviously, in a $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-design, the relation $\lambda_r$-intersection is reflexive and symmetric. However, it is not necessarily transitive:

**Example 3.2.** *$\{0, 1, 3, 10\}$ mod 15 is a $(15, 4, [1, 0]: 2)$-difference set: the multiset of its differences is*

$$\begin{array}{lll} \pm 1 & \pm 3 & \pm 10 \\ \pm 2 & \pm 9 & \\ \pm 7. & & \end{array}$$

*Note that both 4 and 11 are missing from the multiset of differences while each of the other nonzero residues appears as a difference exactly once.*

*The design generated by this difference set is:*

$$\begin{array}{lllll} [0] & 0, & 1, & 3, & 10 \\ & 1, & 2, & 4, & 11 \\ & 2, & 3, & 5, & 12 \\ & 3, & 4, & 6, & 13 \\ [4] & 4, & 5, & 7, & 14 \\ & 5, & 6, & 8, & 0 \\ & 6, & 7, & 9, & 1 \\ & 7, & 8, & 10, & 2 \end{array}$$

$$
\begin{array}{lllll}
 & 8, & 9, & 11, & 3 \\
 & 9, & 10, & 12, & 4 \\
 & 10, & 11, & 13, & 5 \\
[11] & 11, & 12, & 14, & 6 \\
 & 12, & 13, & 0, & 7 \\
 & 13, & 14, & 1, & 8 \\
 & 14, & 0, & 2, & 9.
\end{array}
$$

*Clearly,* $[4] \parallel [0]$ *and* $[11] \parallel [0]$, *but* $[4] \nparallel [11]$ *since they meet at the point* 14.

The Example 3.2 leads us to introduce

**Definition 3.3.** *A* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$*-design* $D$ *is called* $\boldsymbol{\lambda_r}$***-equivalent*** *if the relation* $\lambda_r$*-intersection is an equivalence relation. In this case, if two lines* $l_i$ *and* $l_j$ *in* $D$ *are* $\lambda_r$*-intersecting, we denote this by* $\boldsymbol{l_i \overset{\lambda_r}{\approx} l_j}$*. If* $\lambda_r = 0$, *we also call a* 0*-equivalent design* ***parallel equivalent.***

*A* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$*-difference set* $S$ *is called* $\boldsymbol{\lambda_r}$***-equivalent*** *if the design generated by* $S$ *is* $\lambda_r$*-equivalent.*

*A* $\lambda_r$*-equivalent difference set or design is also called a* ***singly equivalent difference set*** *or* ***design*** *respectively.*

So, to show a design is $\lambda_r$-equivalent, we just need to prove that for the design the relation $\lambda_r$-intersection is transitive.

In an unpublished paper, Professor N. S. Mendelsohn has obtained the following two theorems.

**Theorem 3.4.** *A* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$*-design* $D$ *generated by a* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$*-difference set* $S$ *is* $\lambda_r$*-equivalent* $(1 \leq r \leq m)$ *if and* *only if whenever $d$ and $e$ appear $\lambda_r$ times as differences of $S$, then $d+e$ (or $d-e$) also appears there $\lambda_r$ times as a difference.*

*Proof.* Let $[i_1]$, $[i_2]$ and $[i_3]$ be three lines in $D$. Then the conclusion can be obtained from the following facts based on Theorem 2.8:

(1) $|\,[i_1]\cap[i_2]\,| = \lambda_r \Leftrightarrow i_2 - i_1$ appears as a difference $\lambda_r$ times:

(2) $|\,[i_2]\cap[i_3]\,| = \lambda_r \Leftrightarrow i_3 - i_2$ appears as a difference $\lambda_r$ times:

(3) $|\,[i_1]\cap[i_3]\,| = \lambda_r \Leftrightarrow i_3 - i_1$ appears as a difference $\lambda_r$ times:

(4) $e$ and $v-e$ appear the same number of times as differences and notice that $d \mp e \equiv d \pm (v-e) \pmod v$. □

**Theorem 3.5.** *A $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$-design $D$ generated by a $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$-difference set $S$ is $\lambda_r$-equivalent ($1 \le r \le m$) if and only if $t+1 \mid v$ and all the residues appearing $\lambda_r$ times as differences of $S$ are:*

$$\alpha, 2\alpha, 3\alpha, \dots, t\alpha,$$

*where $t$ is the number of residues appearing $\lambda_r$ times as differences of $S$ and $\alpha = \frac{v}{t+1}$.*

*Proof.* $\Rightarrow$. Assume that $\alpha$ is the smallest positive residue which appears $\lambda_r$ times as a difference of $S$, then, by Theorem 3.4, all the nonzero residues which appear $\lambda_r$ times as differences of $S$ are $\alpha$, $2\alpha$, $3\alpha$, $\dots$ . Therefore lines $[\alpha]$, $[2\alpha]$, $[3\alpha]$, $\dots$ , $[t\alpha]$ and $[(t+1)\alpha]$=[0] are $\lambda_r$-intersecting to each other and no other lines can be $\lambda_r$-intersecting to them, since otherwise $\alpha$ cannot be the smallest positive residue appearing as a difference $\lambda_r$ times. This gives that $(t+1)\alpha = v$ and the conclusion follows.

$\Leftarrow$. This is a immediate result of Theorem 3.4. □

In this Chapter, we always denote $\frac{v}{t+1}$ by $\boldsymbol{\alpha}$.

**Corollary 3.6.** *A $\lambda_2$-equivalent $(v, k, [\lambda_1, \lambda_2]; t)$-difference set is a $(\alpha, t+1, k, \lambda_2, \lambda_1)$-DDS.*

*Proof.* Let $S$ be a $\lambda_2$-equivalent $(v, k, [\lambda_1, \lambda_2]; t)$-difference set and $N = \{0, \alpha, 2\alpha, 3\alpha, \ldots, t\alpha\}$. Then $N$ is a subgroup of $G = \mathbf{Z}_v$, where $\mathbf{Z}_v$ is the additive group of integers mod $v$. Since $\mathbf{Z}_v$ is Abelian, we have that $N$ is a normal subgroup. By Theorem 3.5, all elements of $N\backslash\{0\}$ appear $\lambda_2$ times as differences of $S$ while all elements in $G\backslash N$ appear $\lambda_1$ times as differences of $S$. So, by Definition 1.7, $S$ is a $(\alpha, t+1, k, \lambda_2, \lambda_1)$-DDS. $\square$

When $\lambda_2 = 0$, we have

**Corollary 3.7.** *A 0-equivalent $(v, k, [\lambda, 0]: t)$-difference set is a $(\alpha, t+1, k, \lambda)$- -RDS.*

**Example 3.8.** *$\{0, 1, 3, 7\}$ mod 15 is a $(15, 4, [1, 0]: 2)$-difference set: the multiset of its differences is*

$$\begin{array}{lll} \pm 1 & \pm 3 & \pm 7 \\ \pm 2 & \pm 6 & \\ \pm 4. & & \end{array}$$

*Note that both 5 and 10 are missing from the multiset of differences while each of the other nonzero residues appears as a difference exactly once.*

*By Theorem 3.5, the design generated by this difference set is* 0*-equivalent:*

$$\begin{array}{lllll}
[0] & 0, & 1, & 3, & 7 \\
 & 1, & 2, & 4, & 8 \\
 & 2, & 3, & 5, & 9 \\
 & 3, & 4, & 6, & 10 \\
 & 4, & 5, & 7, & 11 \\
[5] & 5, & 6, & 8, & 12 \\
 & 6, & 7, & 9, & 13 \\
 & 7, & 8, & 10, & 14 \\
 & 8, & 9, & 11, & 0 \\
 & 9, & 10, & 12, & 1 \\
[10] & 10, & 11, & 13, & 2 \\
 & 11, & 12, & 14, & 3 \\
 & 12, & 13, & 0, & 4 \\
 & 13, & 14, & 1, & 5 \\
 & 14, & 0, & 2, & 6.
\end{array}$$

**Example 3.9.** $\{0, 1, 2, 4, 7\}$ *mod* 12 *is a* $(12, 5, [2, 1]; 2)$*-difference set. The multiset of its differences is*

$$\begin{array}{llll}
\pm1 & \pm2 & \pm4 & \pm7 \\
\pm1 & \pm3 & \pm6 & \\
\pm2 & \pm5 & & \\
\pm3. & & &
\end{array}$$

*Note that* $\pm7 \equiv \mp5 \pmod{12}$, $-6 \equiv 6 \pmod{12}$ *and* $-4 \equiv 8 \pmod{12}$. *We have that both* 4 *and* 8 *appear as differences once while all other nonzero* *residues appear twice. By Theorem 3.5, the design generated by this difference set is* 1*-equivalent.*

**Corollary 3.10.** *If a* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m]; t)$*-design* $D$ *is* $\lambda_m$*-equivalent, then* $[i] \overset{\lambda_m}{\sim} [j]$ *if and only if* $i - j = a\alpha$*, where* $a \in \mathbf{Z}$ *and* $\mathbf{Z}$ *is the set of all integers.*

*Proof.* This is a direct result of Theorems 2.8 and 3.5. ☐

**Corollary 3.11.** *A* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m]; 1)$*-design* $D$ *is* $\lambda_m$*-equivalent.*

*Proof.* In a similar manner to the proof of Lemma 2.32, we can see that $v$ must be even and the residue appearing as a difference $\lambda_m$ times is $\frac{v}{2}$. By Theorem 3.5, the conclusion follows. ☐

**Corollary 3.12.** *A* 0*-equivalent* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_{m-1}, 0]; t)$*-design* $D$ *cannot have* 1 *as a missing difference of the base set* $S$ *of* $D$.

*Proof.* If $S$ has 1 as a missing difference, by Theorem 3.4 or Theorem 3.5, $D$ also has $2, 3, \dots, v-1$ as missing differences, which is a contradiction. ☐

By Corollary 3.12, when we want to search for 0-equivalent $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_{m-1}, 0]; t)$-difference sets on a computer, we just search those $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_{m-1}, 0]; t)$-difference sets of form $\{0, 1, a_3, \dots, a_k\}$.

**Corollary 3.13.** *No* $(v, k, [\lambda_1, \lambda_2, \dots, \lambda_m])$*-design* $D$ *is* $\lambda_1$*-,* $\lambda_2$*-,* $\dots$ *and* $\lambda_m$*-equivalent at the same time for* $m > 1$.

*Proof.* Suppose 1 appears $\lambda_i$ times $(1 \le i \le m)$ as a difference of a base set of $D$. Then each of $2, 3, \dots$ also appears $\lambda_i$ times as differences, which is impossible. ☐

**Theorem 3.14.** *If a $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-design $D$ generated by a $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-difference set $S$ is $\lambda_r$-equivalent $(1 \leq r \leq m)$, then the $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-design $E$ generated by $a \cdot S \pmod{v}$ is also $\lambda_r$-equivalent, where $a$ is any integer such that $(a, v) = 1$.*

*Proof 1.* Let $A = \{u, \ldots, tu\} \pmod{v}$ be the set of residues which appear $\lambda_r$ times as differences in the set $S$. Then $B = \{au, \ldots, tau\} \pmod{v}$ is the set of residues which appear $\lambda_r$ times as differences in the set $a \cdot S \pmod{v}$. Obviously, $A \supseteq B$. If $dau \equiv eau \pmod{v}$, where $d$ and $e$ are integers, then $du \equiv eu \pmod{v}$. Thus, $A = B$. Therefore, by Theorem 3.4 or Theorem 3.5, $E$ is also $\lambda_r$-equivalent. □

*Proof 2.* Since $D$ is $\lambda_r$-equivalent and $S \simeq a \cdot S$, so $E$ is also $\lambda_r$-equivalent. □

**Theorem 3.15.** *If there exists a $\lambda_2$-equivalent $(v, k, [\lambda_1, \lambda_2]; s, t)$-design and $\lambda_2$ is odd, then $t$ is even.*

*Proof.* By Theorem 2.36, we have

$$v - 1 = s + t, \tag{3.1}$$

and

$$k(k-1) = s\lambda_1 + t\lambda_2. \tag{3.2}$$

If $t$ is odd, then $v$ is even since $(t+1) \mid v$. Hence, by

$$v = s + (t+1),$$

we have that $s$ is even. Thus, by (3.2), since $k(k-1)$ is also even, but if $\lambda_2$ is odd then $t$ is even, which is a contradiction. Therefore, $t$ has to be even. □

## 3.2 Finite Planes

The following three definitions are taken from L. M. Batten and A. Beutelspacher [3].

**Definition 3.16.** *A **linear space** is a pair $S = (p, L)$ consisting of a set $p$ of elements, which are called points, and a set $L$ of distinguished subsets of points, which are called lines, such that the following axioms hold:*

*(L1) Any two distinct points of $S$ belong to exactly one line of $S$;*

*(L2) Any line of $S$ has at least two points of $S$;*

*(L3) There exist three points of $S$ not on a common line.*

**Definition 3.17.** *An **affine plane** is a linear space satisfying:*

*(A) If a point $p$ is not on a line $L$, then there is a unique line on $p$ missing $L$.*

**Definition 3.18.** *A **projective plane** is a linear space satisfying:*

*(P1) Any two distinct lines meet;*

*(P2) There exist four points, no three of which are on a common line.*

**Theorem 3.19.** *All lines in an affine plane have the same number of points. All lines in a projective plane also have the same number of points.*

*Proof.* See Propositions 1.2.2 and 1.2.6 of L. M. Batten and A. Beutelspacher [3]. □

**Definition 3.20.** *An affine plane is said to be of **order n** if a line contains exactly $n$ points.*

*A projective plane is said to be of **order n** if a line contains exactly $(n+1)$ points.*

**Theorem 3.21.** *Let $n \geq 2$. Then $A$ is an affine plane of order $n$ if and only if $A$ is a $(n^2, n^2+n, n+1, n, 1)$-design.*

*Proof.* By Propositions 1.2.2 to 1.2.4 of L. M. Batten and A. Beutelspacher [3] and Definition 3.16, it is true. □

**Theorem 3.22.** *Let $n \geq 2$. Then $P$ is a projective plane of order $n$ if and only if $P$ is a $(n^2+n+1, n+1, 1)$-design.*

*Proof.* $\Rightarrow$. It follows from Propositions 1.2.6 to 1.2.8 of L. M. Batten and A. Beutelspacher [3] and Definition 3.16.

$\Leftarrow$. Let $A = \{a_1, a_2, a_3, \ldots, a_k\}$ and $B = \{b_1, b_2, b_3, \ldots, b_k\}$ be two distinct lines in a $(n^2+n+1, n+1, 1)$-design, where $k = n+1$. If $A \parallel B$, then pairs $a_i$ and $b_j$ $(i, j = 1, 2, \ldots, k)$ are in different blocks. Thus the number of blocks

$$v \geq k^2 + 2 = (n+1)^2 + 2 = n^2 + 2n + 3,$$

which leads to a contradiction. Therefore, $A \cap B \neq \varnothing$ and the axiom (P1) holds.

Next let $A = \{a_1, a_2, a_3, \ldots, a_k\}$ and $B = \{b_1, b_2, b_3, \ldots, b_k\}$ be two distinct lines and $a_k = b_k$. Then any three of the four points $a_1, a_2, b_1$ and $b_2$ are not on a common line. Hence the axiom (P2) holds.

The rest is straightforward. □

The second part of the following Theorem is due to Bose [6]. Jungnickel [18] Theorem 4.1 gives a more general result for affine geometries.

**Theorem 3.23.** *(1) From a $(n^2+n+1, n+1, 1)$-design, after removing one line and all points on this line, a $(n^2, n^2+n, n+1, n, 1)$-design is obtained.*

*(2) From a* $(n^2, n^2+n, n+1, n, 1)$*-design, after removing one point and all lines through that point, a* 0*-equivalent* $(n^2-1, n, [1,0])$*-design is obtained.*

*Proof.* (1) See Theorem 4.3.2 of L. M. Batten [4].

(2) Let $D$ be a $(n^2, n^2+n, n+1, n, 1)$-design. After removing one point $P$ and all lines on $P$, we have $n^2-1$ lines and $n^2-1$ points left. Since in the design $D$ for every point $Q$ different from $P$, there is exactly one line through points $P$ and $Q$. Thus after removing all lines on $P$, each point has $n$ lines on it. The size of a line remains unchanged. Each pair of distinct points have exactly one line or no line through them. So, we get a $(n^2-1, n, [1,0])$- -design. For a proof that the $(n^2-1, n, [1,0])$ design is generated by a 0-equivalent $(n^2-1, n, [1,0])$-difference set see Theorem 4.1 of Jungnickel [18]. □

There is a natural way of embedding a 0-equivalent $(n^2-1, n, [1,0])$ design in an affine plane of order $n$ due to Bose [6]. This is Part (1) of the following Theorem.

**Theorem 3.24.** *(1) A* 0*-equivalent* $(n^2-1, n, [1,0])$*-design can be embedded into an affine plane of order* $n$*.*

*(2) An affine plane can be embedded into a projective plane of the same order.*

*Proof.* (1) Let $D$ be a $(n^2-1, n, [1,0]; t)$-design. By $\lambda(v-1-t) = k(k-1)$, we get $(n^2-1)-1-t = n(n-1)$. So, $t = n-2$. Thus

$$\alpha = \frac{v}{t+1} = \frac{n^2-1}{n-1} = n+1.$$

We put the $v = (t+1)\alpha$ points $0, 1, \dots, v-1$ into an array of $\alpha$ rows:

$$\begin{array}{ccccc}
0, & \alpha, & 2\alpha, & \dots, & t\alpha \\
1, & 1+\alpha, & 1+2\alpha, & \dots, & 1+t\alpha \\
2, & 2+\alpha, & 2+2\alpha, & \dots, & 2+t\alpha \\
\dots & \dots & \dots & \dots & \dots \\
\alpha-1, & \alpha-1+\alpha, & \alpha-1+2\alpha, & \dots, & \alpha-1+t\alpha.
\end{array}$$

Any two points in a same row are not on a line and any two points not on a line must be in the same row of the array. We add a new point $\infty$ and $\alpha$ new lines to the design: each new line contains all points in one row of the array and the new point $\infty$. For the new design $D^*$, the number of lines is $b^* = (n^2-1)+\alpha = n^2+n$: the number of points is $v^* = (n^2-1)+1 = n^2$: the number of lines on a point $r^* = n+1$ since each point in $D$ is on exactly one new line and the new point is on $\alpha = n+1$ lines: the number of points on a line remains the same: $k^* = n$: finally, each pair of distinct points in $D^*$ is on exactly one line. Therefore, $D^*$ is a $(n^2, n^2+n, n+1, n, 1)$-design and, by Theorem 3.21, it is an affine plane of order $n$.

(2) See the proof of Theorem 12.3.3 of M. Hall [13]. ☐

The embedding result in Part (1) of Theorem 3.24 prompted Bose [6] to introduce the following Definition.

**Definition 3.25.** *A 0-equivalent $(n^2-1, n, [1,0])$-difference set, i.e. a $(n+1, n-1, n, 1)$-RDS, is called an* ***affine difference set of order $n$.***

Affine difference sets have also been studied by Hoffman [15].

## 3.3 Parallel Classes

**Definition 3.26.** *In a 0-equivalent $(v, k, [\dots, 0]; t)$-design, the set of all lines which are parallel to the line $[i]$ is called the* ***parallel class*** $\langle i \rangle$. *0-**equivalence class** $\langle i \rangle$ or **line class** $\langle i \rangle$ $(i = 0, 1, \dots, \frac{v}{t+1} - 1)$. We say that a line class $\langle i \rangle$ **misses** a point $x$ if no line in $\langle i \rangle$ contains the point $x$.*

By Theorem 3.5, in a 0-equivalent $(v, k, [\dots, 0]; t)$-design, the class $\langle i \rangle$ consists of $[i], [i+\alpha], [i+2\alpha], \dots, [i+t\alpha]$ for each $i$ with $0 \leq i < \alpha$, where $\alpha = \frac{v}{t+1}$. So, in a 0-equivalent $(v, k, [\dots . 0]; t)$-design, the lines are divided into $\alpha$ parallel classes and each parallel class contains $t+1$ lines.

**Theorem 3.27.** *In a 0-equivalent $(v, k, [\dots, 0]; t)$-design, the point 0 is missing from the line class $\langle l \rangle$ if and only if the point $a$ is missing from the line class $\langle l + a \rangle$ (mod $\frac{v}{t+1}$), where $(0 \leq a < v)$.*

*Proof.* Let $0 < a < v$. The point 0 appears in the line $[l]$ if and only if the point $a$ appears in the line $[l+a]$ (mod $v$). So, 0 is missing from the line $[l]$ if and only if $a$ is missing from the line $[l+a]$ (mod $v$). Therefore, 0 is missing from the line class $\langle l \rangle$ if and only if $a$ is missing from the line class $\langle l+a \rangle$ (mod $\frac{v}{t+1}$). □

In a 0-equivalent $(v, k, [\dots, 0]; t)$-design, let $\boldsymbol{u}$ be the number of line classes from which the point 0 is missing, where $u$ is a nonnegative integer. We have:

**Lemma 3.28.** *For a 0-equivalent $(v, k, [\dots, 0]; t)$-design, $v = (k+u)(t+1)$.*

*Proof.* By the definition of a $(v, k, [\dots, 0]; t)$-design there are $k$ lines containing 0. Since those $k$ lines must be in $k$ different parallel classes, there are $k$ parallel classes containing 0. In addition, there are $\frac{v}{t+1}$ line classes in total. So, we have

$$\frac{v}{t+1} = k + u.$$

Hence,

$$v = (k + u)(t + 1).$$

$\square$

By Lemma 3.28 $u = \alpha - k$. also in a $(m, n, k, \lambda_1, \lambda_2)$-DDS, $m = k + u$ and as already mentioned $n = t + 1$. Theorem 3.30 and 3.32 are due to Elliot and Butson [12], Theorem 6.2: see also Proposition 3.1 and Example 2.4 (ii) of Jungnickel [18].

**Theorem 3.29.** *If $t \geq 2$, there are no 0-equivalent $(v, k, [\lambda, 0]: t)$-designs such that $u = 0$.*

*Proof.* We prove this by contradiction. Assume that for $t \geq 2$ there is a $(v, k, [\lambda, 0]; t)$-design $D$ such that $u = 0$. Then, by previous Lemma, $v = (k + u)(t + 1) = k(t + 1)$. Since $\lambda(v - 1 - t) = k(k - 1)$, we have $\lambda(k - 1)(t + 1) = k(k - 1)$. Thus $\lambda(t + 1) = k$. So, $\lambda = \frac{k}{t+1}$. Meanwhile, $\alpha = \frac{v}{t+1} = k$.

Let $S = \{0, a_2, a_3, \dots, a_k\}$ be a base set of $D$. Pick $i$ $(2 \leq i \leq k)$ and let $l = v - a_i$. Then $[l]$ is a line which contains the point 0 and is different from $[0]$. Let $[l] = \{b_1, b_2, b_3, \dots, b_k\}$. Since $[l]$ meets $[0]$, it also meets every other line in the parallel class $\langle 0 \rangle$. Furthermore, by Theorem 2.8 $[l]$ meets every line in the parallel class $\langle 0 \rangle$ $\lambda$ times, but $k = \lambda(t+1)$ and there are $t+1$ disjoint lines in $\langle 0 \rangle$, so every point on $[l]$ is on some line in the parallel class $\langle 0 \rangle$. Since $\langle 0 \rangle =$ $= \{[0], [\alpha], [2\alpha], \ldots, [t\alpha]\}$, we have $[l] = \{0 + t_1\alpha, a_2 + t_2\alpha, \ldots, a_k + t_k\alpha\}$ (mod $v$), where $t_1, t_2, \ldots, t_k$ is a permutation of $\lambda$ copies of the set $\{0, 1, \ldots, t\}$. Accordingly,

$$\begin{aligned}\sum_{i=1}^{k} b_i &\equiv \sum_{i=2}^{k} a_i + \lambda\alpha \sum_{i=1}^{t} i \pmod v \\ &= \sum_{i=2}^{k} a_i + \lambda k \frac{(t+1)t}{2}.\end{aligned}$$

However, since $b_i \equiv a_i + l \pmod v$ $(i = 0, 1, \ldots, k)$, where $a_1 = 0$, we have

$$\sum_{i=1}^{k} b_i \equiv \left(\sum_{i=2}^{k} a_i\right) + kl \pmod v.$$

Hence,

$$\lambda k \frac{(t+1)t}{2} \equiv kl \pmod v.$$

Since $v = k(t+1)$, we have

$$\lambda \frac{(t+1)t}{2} \equiv l \pmod{t+1}.$$

So, $t + 1 \mid 2l$. Meanwhile $2l = 2v - 2a_i$. It follows that $t + 1 \mid 2a_i$, for $i = 2, 3, \ldots, k$. Therefore, $t + 1$ divides 2 times every difference of $S$. Since, by Corollary 3.12, 1 is one of the differences, we have $t + 1 \mid 2$, which contradicts $t \geq 2$. □

There is an example with $t = 1$ and $u = 0$:

**Example 3.30.** *$\{0, 1\}$ mod 4 is a $(4, 2, [1, 0]; 1)$-difference set: the set of its differences is*

$$\pm 1.$$

*Note that $-1 \equiv 3 \pmod 4$. We have that 2 is missing from the set of differences.*

*This difference set generates a 0-equivalent design with $u = 0$:*

$$\begin{array}{l} 0,\ 1 \\ 1,\ 2 \\ 2,\ 3 \\ 3,\ 0. \end{array}$$

The following Theorem is more general than Theorem 5.1 in Wei, Gao and Yang [37] and our proof is simpler.

**Theorem 3.31.** *Up to isomorphism, $\{0, 1\}$ mod 4 is the only 0-equivalent $(v, k, [\lambda, 0]; t)$-design with $u = 0$.*

*Proof.* Let $D$ be a 0-equivalent $(v, k, [\lambda, 0]; t)$-design with $u = 0$. By Theorem 3.29, $t = 1$. So, $v = (k + u)(t + 1) = 2k$ and $\alpha = \frac{v}{t+1} = k$. Since $\lambda(v - 1 - t) = k(k - 1)$, we have $2\lambda(k - 1) = k(k - 1)$. Thus $k = 2\lambda$. So $v = 4\lambda$. Hence the type of $D$ is $(4\lambda, 2\lambda, [\lambda, 0]; 1)$.

Let $S = \{0, a_2, a_3, \ldots, a_k\}$ be a base set of $D$ and $l = v - a_i$, where $2 \leq i \leq k$. Similarly to the proof of Theorem 3.29, we have

$$\lambda\frac{(t+1)t}{2} \equiv l \pmod{t+1}.$$

Or

$$\begin{aligned}\lambda &\equiv l \\ &= v - a_i \\ &= 4\lambda - a_i \\ &\equiv a_i \pmod 2.\end{aligned}$$

Hence, $\lambda$ and $a_i$ have the same parity.

If $\lambda$ is even, then all $a_i$'s are even. So, 1, 3, 5, ... are missing from the multiset of differences of $S$. However, by Corollary 3.12, 1 cannot be a missing difference, which leads to a contradiction. Thus $\lambda$ must be odd. Hence $a_2, a_3, \ldots, a_k$ must be also odd. Since 1 must appear as a difference, by Theorem 2.8, [0] and [1] have $\lambda$ objects in common. In addition, [0] and [1] just have one even and one odd object respectively, we have $\lambda \leq 2$. Since $\lambda$ is odd, $\lambda = 1$. Thus $D$ is a $(4, 2, [1, 0]; 1)$-design. The only possible base sets are $\{0,1\}$ and $\{0,3\}$ and by Theorem 2.16 they are isomorphic to each other since $3 \cdot \{0, 1\} = \{0, 3\}$. This finishes the proof. □

**Theorem 3.32.** *For a* 0*-equivalent* $(v, k, [\lambda, 0]; t)$*-design with* $u > 1$, *assume the point* 0 *is missing from the line classes* $\langle i_1 \rangle$, $\langle i_2 \rangle$, ..., $\langle i_u \rangle$, *where* $0 \leq i_1 < i_2 < \ldots < i_u < \alpha$, *then* $\{i_1, i_2, \ldots, i_u\}$ *is an* $(\alpha, u, \mu)$*-difference set, where* $u = \alpha - k$, $\mu = \frac{(\alpha-k)(\alpha-k-1)}{\alpha-1}$. *In addition,* $u = k - \lambda(t+1) + \mu$.

*Proof.* Let $D$ be a 0-equivalent $(v, k, [\lambda, 0]; t)$-design with $u > 1$, with the point 0 is missing from the line classes $\langle i_1 \rangle$, $\langle i_2 \rangle$, ..., $\langle i_u \rangle$, where $0 \leq i_1 < i_2 < \ldots < i_u < \alpha$. By Theorem 3.27, we have (in the following discussion, for each line class $\langle a \rangle$, the value $a$ should be taken mod $\alpha$):

$$\begin{array}{lllll}
\langle i_1 \rangle, & \langle i_2 \rangle, & \ldots, & \langle i_u \rangle & \text{miss} \\
0, & \alpha, & 2\alpha, & \ldots, & t\alpha; \\
& & & & \\
\langle i_1 + 1 \rangle, & \langle i_2 + 1 \rangle, & \ldots, & \langle i_u + 1 \rangle & \text{miss} \\
1, & 1 + \alpha, & 1 + 2\alpha, & \ldots, & 1 + t\alpha; \\
& & & & \\
\langle i_1 + 2 \rangle, & \langle i_2 + 2 \rangle, & \ldots, & \langle i_u + 2 \rangle & \text{miss} \\
2, & 2 + \alpha, & 2 + 2\alpha, & \ldots, & 2 + t\alpha; \\
& & & & \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
& & & & \\
\langle i_1 + \alpha - 1 \rangle, & \langle i_2 + \alpha - 1 \rangle, & \ldots, & \langle i_u + \alpha - 1 \rangle & \text{miss} \\
\alpha - 1, & \alpha - 1 + \alpha, & \alpha - 1 + 2\alpha, & \ldots, & \alpha - 1 + t\alpha.
\end{array}$$

By Theorem 3.27, a line class $\langle l \rangle$ misses a point $x$ if and only if $\langle l - x \rangle$ misses 0, thus $\langle l - x \rangle = \langle i_p \rangle$ for some $p$ $(1 \leq p \leq u)$. So, two line classes $\langle l \rangle$ and $\langle m \rangle$ $(l < m)$ have a common missing point if and only if $m - l \equiv \pm(i_q - i_p)$ (mod $\alpha$) for some $p$ and $q$, where $1 \leq p < q \leq u$.

Any line class contains $k(t+1)$ points. Given two line classes $\langle l \rangle$ and $\langle m \rangle$, by Theorem 2.8 every line in $\langle l \rangle$ meets every line in $\langle m \rangle$ in $\lambda$ points, thus between them they cover $k(t+1) + [k - \lambda(t+1)](t+1)$ points. Let $n$ be the number of common missed points, then $n = v - k(t+1) - [k - \lambda(t+1)](t+1)$, which is independent of the choice of $\langle l \rangle$ and $\langle m \rangle$.

Let $T = \{i_1, i_2, \ldots, i_u\}$. We claim that every nonzero residue mod $\alpha$ should appear the same number of times, say $\mu$ times, as a difference of $T$.

First, if $\langle i_1 \rangle, \langle i_2 \rangle, \dots, \langle i_u \rangle$ do not miss any points other than $0, \alpha, 2\alpha, \dots, t\alpha$, consider the class $\langle l \rangle$ where $1 \le l \le \alpha - 1$. The pair of classes $\langle 0 \rangle$ and $\langle l \rangle$ miss $n$ common points. Suppose $\langle 0 \rangle$ and $\langle l \rangle$ both miss a point $w$, where $0 \le w < \alpha$, then $\langle -w \rangle$ and $\langle l - w \rangle$ both miss the point 0 and so they are $\langle i_p \rangle$ and $\langle i_q \rangle$ respectively for some $p$ and $q$. Thus the difference $l \equiv \pm(i_q - i_p)$ (mod $\alpha$) appears once in $T$ for each common missed point less than $\alpha$. By Theorem 3.5 there are $\frac{n}{t+1}$ such points, so $\mu = \frac{n}{t+1}$. Thus our claim is true in this case.

Second, if $\langle i_1 \rangle, \langle i_2 \rangle, \dots, \langle i_u \rangle$ miss a point, say $x$, other than $0, \alpha, 2\alpha, \dots, t\alpha$, then they also miss $t$ other points: $x+\alpha, x+2\alpha, x+3\alpha, \dots, x+t\alpha$. Take $x$ to be the smallest positive number which is missing from $\langle i_1 \rangle, \langle i_2 \rangle, \dots, \langle i_u \rangle$. Thus $0 < x < \alpha$. Let $B_j = \{i_1 + j, i_2 + j, \dots, i_u + j\}$ (mod $\alpha$), where $j = 0, 1, \dots, \alpha - 1$. Since $\langle i_1 \rangle, \langle i_2 \rangle, \dots, \langle i_u \rangle$ miss $x, x+\alpha, x+2\alpha, \dots, x+t\alpha$, we have that $\langle i_1 + (\alpha - x) \rangle, \langle i_2 + (\alpha - x) \rangle, \dots, \langle i_u + (\alpha - x) \rangle$ also miss $0, \alpha, 2\alpha, \dots, t\alpha$. So, $\langle i_1 + (\alpha - x) \rangle, \langle i_2 + (\alpha - x) \rangle, \dots, \langle i_u + (\alpha - x) \rangle$ are exactly the same as $\langle i_1 \rangle, \langle i_2 \rangle, \dots, \langle i_u \rangle$. Accordingly, $\langle i_1 \rangle, \langle i_2 \rangle, \dots, \langle i_u \rangle$ miss the points $-x, \alpha - x, 2\alpha - x, \dots, t\alpha - x$. Thus $\langle i_1 + x \rangle, \langle i_2 + x \rangle, \dots, \langle i_u + x \rangle$ also miss the points $0, \alpha, 2\alpha, \dots, t\alpha$. Hence $B_0 = B_x$. Since $x$ is the smallest positive number which is missing from $\langle i_1 \rangle, \langle i_2 \rangle, \dots, \langle i_u \rangle$, it is not hard to prove that $B_i = B_j$ if and only if $x \mid j - i$, where $i, j = 0, 1, \dots, \alpha - 1$. Meanwhile we also have $x \mid \alpha$. Let $\alpha = rx$, where $r \in \mathbf{N}$ and $\mathbf{N}$ is the set of all natural numbers. Then, all the common missing points of $\langle i_1\rangle, \langle i_2\rangle, \dots, \langle i_u\rangle$ are:

$$\begin{array}{lllll}
0, & \alpha, & 2\alpha, & \dots, & t\alpha, \\
x, & x+\alpha, & x+2\alpha, & \dots, & x+t\alpha, \\
2x, & 2x+\alpha, & 2x+2\alpha, & \dots, & 2x+t\alpha, \\
\dots & \dots & \dots & \dots & \dots \\
(r-1)x, & (r-1)x+\alpha, & (r-1)x+2\alpha, & \dots, & (r-1)x+t\alpha.
\end{array}$$

Therefore, in this case, we have $\mu = \frac{nr}{r(t+1)} = \frac{n}{t+1}$ and hence our claim is also true. Accordingly, $T = \{i_1, i_2, \dots, i_u\}$ is an $(\alpha, u, \mu)$-difference set.

Since $T$ is an $(\alpha, u, \mu)$-difference set, we have

$$\mu(\alpha - 1) = u(u-1).$$

In addition, since $k + u = \alpha$, we have $u = \alpha - k$ and

$$\mu = \frac{(\alpha - k)(\alpha - k - 1)}{\alpha - 1}.$$

If $\langle i_1\rangle, \langle i_2\rangle, \dots, \langle i_u\rangle$ miss a point $x$ other than $0, \alpha, 2\alpha, \dots, t\alpha$, then as we discussed earlier in this proof we have that $\langle i_1+(\alpha-x)\rangle, \langle i_2+(\alpha-x)\rangle, \dots, \langle i_u+(\alpha-x)\rangle$ are the same as $\langle i_1\rangle, \langle i_2\rangle, \dots, \langle i_u\rangle$. In other words, $B_0$ and $B_{\alpha-x}$ have $u$ objects in common, which means $\mu = u$. Thus $| B_0 \cap B_1 |= u$. So, $\langle i_u + 1\rangle = \langle 0\rangle = \langle i_1\rangle$. However, $\langle i_1\rangle = \langle 0\rangle$ implies that $\langle 0\rangle$ misses 0, which is impossible. Therefore, $\langle i_1\rangle, \langle i_2\rangle, \dots, \langle i_u\rangle$ can not have any common missing points other than $0, \alpha, 2\alpha, \dots, t\alpha$. Counting the total number of points of $D$, whether they are covered by two line classes or not, by Lemma 3.28 we get:

$$(k+u)(t+1) = k(t+1) + [k - \lambda(t+1)](t+1) + \mu(t+1).$$

So,

$$u = k - \lambda(t+1) + \mu.$$

$\square$

**Example 3.33.** $\{0, 1, 2, 4, 6, 11, 12, 20, 23\}$ *mod* 26 *is a* $(26, 9, [3, 0]; 1)$-*-difference set. The multiset of its differences is*

$$\begin{array}{cccccccc}
\pm1 & \pm2 & \pm4 & \pm6 & \pm11 & \pm12 & \pm20 & \pm23 \\
\pm1 & \pm3 & \pm5 & \pm10 & \pm11 & \pm19 & \pm22 & \\
\pm2 & \pm4 & \pm9 & \pm10 & \pm18 & \pm21 & & \\
\pm2 & \pm7 & \pm8 & \pm16 & \pm19 & & & \\
\pm5 & \pm6 & \pm14 & \pm17 & & & & \\
\pm1 & \pm13 & \pm16 & & & & & \\
\pm12 & \pm15 & & & & & & \\
\pm3. & & & & & & &
\end{array}$$

*Note that* $\pm23 \equiv \mp3 \pmod{26}$, $\pm22 \equiv \mp4 \pmod{26}$ *and so on. We have that* 13 *is missing from the multiset of differences while each of other nonzero residues appears as a difference exactly three times. By Theorem 3.5. the design generated by this difference set is* 0*-equivalent:*

$$\begin{array}{rccccccccc}
[0] & \mathbf{0}, & 1, & 2, & 4, & 6, & 11, & 12, & 20, & 23 \\
 & 1, & 2, & 3, & 5, & 7, & 12, & 13, & 21, & 24 \\
 & 2, & 3, & 4, & 6, & 8, & 13, & 14, & 22, & 25 \\
 & 3, & 4, & 5, & 7, & 9, & 14, & 15, & 23, & \mathbf{0} \\
\langle 4 \rangle: & 4, & 5, & 6, & 8, & 10, & 15, & 16, & 24, & 1 \\
\langle 5 \rangle: & 5, & 6, & 7, & 9, & 11, & 16, & 17, & 25, & 2
\end{array}$$

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 6, | 7, | 8, | 10, | 12, | 17, | 18, | 0, | 3 |
| | 7, | 8, | 9, | 11, | 13, | 18, | 19, | 1, | 4 |
| $\langle 8\rangle$ : | 8, | 9, | 10, | 12, | 14, | 19, | 20, | 2, | 5 |
| | 9, | 10, | 11, | 13, | 15, | 20, | 21, | 3, | 6 |
| $\langle 10\rangle$ : | 10, | 11, | 12, | 14, | 16, | 21, | 22, | 4, | 7 |
| | 11, | 12, | 13, | 15, | 17, | 22, | 23, | 5, | 8 |
| | 12, | 13, | 14, | 16, | 18, | 23, | 24, | 6, | 9 |
| [13] | 13, | 14, | 15, | 17, | 19, | 24, | 25, | 7, | 10 |
| | 14, | 15, | 16, | 18, | 20, | 25, | 0, | 8, | 11 |
| | 15, | 16, | 17, | 19, | 21, | 0, | 1, | 9, | 12 |
| | 16, | 17, | 18, | 20, | 22, | 1, | 2, | 10, | 13 |
| $\langle 4\rangle$ : | 17, | 18, | 19, | 21, | 23, | 2, | 3, | 11, | 14 |
| $\langle 5\rangle$ : | 18, | 19, | 20, | 22, | 24, | 3, | 4, | 12, | 15 |
| | 19, | 20, | 21, | 23, | 25, | 4, | 5, | 13, | 16 |
| | 20, | 21, | 22, | 24, | 0, | 5, | 6, | 14, | 17 |
| $\langle 8\rangle$ : | 21, | 22, | 23, | 25, | 1, | 6, | 7, | 15, | 18 |
| | 22, | 23, | 24, | 0, | 2, | 7, | 8, | 16, | 19 |
| $\langle 10\rangle$ : | 23, | 24, | 25, | 1, | 3, | 8, | 9, | 17, | 20 |
| | 24, | 25, | 0, | 2, | 4, | 9, | 10, | 18, | 21 |
| | 25, | 0, | 1, | 3, | 5, | 10, | 11, | 19, | 22. |

0 *is missing from four line classes* $\langle 4\rangle$, $\langle 5\rangle$, $\langle 8\rangle$ *and* $\langle 10\rangle$. $\{4, 5, 8, 10\}$, *or* $\{0, 1, 4, 6\}$, *is a* $(13, 4, 1)$*-difference set.*

## 3.4 Finding 0-equivalent Designs with $u = 1$

**Lemma 3.34.** *For a 0-equivalent $(v, k, [\lambda, 0]: t)$-design with $u = 1$, we have $v = (k+1)(t+1)$ and $k = \lambda(t+1)+1$.*

*Proof.* Since $u = 1$, so, by Lemma 3.28, we have $v = (k+1)(t+1)$. Since $\lambda(v-t-1) = k(k-1)$, we have $\lambda k(t+1) = k(k-1)$. So $\lambda(t+1) = k-1$, or $k = \lambda(t+1)+1$. □

For a 0-equivalent $(v, k, [\lambda, 0]: t)$-design with $u = 1$, we have

$$v = [\lambda(t+1)+2]\,(t+1).$$

Thus,

$$\lambda(t+1)^2 + 2(t+1) - v = 0.$$

So,

$$\begin{aligned} t+1 &= \frac{-2 \pm \sqrt{4+4\lambda v}}{2\lambda} \\ &= \frac{-1+\sqrt{1+\lambda v}}{\lambda} \quad \text{(since } t+1>0\text{)}. \end{aligned}$$

Hence, $1+\lambda v$ should be a square. Let $A^2 = 1+\lambda v$, where $A$ is a positive integer. We have that $v = \frac{A^2-1}{\lambda}$, $t+1 = \frac{A-1}{\lambda}$, $k = \lambda(t+1)+1 = A$ and $\lambda \mid A-1$. That is $v = \frac{k^2-1}{\lambda}$, $t+1 = \frac{k-1}{\lambda}$, and $\lambda \mid k-1$. Since $t \geq 1$, so, $\frac{k-1}{\lambda} = t+1 \geq 2$. Hence, $k = \lambda q + 1$ $(q \geq 2)$. Therefore, assuming $v \leq 100$, we get the possible values for $k$:

when $\lambda = 1$, then $k^2 - 1 \leq 100$, so $k \leq 10$, and

$$k = 3, 4, 5, 6, 7, 8, 9, 10;$$

when $\lambda = 2$, then $k^2 - 1 \leq 200$, and $k$ is odd, hence

$$k = 5, 7, 9, 11, 13;$$

when $\lambda = 3$, then $k^2 - 1 \leq 300$, so

$$k = 7, 10, 13, 16;$$

when $\lambda = 4$, then $k^2 - 1 \leq 400$, so

$$k = 9, 13, 17;$$

when $\lambda = 5$, then $k^2 - 1 \leq 500$, so

$$k = 11, 16, 21;$$

when $\lambda = 6$, then $k^2 - 1 \leq 600$, so

$$k = 13, 19;$$

when $\lambda = 7$, then $k^2 - 1 \leq 700$, so

$$k = 15, 22.$$

We list the tables of base sets of 0-equivalent $(v, k, [\lambda, 0]: t)$-designs with $u = 1$ obtained by computer in the Appendix A. Lam [23] gives a table of all $k \leq 50$ for which a $(m, n, k, \lambda)$-RDS exists.

## 3.5 Designs Generated by 0-equivalent Designs with $u = 1$

If $S = \{0, a_2, a_3, \ldots, a_k\}$ is a base set of a 0-equivalent $(v, k, [\lambda, 0]: t)$-design with $u = 1$, then, since $v = (k+1)(t+1) = k(t+1) + (t+1)$, there are exactly $t + 1$ points which are not on any lines in the parallel class $\langle 0 \rangle$.

**Theorem 3.35.** *Let* $S = \{0, a_2, a_3, \ldots, a_k\}$ *be a base set of a* 0*-equivalent* $(v, k, [\lambda, 0]\colon t)$*-design* $D$ *with* $u = 1$, *let* $t+1$ *points which are not on any line in the parallel class* $\langle 0 \rangle$ *be:* $b, b+\alpha, b+2\alpha, \ldots, b+t\alpha$. *Then the set* $T = \{0, a_2, a_3, \ldots, a_k, b, b+\alpha, b+2\alpha, \ldots, b+t\alpha\}$, *obtained by adding those* $t+1$ *points to* $S$, *generates a* $(t+1)$*-equivalent* $(v, k+t+1, [\lambda+2, t+1]\colon t)$*- -design* $E$ *when* $\lambda+2 \neq t+1$*; otherwise it generates a* $(v, k+t+1, \lambda+2)$*-design* $E$.

*Proof.* Consider the differences among the "new points" which are put into a series:

$$b, b+\alpha, b+2\alpha, \ldots, b+t\alpha.$$

We have that there are $t$ pairs of points, which are next to each other, whose difference is $\pm\alpha$: there are $t-1$ pairs of points, which have a point between them, whose difference is $\pm 2\alpha$: there are $t-2$ pairs of points, which have two points between them, whose difference is $\pm 3\alpha$: ...: there is 1 pair of points, that is $b$ and $b+t\alpha$, whose difference is $\pm t\alpha$. Since

$$\alpha + t\alpha = 2\alpha + (t-1)\alpha = \ldots = v,$$

we have that each of

$$\alpha, 2\alpha, 3\alpha, \ldots, t\alpha$$

appears $t+1$ times as a difference in the set $T$.

Because $D$ is 0-equivalent, every two points of

$$b, b+\alpha, b+2\alpha, \ldots, b+t\alpha$$

are on different lines of $D$. By the theorem assumption, points

$$b, b+\alpha, b+2\alpha, \ldots, b+t\alpha$$

are not on any of the $t+1$ lines in the parallel class $\langle 0\rangle$. Since the number of lines not in the parallel class $\langle 0\rangle$ is: $v-(t+1) = (k+1)(t+1)-(t+1) = k(t+1)$, which equals the total number of appearances in $D$ of those $t+1$ new points, we have that each of the lines of $D$ not in the class $\langle 0\rangle$ contains exactly one of the new points. So all the differences of two points, one an "old point" and one a new point, are:

$$\{\pm 1, \pm 2, \pm 3, \ldots, \pm(v-1)\} \setminus \{\pm\alpha, \pm 2\alpha, \pm 3\alpha, \ldots, \pm t\alpha\}.$$

Because $1+(v-1) = 2+(v-2) = \ldots = v$ and $\alpha + t\alpha = 2\alpha + (t-1)\alpha = = \ldots = v$, so, after adding new points to the set $S$, each number in

$$\{1, 2, \ldots, (v-1)\} \setminus \{\alpha, 2\alpha, 3\alpha, \ldots, t\alpha\}$$

appears as a difference 2 extra times. Since each of them appears $\lambda$ times as a difference in the set $S$, we have that they appear $\lambda + 2$ times as differences in the set $T$.

So, $T = \{0, a_2, a_3, \ldots, a_k, b, b+\alpha, b+2\alpha, \ldots, b+t\alpha\}$ generates a $(t+1)$-equivalent $(v, k+t+1, [\lambda+2, t+1]; t)$-design $E$ if $\lambda + 2 \neq t+1$; otherwise it generates a $(v, k+t+1, \lambda+2)$-design $E$. $\square$

**Example 3.36.** *$S = \{0, 1, 2, 4, 9\}$ mod 12 is a $(12, 5, [2, 0]; 1)$-difference set with $u = 1$ which has a unique missing difference 6, so it generates a 0-equivalent design. The parallel class $\langle 0\rangle$ contains two lines:*

| | | | | | |
|---|---|---|---|---|---|
| [0] | 0, | 1, | 2, | 4, | 9 |
| [6] | 6, | 7, | 8, | 10, | 3. |

*There are two points not on either of those two lines in the class* $\langle 0\rangle$*:* 5 *and* 11. *We add* 5 *and* 11 *to the set* $S$ *and get* $T = \{0, 1, 2, 4, 5, 9, 11\}$. *By Theorem 3.35,* $T$ *generates a* 2*-equivalent* $(12, 7, [4, 2]; 1)$*-design:*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| [0] | 0, | 1, | 2, | 4, | 5, | 9, | 11 |
| | 1, | 2, | 3, | 5, | 6, | 10, | 0 |
| | 2, | 3, | 4, | 6, | 7, | 11, | 1 |
| | 3, | 4, | 5, | 7, | 8, | 0, | 2 |
| | 4, | 5, | 6, | 8, | 9, | 1, | 3 |
| | 5, | 6, | 7, | 9, | 10, | 2, | 4 |
| [6] | 6, | 7, | 8, | 10, | 11, | 3, | 5 |
| | 7, | 8, | 9, | 11, | 0, | 4, | 6 |
| | 8, | 9, | 10, | 0, | 1, | 5, | 7 |
| | 9, | 10, | 11, | 1, | 2, | 6, | 8 |
| | 10, | 11, | 0, | 2, | 3, | 7, | 9 |
| | 11, | 0, | 1, | 3, | 4, | 8, | 10. |

**Example 3.37.** *From Example 3.8, we know that* $S = \{0, 1, 3, 7\}$ *mod* 15 *is a* $(15, 4, [1, 0]; 2)$*-difference set with* $u = 1$ *which has two missing differences* 5 *and* 10 *and it generates a* 0*-equivalent design. The parallel class* $\langle 0\rangle$ *contains three lines:*

| | | | | |
|---|---|---|---|---|
| [0] | 0, | 1, | 3, | 7 |
| [5] | 5, | 6, | 8, | 12 |
| [10] | 10, | 11, | 13, | 2. |

*There are three points not on any line in the class* $\langle 0\rangle$*:* 4, 9 *and* 14. *By adding these three points to* $S$, *we get* $T = \{0, 1, 3, 4, 7, 9, 14\}$. *By Theorem 3.35, since* $\lambda + 2 = t + 1 = 3$, $T$ *generates a* $(15, 7, 3)$*-design.*

$(t+1)$-equivalent $(v, k+t+1, [\lambda+2, t+1]; t)$-difference sets and $(v, k+t+1, \lambda+2)$-difference sets which can not be acquired by adding points to a $(v, k, [1, 0]; t)$-difference set with $u = 1$ are more interesting. A computer search might be used to obtain such difference sets. Appendix B is a list of $(t+1)$-equivalent $(v, k+t+1, [\lambda+2, t+1]; t)$-difference sets or $(v, k+t+1, \lambda+2)$-difference sets obtained by computer.

# Chapter 4

# Doubly Equivalent Designs

In this Chapter, we will introduce the concept of the doubly equivalent design as well as the super class. We will describe the structure of super classes and discuss properties of doubly equivalent designs. We will generalize results in Chapter 3 to doubly equivalent designs. The main result is Theorem 4.10.

## 4.1 Basic Facts

A $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_m])$-design with $m > 2$ can be both $\lambda_1$-equivalent and $\lambda_2$-equivalent.

**Example 4.1.** $\{0, 1, 2, 4, 12, 17\}$ *mod* 21 *is a* $(21, 6, [2, 1, 0] : 12, 6, 2)$-

*-difference set: the multiset of its differences is*

$$\begin{array}{lllll} \pm 1 & \pm 2 & \pm 4 & \pm 12 & \pm 17 \\ \pm 1 & \pm 3 & \pm 11 & \pm 16 & \\ \pm 2 & \pm 10 & \pm 15 & & \\ \pm 8 & \pm 13 & & & \\ \pm 5. & & & & \end{array}$$

*Each of*

$$3, 6, 9, 12, 15, 18$$

*appears in the multiset of differences just once and both 7 and 14 are missing while all other nonzero residues appear twice.*

*By Theorem 3.5, the design generated by this difference set is both 1--equivalent and 0-equivalent:*

$$\begin{array}{lcccccc} [0] & 0, & 1, & 2, & 4, & 12, & 17 \\ & 1, & 2, & 3, & 5, & 13, & 18 \\ & 2, & 3, & 4, & 6, & 14, & 19 \\ [3] & 3, & 4, & 5, & 7, & 15, & 20 \\ & 4, & 5, & 6, & 8, & 16, & 0 \\ & 5, & 6, & 7, & 9, & 17, & 1 \\ [6] & 6, & 7, & 8, & 10, & 18, & 2 \\ [7] & 7, & 8, & 9, & 11, & 19, & 3 \\ & 8, & 9, & 10, & 12, & 20, & 4 \\ [9] & 9, & 10, & 11, & 13, & 0, & 5 \end{array}$$

| | | | | | | |
|---|---|---|---|---|---|---|
| | 10, | 11, | 12, | 14, | 1, | 6 |
| | 11, | 12, | 13, | 15, | 2, | 7 |
| [12] | 12, | 13, | 14, | 16, | 3, | 8 |
| | 13, | 14, | 15, | 17, | 4, | 9 |
| [14] | 14, | 15, | 16, | 18, | 5, | 10 |
| [15] | 15, | 16, | 17, | 19, | 6, | 11 |
| | 16, | 17, | 18, | 20, | 7, | 12 |
| | 17, | 18, | 19, | 0, | 8, | 13 |
| [18] | 18, | 19, | 20, | 1, | 9, | 14 |
| | 19, | 20, | 0, | 2, | 10, | 15 |
| | 20, | 0, | 1, | 3, | 11, | 16. |

**Definition 4.2.** *A $(v, k, [\lambda_1, \lambda_2, \ldots]: s, t, \ldots)$-design which is both $\lambda_1$--equivalent and $\lambda_2$-equivalent is called a* ***doubly equivalent design****. A* ***doubly equivalent difference set*** *is defined similarly.*

Clearly, a doubly equivalent design (or difference set) is also a singly equivalent design (or difference set respectively). In this Chapter, we always denote $\frac{v}{s+1}$ by $\alpha$ and $\frac{v}{t+1}$ by $\beta$ respectively.

**Theorem 4.3.** *If there exists a $(v, k, [\lambda_1, \lambda_2, \ldots]: s, t, \ldots)$-design which is both $\lambda_1$- and $\lambda_2$-equivalent, then $(s+1, t+1) = 1$ and $(s+1)(t+1) \mid v$.*

*Proof.* By Theorem 3.5, we have $s+1 \mid v$ and $t+1 \mid v$. Let $\alpha = \frac{v}{s+1}$ and $\beta = \frac{v}{t+1}$. Since $\lambda_1 \neq \lambda_2$, a nonzero residue cannot appear both $\lambda_1$ and $\lambda_2$ times as a difference. Hence, we must have $v = [\alpha, \beta]$, where $[\alpha, \beta]$ is the least common multiple of $\alpha$ and $\beta$. Thus $(s+1, t+1) = (\frac{v}{\alpha}, \frac{v}{\beta}) = 1$. Therefore, $(s+1)(t+1) \mid v$. □

## 4.2 Super Classes

**Definition 4.4.** *In a $\lambda$-equivalent $(v, k, [\dots, \lambda]: t)$-design, the set $C$ of all lines which are $\lambda$-intersecting to the line $[i]$ is called the* **$\lambda$-equivalence class** $\langle i\rangle_\lambda$ *$(i = 0, 1, \dots, \frac{v}{t+1} - 1)$. If $\lambda = 0$, then we just simply denote $\langle i\rangle_\lambda$ by $\langle i\rangle$.*

**Definition 4.5.** *Let $D$ be a $(v, k, [\lambda_1, \lambda_2, \dots]: s, t, \dots)$-design which is both $\lambda_1$- and $\lambda_2$-equivalent. A* **super class $\mathcal{S}$** *containing a line $[i]$ in $D$ is the $\lambda_1$-equivalence class $\langle i\rangle_{\lambda_1}$ union all the $\lambda_2$-equivalence classes containing a line in $\langle i\rangle_{\lambda_1}$. We denote the super class $\mathcal{S}$ containing the line $[i]$ by $\hat{i}$.*

**Theorem 4.6.** *Let $D$ be a $(v, k, [\lambda_1, \lambda_2, \dots]: s, t, \dots)$-design which is both $\lambda_1$- and $\lambda_2$-equivalent and $\mathcal{S}$ be a super class in $D$. Then the following five statements are equivalent to each other:*

*(1)* $[i_1], [i_2] \in \mathcal{S}$;

*(2)* $\exists\, [i_3]$ *such that* $[i_1] \overset{\lambda_1}{\approx} [i_3]$ *and* $[i_2] \overset{\lambda_2}{\approx} [i_3]$;

*(3)* $\exists\, [i_4]$ *such that* $[i_1] \overset{\lambda_2}{\approx} [i_4]$ *and* $[i_2] \overset{\lambda_1}{\approx} [i_4]$;

*(4)* $i_1 - i_2 = a\alpha + b\beta$, *where* $a, b \in \mathbf{Z}$;

*(5)* $d \mid i_1 - i_2$, *where* $d = (\alpha, \beta)$.

*Proof.* Let $\alpha = \frac{v}{s+1}$ and $\beta = \frac{v}{t+1}$.

(1) $\Rightarrow$ (2). Since $[i_1], [i_2] \in \mathcal{S}$, there exist $a, b \in \mathbf{Z}$ such that $[i_1 + a\beta] \overset{\lambda_1}{\approx} [i_2 + b\beta]$. Thus $[i_1] \overset{\lambda_1}{\approx} [i_2 + (b-a)\beta]$. Take $i_3 = i_2 + (b-a)\beta$. Then $[i_1] \overset{\lambda_1}{\approx} [i_3]$ and $[i_2] \overset{\lambda_2}{\approx} [i_3]$.

(2) $\Rightarrow$ (1). If $\exists$ $[i_3]$ such that $[i_1] \overset{\lambda_1}{\sim} [i_3]$ and $[i_2] \overset{\lambda_2}{\sim} [i_3]$, then, by Definition 4.5, we have $[i_1], [i_2] \in \widehat{i_1}$.

Therefore, (1) and (2) are equivalent. Similarly, (1) and (3) are equivalent.

(2) $\Rightarrow$ (4). If $[i_1] \overset{\lambda_1}{\sim} [i_3]$ and $[i_2] \overset{\lambda_2}{\sim} [i_3]$, then $i_1 - i_3 = a\alpha$ and $i_2 - i_3 = b'\beta$, where $a, b' \in \mathbf{Z}$. So, $i_1 - i_2 = a\alpha - b'\beta = a\alpha + b\beta$, where $b = -b'$.

(4) $\Rightarrow$ (2). If $i_1 - i_2 = a\alpha + b\beta$, then set $i_3 = i_1 - a\alpha = i_2 + b\beta$. Hence, $[i_1] \overset{\lambda_1}{\sim} [i_3]$ and $[i_2] \overset{\lambda_2}{\sim} [i_3]$.

Thus, (2) and (4) are equivalent.

(4) $\Rightarrow$ (5). Since $i_1 - i_2 = a\alpha + b\beta$ and $d \mid \alpha, \beta$, so, $d \mid i_1 - i_2$.

(5) $\Rightarrow$ (4). Because $d = (\alpha, \beta)$, we have $d = a_1\alpha + b_1\beta$, where $a_1, b_1 \in \mathbf{Z}$. Let $i_1 - i_2 = n_1 d$, where $n_1 \in \mathbf{Z}$. Then, $i_1 - i_2 = (n_1 a_1)\alpha + (n_1 b_1)\beta = a\alpha + b\beta$, where $a = n_1 a_1, b = n_1 b_1 \in \mathbf{Z}$.

Accordingly, (4) and (5) are equivalent.

Therefore, all five statements are equivalent to each other. $\square$

**Corollary 4.7.** *Let $D$ be a $(v, k, [\lambda_1, \lambda_2, \dots]: s, t, \dots)$-design which is both $\lambda_1$- and $\lambda_2$-equivalent. Then all super classes in $D$ constitute a partition of all lines of $D$. Let $S$ be a super class in $D$. Then $\mid S \mid = (s+1)(t+1)$.*

*Proof.* By (4) of Theorem 4.6, the relation that two lines are in the same super class is an equivalence relation. So, all super classes in $D$ constitute a partition of all lines of $D$. Because a super class contains $s+1$ $\lambda_2$-equivalence classes, so, $\mid S \mid = (s+1)(t+1)$. $\square$

Let $D$ be a $(v, k, [\lambda_1, \lambda_2, \dots]: s, t, \dots)$-design which is both $\lambda_1$- and $\lambda_2$-equivalent. Since the lines in the same $\lambda_1$-equivalence class are in the same super class, we see that all super classes in $D$ constitute a partition of all $\lambda_1$-equivalence classes in $D$. Similarly, we also see that all super classes in $D$ constitute a partition of all $\lambda_2$-equivalence classes in $D$.

**Theorem 4.8.** *Let $D$ be a $(v, k, [\lambda_1, \lambda_2, \ldots]; s, t, \ldots)$-design which is both $\lambda_1$- and $\lambda_2$-equivalent and $d = (\alpha, \beta)$, where $\alpha = \frac{v}{s+1}$ and $\beta = \frac{v}{t+1}$. Then $v = (s+1)(t+1)d$.*

*Proof.* By (5) of Theorem 4.6, two $\lambda_2$-equivalent classes $\langle i\rangle_{\lambda_2}$ and $\langle j\rangle_{\lambda_2}$ are in the same super class if and only if $d \mid i-j$. So, two $\lambda_2$-equivalent classes in

$$\langle 0\rangle_{\lambda_2}, \langle 1\rangle_{\lambda_2}, \ldots, \langle \beta-1\rangle_{\lambda_2}$$

are in the same super class if and only if their "distance" is a multiple of $d$. Hence, we have exactly $d$ super classes:

$$\hat{0}, \hat{1}, \ldots, \widehat{d-1}.$$

Counting the total lines of $D$, by Corollary 4.7, we have $v = (s+1)(t+1)d$. $\square$

Although $v = (s+1)(t+1)d$ can be proved directly by Number Theory, the above proof is from the point of view of the super classes. Meanwhile, the equivalence relation generated by super classes is the join of two equivalence relations: $\lambda_1$- and $\lambda_2$-equivalence. So, we can also obtain the above results from Ring Theory.

**Example 4.9.** $\{0, 1, 2, 4, 6, 7, 11, 17\}$ *mod* 24 *is a* $(24, 8, [3, 2, 1, 0]; 14, 6, 2, 1)$-

*-difference set: the multiset of its differences is*

$$\begin{array}{lllllll}
\pm 1 & \pm 2 & \pm 4 & \pm 6 & \pm 7 & \pm 11 & \pm 17 \\
\pm 1 & \pm 3 & \pm 5 & \pm 6 & \pm 10 & \pm 16 & \\
\pm 2 & \pm 4 & \pm 5 & \pm 9 & \pm 15 & & \\
\pm 2 & \pm 3 & \pm 7 & \pm 13 & & & \\
\pm 1 & \pm 5 & \pm 11 & & & & \\
\pm 4 & \pm 10 & & & & & \\
\pm 6. & & & & & &
\end{array}$$

*Each of*

$$8, 16$$

*appears in the multiset of differences just once and* 12 *is missing while all other nonzero residues appear either twice or three times.*

*By Theorem 3.5, the design generated by this difference set is both* 1*- and* 0*-equivalent:*

$$\begin{array}{lllllllll}
[0] & 0, & 1, & 2, & 4, & 6, & 7, & 11, & 17 \\
 & 1, & 2, & 3, & 5, & 7, & 8, & 12, & 18 \\
 & 2, & 3, & 4, & 6, & 8, & 9, & 13, & 19 \\
 & 3, & 4, & 5, & 7, & 9, & 10, & 14, & 20 \\
 & 4, & 5, & 6, & 8, & 10, & 11, & 15, & 21 \\
 & 5, & 6, & 7, & 9, & 11, & 12, & 16, & 22 \\
 & 6, & 7, & 8, & 10, & 12, & 13, & 17, & 23 \\
 & 7, & 8, & 9, & 11, & 13, & 14, & 18, & 0 \\
[8] & 8, & 9, & 10, & 12, & 14, & 15, & 19, & 1
\end{array}$$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 9, | 10, | 11, | 13, | 15, | 16, | 20, | 2 |
| | 10, | 11, | 12, | 14, | 16, | 17, | 21, | 3 |
| | 11, | 12, | 13, | 15, | 17, | 18, | 22, | 4 |
| [12] | 12, | 13, | 14, | 16, | 18, | 19, | 23, | 5 |
| | 13, | 14, | 15, | 17, | 19, | 20, | 0, | 6 |
| | 14, | 15, | 16, | 18, | 20, | 21, | 1, | 7 |
| | 15, | 16, | 17, | 19, | 21, | 22, | 2, | 8 |
| [16] | 16, | 17, | 18, | 20, | 22, | 23, | 3, | 9 |
| | 17, | 18, | 19, | 21, | 23, | 0, | 4, | 10 |
| | 18, | 19, | 20, | 22, | 0, | 1, | 5, | 11 |
| | 19, | 20, | 21, | 23, | 1, | 2, | 6, | 12 |
| | 20, | 21, | 22, | 0, | 2, | 3, | 7, | 13 |
| | 21, | 22, | 23, | 1, | 3, | 4, | 8, | 14 |
| | 22, | 23, | 0, | 2, | 4, | 5, | 9, | 15 |
| | 23, | 0, | 1, | 3, | 5, | 6, | 10, | 16. |

*Since* $\alpha = \frac{v}{s+1} = 8$ *and* $\beta = \frac{v}{t+1} = 12$, *we have* $d = (\alpha, \beta) = 4$. *By Theorem 4.6, the super class* $\hat{0}$ *contains* 6 *lines:* [0], [4], [8], [12], [16] *and* [20]. *By Theorem 4.8,*

$$v = (s+1)(t+1)d = 3 \cdot 2 \cdot 4 = 24.$$

**Theorem 4.10.** *For a* $\lambda_2$*- and* 0*-equivalent* $(v, k, [\lambda_1, \lambda_2, 0]; r, s, t)$*-design* $D$, *let* $\alpha = \frac{v}{s+1}$ *and* $\beta = \frac{v}{t+1}$. *If* $d = \frac{v}{(s+1)(t+1)} > 1$, *then* $u > 1$. *In addition, assume the point* 0 *is missing from the parallel classes* $\langle i_1 \rangle, \langle i_2 \rangle, \ldots, \langle i_u \rangle$, *where* $0 \le i_1 < i_2 < \ldots < i_u < \beta$, *then* $\{i_1, i_2, \ldots, i_u\}$ *is a* $\mu_2$*-equivalent* $(\beta, u, [\mu_1, \mu_2]; s)$*-difference set and* $u = k - \lambda_1(t+1) + \mu_1$, $u = k - \lambda_1 t - \lambda_2 + \mu_2$.

*Thus we have* $\lambda_1 - \lambda_2 = \mu_1 - \mu_2$ *(when* $\lambda_1 < \lambda_2$, *we may write* $\lambda_2 - \lambda_1 = = \mu_2 - \mu_1$*).*

*Proof.* Since $v = (s+1)(t+1)d$, by Theorem 4.8, $d = (\alpha, \beta)$. $D$ has $d$ super classes:

$$\hat{0}, \hat{1}, \ldots, \widehat{d-1}.$$

Since $d > 1$, we have that $\langle 0 \rangle$ and $\langle d \rangle$ are in the same super class while $\langle 0 \rangle$ and $\langle 1 \rangle$ are in different super classes. So, every line in $\langle d \rangle$ meets one line in $\langle 0 \rangle$ in $\lambda_2$ points while it meets every other line in $\langle 0 \rangle$ in $\lambda_1$ points. Every line in $\langle 1 \rangle$ meets every line in $\langle 0 \rangle$ in $\lambda_1$ points. If $\lambda_1 > \lambda_2$, then there are some points not on any lines of $\langle 0 \rangle$ and $\langle 1 \rangle$; if $\lambda_1 < \lambda_2$, then there are some points not on any lines of $\langle 0 \rangle$ and $\langle d \rangle$. In either case, by Theorem 3.27, 0 is missing from more than one parallel class, that is, $u > 1$.

Assume 0 is missing from the line classes $\langle i_1 \rangle$, $\langle i_2 \rangle$, ..., $\langle i_u \rangle$, where $0 \leq i_1 < i_2 < \ldots < i_u < \beta$. By Theorem 3.27 again, we have (in the following discussion, for each line class $\langle a \rangle$, the value $a$ should be taken mod $\beta$):

$$\begin{array}{lllll}
\langle i_1\rangle, & \langle i_2\rangle, & \dots, & \langle i_u\rangle & \text{miss} \\
0, & \beta, & 2\beta, & \dots, & t\beta; \\
\\
\langle i_1+1\rangle, & \langle i_2+1\rangle, & \dots, & \langle i_u+1\rangle & \text{miss} \\
1, & 1+\beta, & 1+2\beta, & \dots, & 1+t\beta; \\
\\
\langle i_1+2\rangle, & \langle i_2+2\rangle, & \dots, & \langle i_u+2\rangle & \text{miss} \\
2, & 2+\beta, & 2+2\beta, & \dots, & 2+t\beta; \\
\\
\dots & \dots & \dots & \dots & \dots \\
\\
\langle i_1+\beta-1\rangle, & \langle i_2+\beta-1\rangle, & \dots, & \langle i_u+\beta-1\rangle & \text{miss} \\
\beta-1, & \beta-1+\beta, & \beta-1+2\beta, & \dots, & \beta-1+t\beta.
\end{array}$$

By Theorem 3.27, a line class $\langle l\rangle$ misses a point $x$ if and only if $\langle l-x\rangle$ misses 0, thus $\langle l-x\rangle = \langle i_p\rangle$ for some $p$ ($1 \le p \le u$). So, two line classes $\langle l\rangle$ and $\langle m\rangle$ ($l < m$) have a common missing point if and only if $m-l \equiv \pm(i_q - i_p)$ (mod $\beta$) for some $p$ and $q$, where $1 \le p < q \le u$.

Let $T = \{i_1, i_2, \dots, i_u\}$. Any line class contains $k(t+1)$ points. Given two line classes $\langle l\rangle$ and $\langle m\rangle$ in the same super class, we have that every line in $\langle l\rangle$ meets one line in $\langle m\rangle$ in $\lambda_2$ points while it meets every other line in $\langle m\rangle$ in $\lambda_1$ points. Thus between them they cover $k(t+1) + [k - \lambda_1 t - \lambda_2)](t+1)$ points. Let $n$ be the number of common missed points, then $n = v -$ $-k(t+1) - [k - \lambda_1 t - \lambda_2)](t+1)$, which is independent of the choice of $\langle l\rangle$ and $\langle m\rangle$ as far as they are in the same super class. Meanwhile, two line classes $\langle l\rangle$ and $\langle m\rangle$ are in the same super class if and only if $d \mid m-l$. Notice that $(s+1)d = \beta$. Then, as in Theorem 3.32, we have that each of $d,\ 2d,\ \ldots,\ sd$ must appear the same number of times, say $\mu_2$ times, as a difference of $T$. Similarly, each nonzero residue not in $\{d, 2d, \ldots, sd\}$ must appear the same number of times, say $\mu_1$ times, as a difference of $T$. Therefore, $T = \{i_1, i_2, \ldots, i_u\}$ is a $(\beta, u, [\mu_1, \mu_2]\colon s)$-difference set. By Theorem 3.5, it is a $\mu_2$-equivalent difference set.

If $\langle i_1\rangle, \langle i_2\rangle, \ldots, \langle i_u\rangle$ miss a point, say $x$, other than $0, \beta, 2\beta, \ldots, t\beta$, then they also miss $t$ other points: $x+\beta, x+2\beta, \ldots, x+t\beta$. We may assume $0 < x < \beta$. Since $\langle i_1\rangle, \langle i_2\rangle, \ldots, \langle i_u\rangle$ miss $x, x+\beta, \ldots, x+t\beta$, we have that $\langle i_1+(\beta-x)\rangle, \langle i_2+(\beta-x)\rangle, \ldots, \langle i_u+(\beta-x)\rangle$ also miss $0, \beta, 2\beta, \ldots, t\beta$. Thus $\langle i_1+(\beta-x)\rangle, \langle i_2+(\beta-x)\rangle, \ldots, \langle i_u+(\beta-x)\rangle$ are the same as $\langle i_1\rangle, \langle i_2\rangle, \ldots, \langle i_u\rangle$. In other words, if we use $B_i$ to denote the $i$-th block of the design generated by $T$ $(i = 0, 1, \ldots, \beta-1)$, then $B_0$ and $B_{\beta-x}$ have $u$ objects in common. By Theorem 2.8, $\beta - x$ appears $u$ times as a difference in $T$. If $d \nmid \beta - x$, then $\mu_1 = u$. Thus $\mid B_0 \cap B_1 \mid = u$. So, $\langle i_u + 1\rangle = \langle 0\rangle = \langle i_1\rangle$. However, $\langle i_1\rangle = \langle 0\rangle$ implies that $\langle 0\rangle$ misses 0, which is impossible. Therefore, $d \mid \beta - x$. So, $\mu_2 = u$ and $d \mid x$.

If $\lambda_1 > \lambda_2$, then $\mu_1 > \mu_2 = u$, which is a contradiction by Corollary 2.9. Hence $\lambda_1 < \lambda_2$. Since $\mu_2 = u$, we have $B_0 = B_d$. Thus, $\langle i_1\rangle, \langle i_2\rangle, \ldots, \langle i_u\rangle$ also miss $d, d+\beta, d+2\beta, \ldots, d+t\beta$. Similarly, they also miss $id, id+\beta, id+2\beta, \ldots, id+t\beta$, for $i = 2, 3, \ldots s$. Accordingly, since $d \mid x$, all the common missed points of $\langle i_1\rangle, \langle i_2\rangle, \ldots, \langle i_u\rangle$ are:

$$\begin{array}{lllll}
0, & \beta, & 2\beta, & \ldots, & t\beta, \\
d, & d+\beta, & d+2\beta, & \ldots, & d+t\beta, \\
2d, & 2d+\beta, & 2d+2\beta, & \ldots, & 2d+t\beta, \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
sd, & sd+\beta, & sd+2\beta, & \ldots, & sd+t\beta.
\end{array}$$

Hence, counting the total number of points of $D$, whether they are covered by $\langle 0\rangle$ and $\langle d\rangle$ or not, by Lemma 3.28 we have

$$(k+u)(t+1) = k(t+1) + [k - \lambda_1 t - \lambda_2](t+1) + \frac{\mu_2}{s+1}(s+1)(t+1).$$

Thus

$$u = k - \lambda_1 t - \lambda_2 + \mu_2.$$

Similarly, counting the total number of points of $D$, whether they are covered by $\langle 0\rangle$ and $\langle 1\rangle$ or not, we obtain

$$u = k - \lambda_1(t+1) + \mu_1.$$

(Notice that in this case we have $\mu_2 = u$ and $k - \lambda_1 t - \lambda_2 = 0$).

If $\langle i_1\rangle, \langle i_2\rangle, \ldots, \langle i_u\rangle$ do not have any common missed points other than $0, \beta, 2\beta, \ldots, t\beta$, then counting the total number of points of $D$, whether they are covered by $\langle 0\rangle$ and $\langle d\rangle$ or not, we get

$$(k+u)(t+1) = k(t+1) + [k - \lambda_1 t - \lambda_2](t+1) + \mu_2(t+1).$$

So,

$$u = k - \lambda_1 t - \lambda_2 + \mu_2.$$

Similarly, counting the total number of points of $D$, whether they are covered by $\langle 0\rangle$ and $\langle 1\rangle$ or not, we obtain

$$u = k - \lambda_1(t+1) + \mu_1.$$

□

## 4.3 $\lambda$- and 0-equivalent Designs with $u = 0$

**Theorem 4.11.** *Let $D$ be a $\lambda_2$- and 0-equivalent $(v, k, [\lambda_1, \lambda_2, 0]: r, s, t)$--design with $u = 0$, then $v = k(t+1)$, $k = t\lambda_1 + \lambda_2$, $k = s+1$, $r = st$.*

*Proof.* Since $u = 0$, by Lemma 3.28, $v = (k+u)(t+1) = k(t+1)$. Because $u = 0$ again, by Theorem 4.10, we have that $d = 1$. Accordingly, a line $[l]$ not in the parallel class $\langle 0\rangle$ meets one line in $\langle 0\rangle$ in $\lambda_2$ points while meeting every other line in $\langle 0\rangle$ in $\lambda_1$ points. Since $u = 0$, every point on the line $[l]$ should be on some line in $\langle 0\rangle$ by Theorem 3.27. Thus, $k = t\lambda_1 + \lambda_2$. Since $v = k(t+1) = (s+1)(t+1)d$ and $d = 1$, we have $k = (s+1)d = s+1$. Since $v = (s+1)(t+1)$ and $r+s+t = v-1$, we have $r = st$. □

We can also derive $k = t\lambda_1 + \lambda_2$ from the equalities $k(k-1) = r\lambda_1 + s\lambda_2$, $k = s+1$ and $r = st$.

Under the assumption of Theorem 4.11, since $d = 1$, $D$ just has one superclass, which contains all the lines of $D$.

By Theorem 4.11, given $\lambda_1$, $\lambda_2$ and $t$, we can determine the values of the other parameters $v$, $k$, $r$ and $s$. Then we run a computer program to see whether there exist any $\lambda_2$- and 0-equivalent difference sets $(v, k, [\lambda_1, \lambda_2, 0]: r, s, t)$ with $u = 0$.

**Example 4.12.** $\{0, 1, 2, 4, 14, 15, 19, 21\}$ *mod* 24 *is a* $(24, 8, [3, 2, 0]: 14, 7, 2)$-*-difference set: the multiset of its differences is*

$$\begin{array}{lllllll}
\pm 1 & \pm 2 & \pm 4 & \pm 14 & \pm 15 & \pm 19 & \pm 21 \\
\pm 1 & \pm 3 & \pm 13 & \pm 14 & \pm 18 & \pm 20 & \\
\pm 2 & \pm 12 & \pm 13 & \pm 17 & \pm 19 & & \\
\pm 10 & \pm 11 & \pm 15 & \pm 17 & & & \\
\pm 1 & \pm 5 & \pm 7 & & & & \\
\pm 4 & \pm 6 & & & & & \\
\pm 2. & & & & & &
\end{array}$$

*Each of*

$$3, 6, 9, 12, 15, 18, 21$$

*appears in the multiset of differences exactly twice and both* 8 *and* 16 *are missing, while all other nonzero residues appear three times.*

*By Theorem 3.5, the design generated by this difference set is both* 2*-equivalent and* 0*-equivalent.*

## 4.4 Designs Generated by $\lambda$- and 0-equivalent Designs with $u = 1$

If $S = \{0, a_2, a_3, \ldots, a_k\}$ is a base set of a $\lambda$- and 0-equivalent $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_{m-2}, \lambda, 0]: t)$-design with $u = 1$, then, since

$$v = (k + 1)(t + 1) = k(t + 1) + (t + 1),$$

there are exactly $t + 1$ points which are not on any lines in the parallel class $\langle 0 \rangle$. So, we can extend Theorem 3.35 to the case of doubly equivalent designs.

**Theorem 4.13.** *Let* $S = \{0, a_2, a_3, \ldots, a_k\}$ *be a base set of a* $\lambda$*- and* 0*-equivalent* $(v, k, [\lambda_1, \lambda_2, \ldots, \lambda_{m-2}, \lambda, 0]; \ldots, s, t)$*-design* $D$ *with* $u = 1$, *let* $t+1$ *points which are not on any lines in the parallel class* $\langle 0 \rangle$ *be:*

$$b, b + \alpha, b + 2\alpha, \ldots, b + t\alpha.$$

*Then the set* $T = \{0, a_2, a_3, \ldots, a_k, b, b + \alpha, b + 2\alpha, \ldots, b + t\alpha\}$*. obtained by adding those* $t + 1$ *points to* $S$*, generates another design:*

*(1) if* $t + 1 = \lambda_i + 2$ *for some* $i$ $(1 \leq i \leq m - 2)$*, then it generates a* $(\lambda + 2)$*-equivalent* $(v, k + t + 1, [\lambda_1 + 2, \lambda_2 + 2, \ldots, \lambda_{m-2} + 2, \lambda + 2]; s)$*-design;*

*(2) if* $t + 1 = \lambda + 2$*, then it generates a* $(v, k + t + 1, [\lambda_1 + 2, \lambda_2 + 2, \ldots, \lambda_{m-2} + 2, \lambda + 2]; s + t)$*-design;*

*(3) if* $t + 1 \neq \lambda_1 + 2, \lambda_2 + 2, \ldots, \lambda_{m-2} + 2, \lambda + 2$*, then it generates a* $(\lambda + 2)$*- and* $(t + 1)$*-equivalent* $(v, k + t + 1, [\lambda_1 + 2, \lambda_2 + 2, \ldots, \lambda_{m-2} + 2, \lambda + 2, t + 1]; \ldots, s, t)$*-design.*

*Proof.* The proof is similar to the proof of Theorem 3.35. $\square$

# Chapter 5

# Some More Results

In this Chapter, we will give some more results on singly or doubly equivalent designs.

## 5.1 Difference Set Constructions

An example of a $(v, k, [\lambda_1, \lambda_2, \lambda_3])$-design, based on a difference set, is the following. Let $m$ and $n$ be distinct positive integers each greater than or equal to 2. Consider an $m$-by-$n$ chessboard whose squares are coordinatized by the pairs $(i, j)$, $i = 0, 1, \ldots, m-1$; $j = 0, 1, \ldots, n-1$. The design is formed in this way: the points are all the squares $(i, j)$, where $(i, j) \in \mathbf{Z}_m \times \mathbf{Z}_n$, and for each $(i, j) \in \mathbf{Z}_m \times \mathbf{Z}_n$ we take as a block the set of all the squares $(k, l)$ such that the square $(k, l)$ is on the same row or the same column as the square $(i, j)$ and $(k, l) \neq (i, j)$. Such a design has parameters $(v, k, [\lambda_1, \lambda_2, \lambda_3])$ where $v = mn$, $k = m + n - 2$, $\lambda_1 = 2$, $\lambda_2 = m - 2$ and $\lambda_3 = n - 2$. A second such design has the same points as the first design, however, for each

$(i,j) \in \mathbf{Z}_m \times \mathbf{Z}_n$ we take as a block the set of all the squares $(k,l)$ on the same row or the same column as the square $(i,j)$. For this design $v = mn$, $k = m+n-1$, $\lambda_1 = 2$, $\lambda_2 = m$ and $\lambda_3 = n$. An important special case is when $m$ and $n$ are relatively prime. In this case we may consider the points of the design as elements of $\mathbf{Z}_{mn}$ where the elements of $\mathbf{Z}_m \times \mathbf{Z}_n$ are mapped into the elements of $\mathbf{Z}_{mn}$ by mapping the generator $(1,1)$ to 1. In this case the first design has as a difference set $m, 2m, \ldots, (n-1)m, n, 2n, \ldots, (m-1)n$ while adjoining a 0 to this set yields a difference set for the second design.

**Theorem 5.1.** *There exists a $(n-2)$-equivalent $(4n, n+2, [2, n-2])$-difference set, where $(n,4) = 1$.*

*Proof.* Let $m = 4$. Construct the first design $D$ in the previous example. Let $E$ be the image of the design $D$ under the isomorphism $\phi$, between $\mathbf{Z}_m \times \mathbf{Z}_n$ and $\mathbf{Z}_{mn}$, which maps the generator $(1,1)$ to 1. Let the block, in $D$, which consists of all the squares not equal to $(1,1)$ but on the same row or column as the square $(1,1)$ be $S$, and let $[0] = \phi(S)$, which is a block in $E$. Then all blocks of $E$ are $[0], [1], \ldots, [4n-1]$.

We have that $|\ [i] \cap [0]\ | = n-2$ if and only if $4 \mid i$, where $0 < i \leq 4n-1$. So, by Theorem 2.8 and Theorem 3.5, $E$ is a $(n-2)$-equivalent $(4n, n+2, [2, n-2])$-design. A base set of $E$ is a $(n-2)$-equivalent $(4n, n+2, [2, n-2])$-difference set. $\square$

Similarly, we have

**Theorem 5.2.** *If $(m,n) = 1$ and $m, n \neq 4$, then there exists a $(m-2)$- and $(n-2)$-equivalent $(mn, m+n-2, [2, m-2, n-2])$-difference set.*

Let $m = 3$ and $n = 2$. Based on Theorem 5.2 and the construction of the first design in the above example, we have that $\{0, 1, 2\}$ is a $(6, 3, [2, 1, 0])$--difference set and it is 1- and 0-equivalent.

## 5.2 Some Necessary Conditions

By Lemma 2.42, we have

**Lemma 5.3.** *All eigenvalues of the $n \times n$ matrix $J$ of all 1's are 0 ($(n-1)$--multiplicity) and $n$.*

We now generalize Theorem 2.3 of Elliot and Butson [12] to the case of arbitrary divisible difference sets in $\mathbf{Z}_v$. This also represents a generalization of Theorem 2.44 of this thesis. Part (2) of this Theorem appears in Ko and Ray-Chaudhuri [20], we give an alternate proof and give an explicit form for the square.

**Theorem 5.4.** *Assume that $v$ is even and there exists a $\lambda_2$-equivalent $(v, k, [\lambda_1, \lambda_2]; t)$-design, then:*

*(1) if $\alpha = \frac{v}{t+1}$ is even, then $k - (t+1)\lambda_1 + t\lambda_2$ is a square;*

*(2) (Corollary 2.2 [20]) if $\alpha = \frac{v}{t+1}$ is odd, then $k - \lambda_2$ is a square.*

*Proof 1.* Let $S = \{a_1, a_2, \dots, a_k\}$ be a base set of a $\lambda_2$-equivalent $(v, k, [\lambda_1, \lambda_2]; t)$-design. Define

$$\theta(x) \equiv x^{a_1} + x^{a_2} + \cdots + x^{a_k} \pmod{x^v - 1}.$$

By Theorem 3.5, we obtain:

$$\begin{aligned} & \theta(x)\theta(x^{-1}) \\ \equiv\ & k + \lambda_1(x^1 + x^2 + \cdots + x^{v-1}) + \\ & +(\lambda_2 - \lambda_1)(x^{\alpha} + x^{2\alpha} + \cdots + x^{t\alpha}) \pmod{x^v - 1}. \end{aligned}$$

Since $v$ is even, $(-1)^v = 1$. Thus, setting $x = -1$, we have:

$$\begin{aligned} & \theta^2(-1) \\ =\ & k + \lambda_1\left[(-1+1) + (-1+1) + \cdots + (-1+1) - 1\right] + \\ & +(\lambda_2 - \lambda_1)\left[(-1)^{\alpha} + (-1)^{2\alpha} + \cdots + (-1)^{t\alpha}\right] \\ =\ & k - \lambda_1 + (\lambda_2 - \lambda_1)\left[(-1)^{\alpha} + (-1)^{2\alpha} + \cdots + (-1)^{t\alpha}\right]. \end{aligned}$$

Hence, if $\alpha$ is even, then

$$\theta^2(-1) = k - \lambda_1 + t(\lambda_2 - \lambda_1) = k - (t+1)\lambda_1 + t\lambda_2$$

must be a square.

If $\alpha$ is odd, then $t$ is odd since $v = (t+1)\alpha$ and $v$ is even. Thus,

$$\theta^2(-1) = k - \lambda_1 - (\lambda_2 - \lambda_1) = k - \lambda_2$$

must be a square. □

*Proof 2.* Let $A$ be the incidence matrix of a $\lambda_2$-equivalent $(v, k, [\lambda_1, \lambda_2]; t)$-design and $B = AA^T$, then by Theorem 3.5, we have that $B - (k - \lambda_2)I$ is the Kronecker product of the $\alpha \times \alpha$ matrix

$$M = \begin{bmatrix} \lambda_2 & \lambda_1 & \cdots & \lambda_1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_1 \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_1 & \lambda_1 & \cdots & \lambda_2 \end{bmatrix}$$

and the $(t+1)\times(t+1)$ matrix $J$. Therefore, by Lemma 2.41, Lemma 2.42 and Lemma 5.3, all eigenvalues of the matrix $B-(k-\lambda_2)I$ are 0 ($t\alpha$-multiplicity), $(t+1)(\lambda_2-\lambda_1)$ ($(\alpha-1)$-multiplicity) and $(t+1)\left[\lambda_2+(\alpha-1)\lambda_1\right]$. Thus, by Lemma 2.40, all eigenvalues of the matrix $B=[B-(k-\lambda_2)I]+(k-\lambda_2)I$ are $0+(k-\lambda_2)=k-\lambda_2$ ($t\alpha$-multiplicity), $(t+1)(\lambda_2-\lambda_1)+(k-\lambda_2)= = k-(t+1)\lambda_1+t\lambda_2$ ($(\alpha-1)$-multiplicity) and $(t+1)\left[\lambda_2+(\alpha-1)\lambda_1\right]+(k-\lambda_2)=\left[v-(t+1)\right]\lambda_1+t\lambda_2+k=k(k-1)+k=k^2$. Since the determinant of a square matrix equals the product of all its eigenvalues, we obtain:

$$det(B)=(k-\lambda_2)^{t\alpha}\left[k-(t+1)\lambda_1+t\lambda_2\right]^{\alpha-1}k^2.$$

Because $B=AA^T$, $det(B)$ must be a square. From the expression of $det(B)$, if $\alpha=\frac{v}{t+1}$ is even, then $\left[k-(t+1)\lambda_1+t\lambda_2\right]^{\alpha-1}$ must be a square since $(k-\lambda_2)^{t\alpha}$ is a square. Because $\alpha-1$ is odd, we have that $k-(t+1)\lambda_1+t\lambda_2$ is a square. If $\alpha=\frac{v}{t+1}$ is odd, then $\left[k-(t+1)\lambda_1+t\lambda_2\right]^{\alpha-1}$ is a square. Thus, $(k-\lambda_2)^{t\alpha}$ must be a square. Since $v=(t+1)\alpha$ is even, $t$ is odd. So is $t\alpha$ since $\alpha$ is odd. Therefore, $k-\lambda_2$ is a square. □

Note. Let $m_0$ be the number of even elements in the base set $S$ and $m_1$ the number of odd elements in $S$. Since $\theta^2(-1)=(m_0-m_1)^2$, we have that $k-(t+1)\lambda_1+t\lambda_2=(m_0-m_1)^2$ if $\alpha$ is even and $k-\lambda_2=(m_0-m_1)^2$ if $\alpha$ is odd.

We can extend the above result to doubly equivalent designs:

**Theorem 5.5.** *Assume that $v$ is even and there exists a $\lambda_2$- and $\lambda_3$-equivalent $(v,k,[\lambda_1,\lambda_2,\lambda_3];r,s,t)$-design. Let $\alpha=\frac{v}{s+1}$ and $\beta=\frac{v}{t+1}$. Then at least one of $\alpha$ and $\beta$ is even and we have:*

*(1) if $\alpha$ and $\beta$ are both even, then $k-(s+t+1)\lambda_1+s\lambda_2+t\lambda_3$ is a square;*

*(2) if $\alpha$ is even and $\beta$ is odd, then $k-\lambda_3+s(\lambda_2-\lambda_1)$ is a square;*

*(3) if $\alpha$ is odd and $\beta$ is even, then $k-\lambda_2+t(\lambda_3-\lambda_1)$ is a square.*

Note. In each of the three cases of Theorem 5.5, the square equals $(m_0-m_1)^2$, where $m_0$ and $m_1$ are defined in the Note after Theorem 5.4.

*Proof.* Let $S=\{a_1,a_2,\dots,a_k\}$ be a base set of a $\lambda_2$- and $\lambda_3$-equivalent $(v,k,[\lambda_1,\lambda_2,\lambda_3];r,s,t)$-design. Since $v=(s+1)(t+1)d$ is even, so at least one of $\alpha$ and $\beta$ is even. Define

$$\theta(x)\equiv x^{a_1}+x^{a_2}+\cdots+x^{a_k} \pmod{x^v-1}.$$

By Theorem 3.5, we obtain:

$$\begin{aligned}&\theta(x)\theta(x^{-1})\\ \equiv\ & k+\lambda_1(x^1+x^2+\cdots+x^{v-1})+\\ &+(\lambda_2-\lambda_1)(x^{\alpha}+x^{2\alpha}+\cdots+x^{s\alpha})+\\ &+(\lambda_3-\lambda_1)(x^{\beta}+x^{2\beta}+\cdots+x^{t\beta}) \pmod{x^v-1}.\end{aligned}$$

The rest discussion is similar to Theorem 5.4. □

## 5.3 Constructions of New Difference Sets From Old

The following Lemma is just a special case of Theorem 2.16.

**Lemma 5.6.** *If $S=\{a_1,a_2,a_3,\dots,a_k\}$ mod $v$ is a $(v,k,[\lambda_1,\lambda_2,\dots,\lambda_m])$--difference set, then $-S=\{-a_1,-a_2,-a_3,\dots,-a_k\}$ mod $v$ is also a $(v,k,[\lambda_1,\lambda_2,\dots,\lambda_m])$-difference set.*

For a 0-equivalent $(v, k, [\dots, 0]; t)$-design, recall that $\boldsymbol{u}$ is the number of parallel classes from which the point 0 is missing, where $u$ is a nonnegative integer. For a 0-equivalent $(v, k, [\dots, 0]; t)$-difference set $S$, $\boldsymbol{u}$ is defined to be the u in the design generated by $S$.

We can restate Theorem 3.32 into:

**Theorem 5.7.** *For a 0-equivalent $(v, k, [\lambda, 0]: t)$-difference set $S$ with $u > 1$, the set $\{0, 1, \dots, \alpha - 1\} \setminus [-S \pmod{\alpha}]$ is an $(\alpha, u, \mu)$-difference set, where $u = \alpha - k$, $\mu = \frac{(\alpha-k)(\alpha-k-1)}{\alpha-1}$. In addition, $u = k - \lambda(t+1) + \mu$.*

*Proof.* Let $S = \{a_1, a_2, a_3, \dots, a_k\}$ mod $v$. Then all lines containing the point 0 are: $[-a_1], [-a_2], [-a_3], \dots, [-a_k]$ mod $v$. Hence all parallel classes containing the point 0 are: $\langle -a_1\rangle, \langle -a_2\rangle, \langle -a_3\rangle, \dots, \langle -a_k\rangle$ mod $\alpha$. Therefore, the set $\{i_1, i_2, \dots, i_u\}$ defined in Theorem 3.32 is: $\{0, 1, \dots, \alpha - 1\} \setminus [-S \pmod{\alpha}]$. This completes the proof. □

**Corollary 5.8.** *For a 0-equivalent $(v, k, [\lambda, 0]; t)$-difference set $S$ with $u > 1$, the set $\{0, 1, \dots, \alpha - 1\} \setminus [S \pmod{\alpha}]$ is an $(\alpha, u, \mu)$-difference set, where $u = \alpha - k$, $\mu = \frac{(\alpha-k)(\alpha-k-1)}{\alpha-1}$. In addition, $u = k - \lambda(t+1) + \mu$.*

*Proof.* We have

$$\{0, 1, \dots, \alpha - 1\} \setminus [-S \pmod{\alpha}] = -\{\{0, 1, \dots, \alpha - 1\} \setminus [S \pmod{\alpha}]\} \pmod{\alpha}.$$

By Theorem 5.7, $\{0, 1, \dots, \alpha-1\} \setminus [-S \pmod{\alpha}]$ is an $(\alpha, u, \mu)$-difference set. Therefore, by Lemma 5.6,

$$\{0, 1, \dots, \alpha - 1\} \setminus [S \pmod{\alpha}] = -\{\{0, 1, \dots, \alpha - 1\} \setminus [-S \pmod{\alpha}]\} \pmod{\alpha}$$

is also an $(\alpha, u, \mu)$-difference set. □

**Example 5.9.** $\{0,1,2,4,6,11,12,20,23\}$ *mod* 26 *in Example 3.33 is a* 0*-equivalent* $(26,9,[3,0];1)$*-difference set with* $\alpha = 13$ *and* $u = 4$. *By Theorem 5.7,* $\{4,5,8,10\}$, *or* $\{0,1,4,6\}$, *is a* $(13,4,1)$*-difference set. By Corollary 5.8,* $\{3,5,8,9\}$, *or* $\{0,2,5,6\}$, *is also a* $(13,4,1)$*-difference set.*

Other 0-equivalent $(v,k,[\lambda,0];t)$-difference sets with $u > 1$: $\{0,1,9,11\}$ (mod 14) is a $(14,4,[1,0];1)$-difference set with $u = 3$: $\{0,1,2,4,6,7,16,17,24,26,29,31,32,35,36,40\}$ mod 42 is a $(42, 16, [6, 0]; 1)$-difference set with $u = 5$.

Similarly to the singly equivalent case, we can restate Theorem 4.10 into:

**Theorem 5.10.** *For a* $\lambda_2$*- and* 0*-equivalent* $(v,k,[\lambda_1,\lambda_2,0];r,s,t)$*-design* $D$, *let* $\alpha = \frac{v}{s+1}$ *and* $\beta = \frac{v}{t+1}$. *If* $d = \frac{v}{(s+1)(t+1)} > 1$, *then* $u > 1$ *and the set* $\{0,1,\ldots,\alpha-1\}\setminus[-S \pmod{\alpha}]$ *is a* $\mu_2$*-equivalent* $(\beta,u,[\mu_1,\mu_2];s)$*-difference set and* $u = k-\lambda_1(t+1)+\mu_1$, $u = k-\lambda_1 t-\lambda_2+\mu_2$. *Thus we have* $\lambda_1-\lambda_2 = \mu_1-\mu_2$ *(when* $\lambda_1 < \lambda_2$, *we may write* $\lambda_2-\lambda_1 = \mu_2-\mu_1$*).*

We also have

**Corollary 5.11.** *For a* $\lambda_2$*- and* 0*-equivalent* $(v,k,[\lambda_1,\lambda_2,0];r,s,t)$*-design* $D$, *let* $\alpha = \frac{v}{s+1}$ *and* $\beta = \frac{v}{t+1}$. *If* $d = \frac{v}{(s+1)(t+1)} > 1$, *then* $u > 1$ *and the set* $\{0,1,\ldots,\alpha-1\}\setminus[S \pmod{\alpha}]$ *is a* $\mu_2$*-equivalent* $(\beta,u,[\mu_1,\mu_2];s)$*-difference set and* $u = k-\lambda_1(t+1)+\mu_1$, $u = k-\lambda_1 t-\lambda_2+\mu_2$. *Thus we have* $\lambda_1-\lambda_2 = \mu_1-\mu_2$ *(when* $\lambda_1 < \lambda_2$, *we may write* $\lambda_2-\lambda_1 = \mu_2-\mu_1$*).*

The following Theorem was given as Theorem 3.2 in A. T. Butson [7] in 1963 and as Corollary 2.1.2 in Elliott and Butson [12] in 1966. In fact the result of Elliot and Butson [12] is slightly stronger than this since it applies to arbitrary groups. Ryser [35] in 1973 and Wei, Gao and Yang [37] in 1993 obtained weaker versions of this Theorem, but did not mention that what they had obtained was just a special case of the results in [7] and [12]. Elliot and Butson's proof [12] is very elegant, however we provide two alternative proofs and the first proof allows the generalization given in Theorem 5.14.

**Theorem 5.12.** *For a 0-equivalent $(v, k, [\lambda, 0]: t)$-difference set $S$, $S \pmod{\alpha}$ is an $(\alpha, k, \lambda(t+1))$-difference set.*

*Proof 1.* Let $S=\{a_1, a_2, \ldots, a_k\}$ be a 0-equivalent $(v, k, [\lambda, 0]: t)$-difference set. By Theorem 3.5, we have:

$$a_i \not\equiv a_j \pmod{\alpha}. \ \forall a_i, a_j \in S \ (i \neq j).$$

It follows that we have that the size of $S \pmod{\alpha}$ is $k$. Let $D$ and $D'$ be the design generated by $S$ or $S \pmod{\alpha}$ respectively. After taking mod $\alpha$, all lines in a parallel class in $D$ coincide. A line $l$ in $D$ meets every line in a parallel class of $D$ not containing $l$ in $\lambda$ points. So, a line in $D'$ meets every other line of $D'$ in $\lambda(t+1)$ points. Therefore, by Theorem 2.8, $S \pmod{\alpha}$ is an $(\alpha, k, \lambda(t+1))$-difference set. □

*Proof 2.* Let $S=\{a_1, a_2, \ldots, a_k\}$ be a 0-equivalent $(v, k, [\lambda, 0]: t)$-difference set. Define

$$\theta(x) \equiv x^{a_1} + x^{a_2} + \cdots + x^{a_k} \pmod{x^v - 1}.$$

By Theorem 3.5, we obtain:

$$\begin{aligned} & \theta(x)\theta(x^{-1}) \\ \equiv\ & k + \lambda(x^1 + x^2 + \cdots + x^{v-1}) - \\ & -\lambda(x^\alpha + x^{2\alpha} + \cdots + x^{t\alpha}) \pmod{x^v - 1}. \end{aligned}$$

Thus,

$$\begin{aligned}&\theta(x)\theta(x^{-1})\\ \equiv\ & k+\lambda(t+1)(x^1+x^2+\cdots+x^{\alpha-1}) \pmod{x^\alpha-1}.\end{aligned}$$

Since

$$a_i \not\equiv a_j \pmod{\alpha}, \forall a_i, a_j \in S\ (i \neq j),$$

we have that $S \pmod{\alpha}$ is an $(\alpha, k, \lambda(t+1))$-difference set. □

**Example 5.13.** *From Example 5.9. by Theorem 3.5.* $\{0, 1, 2, 4, 6, 7, 10, 11, 12\}$ *mod* 13 *is a* $(13, 9, 6)$*-difference set.*

We can extend Theorem 5.12 to the doubly equivalent case.

**Theorem 5.14.** *For a $\lambda_2$- and 0-equivalent $(v, k, [\lambda_1, \lambda_2, 0]: r, s, t)$-difference set $S$, let $\alpha = \frac{v}{s+1}$, $\beta = \frac{v}{t+1}$ and $d = (\alpha, \beta)$. If $d = 1$, then $S \pmod{\beta}$ is a $(\beta, k, \lambda_1 t + \lambda_2)$-difference set; if $d > 1$, then $S \pmod{\beta}$ is a $(\lambda_1 t + \lambda_2)$--equivalent $(\beta, k, [\lambda_1(t+1), \lambda_1 t + \lambda_2])$-difference set.*

*Proof.* As in Proof 1 of Theorem 5.12, the size of $S \pmod{\beta}$ is $k$. Let $D$ and $D'$ be the design generated by $S$ or $S \pmod{\beta}$ respectively. $D$ has $d$ super classes:

$$\hat{0}, \hat{1}, \ldots, \widehat{d-1}.$$

If parallel classes $\langle i\rangle$ and $\langle j\rangle$ are in the same super class, then every line in $\langle i\rangle$ meets one line in $\langle j\rangle$ in $\lambda_2$ points while it meets every other line in $\langle j\rangle$ in $\lambda_1$ points. If parallel classes $\langle i\rangle$ and $\langle j\rangle$ are in different super classes, then every line in $\langle i\rangle$ meets every line in $\langle j\rangle$ in $\lambda_1$ points. If $d = 1$, then $D$ just has one super class. So, similarly to Proof 1 of Theorem 5.12, we have that a line in $D'$ meets every other line of $D'$ in $\lambda_1 t + \lambda_2$ points. Therefore, $S$ (mod $\beta$) is an $(\alpha, k, \lambda_1 t + \lambda_2)$-difference set. If $d > 1$, then similarly we have that $S$ (mod $\beta$) is a $(\beta, k, [\lambda_1(t+1), \lambda_1 t + \lambda_2])$-difference set. Since $\langle i \rangle$ and $\langle j \rangle$ are in the same super class if and only if $i - j \equiv 0$ (mod $d$), by Theorem 3.5, $S$ (mod $\beta$) is $(\lambda_1 t + \lambda_2)$-equivalent. □

**Example 5.15.** $S = \{0, 1, 2, 4, 12, 17\}$ *mod* 21 *in Example 4.1 is a* 1- *and* 0-*equivalent* $(21, 6, [2, 1, 0]; 12, 6, 2)$-*difference set with* $d = 1$. *By Theorem 5.14, since* $\beta = \frac{v}{t+1} = 7$, $S$ *(mod 7)* $= \{0, 1, 2, 3, 4, 5\}$ *is a* $(7, 6, 5)$-*difference set.*

# Appendix A

# 0-equivalent Designs with $u = 1$

| $(v, k, [1, 0]; t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (8, 3, [1, 0]; 1) | Yes | $\{0, 1, 3\}$ |
| (15, 4, [1, 0]; 2) | Yes | $\{0, 1, 3, 7\}$ |
| (24, 5, [1, 0]; 3) | Yes | $\{0, 1, 3, 11, 20\}$ |
| (35, 6, [1, 0]; 4) | No | $\exists$ non 0-equivalent designs only |
| (48, 7, [1, 0]; 5) | Yes | $\{0, 1, 3, 15, 20, 38, 42\}$ |
| (63, 8, [1, 0]; 6) | Yes | $\{0, 1, 3, 7, 15, 20, 31, 41\}$ |
| (80, 9, [1, 0]; 7) | Yes | $\{0, 1, 3, 9, 22, 27, 34, 38, 66\}$ |
| (99, 10, [1, 0]; 8) | No | $\nexists$ non 0-equivalent designs |
| (120, 11, [1, 0]; 9) | Yes | $\{0, 1, 3, 20, 31, 35, 45, 53, 58, 74, 114\}$ |
| (143, 12, [1, 0]; 10) | No | $\nexists$ non 0-equivalent designs of the form $\{0, 1, a_3, \dots\}$ either |

Table 1. Case of $(v, k, [1, 0]; t)$

| $(v, k, [2, 0]; t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (12, 5, [2, 0]; 1) | Yes | $\{0, 1, 2, 4, 9\}$ |
| (24, 7, [2, 0]; 2) | Yes | $\{0, 1, 2, 5, 7, 11, 14\}$ |
| (40, 9, [2, 0]; 3) | Yes | $\{0, 1, 2, 5, 8, 13, 17, 19, 26\}$ |
| (60, 11, [2, 0]; 4) | Yes | $\{0, 1, 3, 6, 10, 14, 16, 21, 35, 43, 44\}$ |
| (84, 13, [2, 0]; 5) | Yes | $\{0, 1, 2, 4, 12, 20, 25, 31, 35, 38, 47, 64, 79\}$ |

Table 2. Case of $(v, k, [2, 0]; t)$

| $(v, k, [3, 0]; t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (16, 7, [3, 0]; 1) | Yes | $\{0, 1, 2, 4, 5, 7, 11\}$ |
| (33, 10, [3, 0]; 2) | No | $\nexists$ non 0-equivalent designs of the form $\{0, 1, a_3, \dots\}$ either |
| (56, 13, [3, 0]; 3) | Yes | $\{0, 1, 2, 4, 8, 9, 13, 19, 21, 24, 31, 34, 40\}$ |
| (85, 16, [3, 0]; 4) | | |

Table 3. Case of $(v, k, [3, 0]; t)$

| $(v, k, [4, 0]; t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (20, 9, [4, 0]; 1) | Yes | $\{0, 1, 2, 3, 5, 9, 14, 16, 17\}$ |
| (42, 13, [4, 0]; 2) | Yes | $\{0, 1, 2, 4, 5, 12, 20, 22, 25, 31, 35, 37, 38\}$ |
| (72, 17, [4, 0]; 3) | | |

Table 4. Case of $(v, k, [4, 0]; t)$

| $(v, k, [5, 0]; t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (24, 11, [5, 0]; 1) | Yes | $\{0, 1, 2, 3, 5, 7, 10, 11, 18, 20, 21\}$ |
| (51, 16, [5, 0]; 2) | Yes | $\{0, 1, 2, 3, 5, 7, 11, 12, 15, 23, 25, 26, 31, 38, 44, 47\}$ |
| (88, 21, [5, 0]; 3) | | |

Table 5. Case of $(v, k, [5, 0]: t)$

| $(v, k, [6, 0]: t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (28, 13, [6, 0]: 1) | Yes | $\{0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 19, 21, 24\}$ |
| (60, 19, [6, 0]: 2) | | |

Table 6. Case of $(v, k, [6, 0]: t)$

| $(v, k, [7, 0]: t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (32, 15, [7, 0]: 1) | No | $\nexists$ non 0-equivalent designs of the form $\{0, 1, a_3, \ldots\}$ either |
| (69, 22, [7, 0]: 2) | | |

Table 7. Case of $(v, k, [7, 0]: t)$

# Appendix B

# Tables of $\lambda$-equivalent Designs

| $(v, k, [\lambda_1, \lambda_2]; t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (8, 5, [3, 2]; 1) | Yes | $\{0, 1, 2, 3, 5\}$ |
| (15, 7, 3) | Yes | $\{0, 1, 2, 4, 5, 8, 10\}$ |
| (24, 9, [3, 4]; 3) | Yes | $\{0, 1, 2, 3, 6, 11, 14, 18, 20\}$ |
| (35, 11, [3, 5]; 4) | No | $\nexists$ non 5-equivalent designs of the form $\{0, 1, a_3, \dots\}$ either |

Table 1. $(t+1)$-equivalent $(v, k+t+1, [3, t+1]: t)$-difference sets corresponding to $(v, k, [1, 0]: t)$-difference sets with $u = 1$

| $(v, k, [\lambda_1, \lambda_2]; t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (12, 7, [4, 2]; 1) | Yes | $\{0, 1, 2, 3, 5, 6, 10\}$ |
| (24, 10, [4, 3]; 2) | Yes | $\{0, 1, 2, 3, 5, 6, 11, 13, 17, 20\}$ |
| (40, 13, 4) | Yes | $\{0, 1, 2, 4, 5, 8, 13, 17, 19, 24, 26, 34\}$ |

Table 2. $(t+1)$-equivalent $(v, k+t+1, [4, t+1]; t)$-difference sets corresponding to $(v, k, [2, 0]; t)$-difference sets with $u = 1$

| $(v, k, [3, 0]; t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (16, 9, [5, 2]; 1) | Yes | $\{0, 1, 2, 3, 4, 6, 7, 11, 13\}$ |
| (33, 13, [5, 3]; 2) | No | $\nexists$ non 3-equivalent designs of the form $\{0, 1, a_3, \dots\}$ either |

Table 3. $(t+1)$-equivalent $(v, k+t+1, [5, t+1]; t)$-difference sets corresponding to $(v, k, [3, 0]; t)$-difference sets with $u = 1$

| $(v, k, [4, 0]; t)$ | $\exists$ | Example/Remark |
|---|---|---|
| (20, 11, [6, 2]; 1) | Yes | $\{0, 1, 2, 3, 5, 6, 7, 9, 14, 15, 18\}$ |
| (42, 16, [6, 3]; 2) | Yes | $\{0, 1, 2, 3, 5, 6, 13, 14, 21, 23, 26, 28, 32, 36, 38, 39\}$ |

Table 4. $(t+1)$-equivalent $(v, k+t+1, [6, t+1]; t)$-difference sets corresponding to $(v, k, [4, 0]; t)$-difference sets with $u = 1$

# Appendix C

# A $C^{++}$ program to search $(v, k, [\lambda_1, \lambda_2])$-difference sets

```
//-----------------------------------------------------------------------------
// This program reads values of v, k, l_1 and l_2(l_1>l_2) from the key board,
// finds all (v, k, [l_1, l_2])-difference sets {0, 1, a_3, ...} and prints
// them out with the differences which appear l_2 times.
//-----------------------------------------------------------------------------


#include <iostream.h>
#include <fstream.h>
#include <vector>
#include <algorithm>

void Check(ostream & out, vector<int> set, vector<int> num, int v, int
k, int l1, int l2, int indx, char & flag, bool OK);

void Findout(ostream & out, vector<int> set, vector<int> num, int v,
int k, int l1, int l2, int indx, char flag, bool OK);

int main()
{
   ofstream fout;        // open an input stream to the input file
   fout.open("DS2N.txt");// establish connection

   vector<int> theVec;  //set of integers to check whether is a dif set
```

```
   vector<int> num;       //num holds the number of times each dif appears

   char flag='A';         //'A' means that difference sets have not been found
                          //before, otherwise flag='B'
   bool OK=true;          //OK is true if the set is a dif set otherwise is false

   cout<<"Input v, k, l_1 and l_2 (l_1>l_2):\n";
   int v, k, l1, l2;      //v is mod, k is the set size, l1 and l2 are #'s
                          //of times a residue appears as a difference.
   cin>>v>>k>>l1>>l2;
   if (l_1<=l_2)
      {
         cout<<"l_1 should be bigger than l_2!\n";
         cout<<"Input v, k, l_1 and l_2 (l_1>l_2) again:\n";
         int v, k, l1, l2;
      }
   int indx=k-1;
   Findout(fout,theVec,num,v,k,l1,l2,indx,flag,OK);
   fout.close();
   cout<<"\n("<<v<<", "<<k<<", ["<<l1<<", "<<l2<<"])-difference sets have been
done!\n";
   return 0;
}

//----------------------------------------------------------------------
//This function inserts dif's and print the data of the set if it is a dif set
//----------------------------------------------------------------------
void Check(ostream & out, vector<int> set, vector<int> num, int v, int
k, int l1, int l2, int indx, char & flag, bool OK)
{
   int r=0;        // r is # of times l1 appears
   int s=0;        // s is # of times l2 appears

   for (int i=0; i<v; i++)
      {
         num.push_back(0);
      }

   for (int i=0; i<k-1; i++) //calculate all the dif's in the set and update
                             //dif's and num
      {
      for (int j=i+1; j<=k-1; j++)
           {
              int dif1=set[i]-set[j];
              dif1+=v;               //since dif1 was negative
              num[dif1]++;
              if (num[dif1]>l1)
                 {
                   OK=false;
                   indx=i;
                 }
              else
                 {
                   int dif2=set[j]-set[i];
                   num[dif2]++;
                   if (num[dif2]>l1)
```

```
                    {
                     OK=false;
                     indx=i;
                    }
               }
            if (!OK)
               break;
         }
      if (!OK)
         break;
   }

   for (int i=1; i<v; i++)      //If it appears l1 or l2 times, update r or
                                //s respectively; otherwise set OK to be false
   {
      if (!OK)
         break;
      if (num[i]==l1)
         r++;
      else if (num[i]==l2)
         s++;
      else
         {
          OK=false;
          break;
         }
   }

   OK=(OK && (r+s==v-1) && (k*(k-1)==r*l1+s*l2));//These 2 equalities
                                                   //should hold
   if (OK)        //If is a dif set
   {
    if (flag=='A')    //If we have not found difference set before,
                      //print the title
      {
          out<<"The ("<<v<<", "<<k<<", ["<<l1<<", "
         <<l2<<"])-difference sets {0, 1, ...}:\n\n";
          flag='B'; //set the flag to be 'B'
      }
      for(int i=0; i<k; i++) //print out the set
         out<<"  "<<set[i];
      out<<"; r="<<r<<", s="<<s<<" \n\t\t differences:";
      for(int i=1; i<v; i++)
       {
           if (num[i]==l2) //If a dif appears l2 times,
              out<<"   "<<i<<"("<<num[i]<<"),";//then print it out
       }
      out<<endl;
   }
}

//-----------------------------------------------------------------------
//This function calls the function "Check" to search all the
//(v, k, [l_1, l_2])-difference sets, starting with {0, 1,..., k-1}
//-----------------------------------------------------------------------
void Findout(ostream & out, vector<int> set, vector<int> num, int v,
int k, int l1, int l2, int indx, char flag, bool OK)
```

```
{
   int fstEle=0;
   bool ready=false;
   for (int i=0; i<k; i++) //initialize the set to {0, 1,..., k-1}
      {
         set.push_back(i);
      }
   out<<endl;

   while (set[2]<v-k+2)   //we start with {0, 1, 2, ..., k-1} and check till
     {                    //{0, 1, v-k+2,..., v-1} (exclude these 2 sets).
      for (int i=0; i<k-2; i++) //start with the last element of the set
        {
          if (set[k-i-1]<v-i-1)
             {
               if (ready==false)
                  {
                    set[k-i-1]++;
                    for(int j=i-1; j>=0; j--) //set elements after the (k-i-1)th
                                    //position to be 1 plus the element before
                       set[k-j-1]=set[k-j-2]+1;
                  }
               ready=false;
               Check(out, set, num, v, k, l1, l2, indx, flag, OK);
               if (indx<k-1)
                  for (int m=indx; m>=2; m--)
                     {
                       if (set[m]<v+m-k)
                          {
                            set[m]++;
                            for(int n=k-m-1; n>0; n--)
                               set[m+n]=set[m]+n;
                            indx=k-1;
                            ready=true;
                            break;
                          }
                     }
                  break;
             }
        }
      if (set[2]!=fstEle)
        {
          fstEle=set[2];
          cout<<fstEle<<" ";
        }
     }
   if (flag=='A') //if no difference sets have been found
     {
       out<<"No ("<<v<<", "<<k<<", ["<<l1<<", "<<l2<<"])-difference sets
{0, 1, ...} exist!\n\n";
     }
   out<<"\nEnd of processing.\n\n\n";
}
```

# Bibliography


[1] K. T. Arasu, J. Davis, D. Jungnickel, and A. Pott, *Some Non-Existence Results on Divisible Difference Sets*, Combinatorica 11 (1991), 1-8.

[2] K. T. Arasu, D. Jungnickel, S. L. Ma and A. Pott, *Relative Difference Sets with $n = 2$*, Discrete Math. 147 (1995), 1-17.

[3] L. M. Batten and A. Beutelspacher, *The Theory of Finite Linear Spaces*, Cambridge University Press, Cambridge, 1993.

[4] L. M. Batten, *Combinatorics of Finite Geometries*, 2nd edition, Cambridge University Press, Cambridge, 1997.

[5] L. M. Blumenthal, *A Modern View of Geometry*, Dover Publications, New York, 1961.

[6] R. C. Bose, *An Affine Analogue of Singer's Theorem*, J. Ind. Math. Soc., 6 (1942), 1-15.

[7] A. T. Butson, *Relations Among Generalized Hadamard Matrices*, Canad. J. Math., 15 (1963), 42-48.

[8] Y. Q. Chen, D. K. Ray-Chaudhuri and Q. Xiang, *Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings II*, J. Combin. Theory A 76 (1996), 179-196.

[9] C. J. Colbourn and J. H. Dinitz (editors), *The CRC Handbook of Combinatorial Designs*, CRC Press, Inc., Boca Raton, 1996.

[10] H. S. M. Coxeter, *The Real Projective Plane*, 2nd edition, Cambridge University Press, Cambridge, 1960.

[11] H. S. M. Coxeter, *Introduction to Geometry*, 2nd edition, John Wiley & Sons, New York, 1969.

[12] J. E. H. Elliott and A. T. Butson, *Relative Difference Sets*, Illinois J. Math. 10 (1966), 517-531.

[13] M. Hall, Jr, *Combinatorial Theory*, 2nd edition, John Wiley & Sons, New York, 1986.

[14] H. Hanani, *Balanced Incomplete Block Designs and Related Designs*, Discrete Math. 11 (1975), 255-369.

[15] A. J. Hoffman, *Cyclic Affine Planes*, Can. J. Math. 78 (1952), 295-301.

[16] K. Hoffman and R. Kunze, *Linear Algebra*, 2nd edition, Prentice-Hall, Inc., Englewood Cliffs, 1971.

[17] N. Jacobson, *Basic Algebra I*, 2nd edition. W. H. Freeman and Company, New York, 1985.

[18] D. Jungnickel, *On Automorphism Groups of Divisible Designs*, Can. J. Math. XXXIV 2 (1982), 257-297.

[19] D. Jungnickel, *A New Family of Relative Difference Sets*, J. Combin. Theory A 52 (1989), 301-303.

[20] H. P. Ko and D. K. Ray-Chaudhuri, *Intersection Theorems for Group Divisible Difference Sets*, Discrete Math. 39 (1982), 37-58.

[21] C. Koukouvinos and A. L. Whiteman, *Near Difference Sets*, Bull. Inst. Combin. Appl. 15 (1995), 57-67.

[22] C. Koukouvinos and A. L. Whiteman, *Relative Difference Sets*, J. Combin. Theory A 74 (1996), 153-157.

[23] Clement W. H. Lam, *On Relative Difference Sets*, Proceedings of the Seventh Manitoba Conference on Numerical Mathematics and Computing, (Univ. Manitoba, Winnipeg, Man., 1977), Congress. Numer., Utilitas Math., Winnipeg, Man., XX (1978), 445-474.

[24] P. A. Leonard, *Cyclic Relative Difference Sets*, Amer. Math. Monthly 93 (1986), no. 2, 134-157.

[25] S. L. Ma, *Partial Difference Sets*, Discrete Math. 52 (1984), 75-89.

[26] S. L. Ma, *On Subsets of Partial Difference Sets*, Discrete Math. 125 (1994), 263-272.

[27] S. L. Ma, *A Survey of Partial Difference Sets*, Des. Codes Cryptogr. 4 (1994), 221-261.

[28] N. H. McCoy, *The Theory of Numbers*, The Macmillan Company Collier-Macmillan Limited, London, 1965.

[29] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, New York, 1998.

[30] J. M. Ortega, *Matrix Theory: A Second Course*, Plenum Pless, New York, 1987.

[31] S. E. Payne, *A Nonexistence Theorem for Relative Difference Sets*, Illinois J. Math. 14 (1970), 648-649.

[32] F. Piper, *On Relative Difference Sets and Projective Planes*. Glasgow Math. J. 15 (1974), 150-154.

[33] D. K. Ray-Chaudhuri and Q. Xiang, *Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings*, Des. Codes Cryptogr. 8(1996), 215-227.

[34] H. J. Ryser, *Combinatorial Mathematics*, Quinn & Boden, New Jersey, 1963.

[35] H. J. Ryser, *Variants of Cyclic Difference Sets*, Proc. Amer. Math. Soc. 41 (1973), 45-50.

[36] J. Sumner and A. T. Butson, *Generalized Relative Difference Sets and Partially Balanced Incomplete Block Designs*, J. Combin. Theory A 32 (1982), 370-377.

[37] W. D. Wei, S. Gao and B. Yang *Cyclic Near Difference Sets of Type 1*, Discrete Math. 123 (1993), 151-177.

[38] R. M. Wilson, *An Existence Theory for Pairwise Balanced Designs I*, J. Combin. Theory A 13 (1972), 220-245.

[39] R. M. Wilson, *An Existence Theory for Pairwise Balanced Designs II*, J. Combin. Theory A 13 (1972), 246-273.

[40] R. M. Wilson, *An Existence Theory for Pairwise Balanced Designs III*, J. Combin. Theory A 18 (1975), 71-79.

[41] J. Y. Xu, *A Class of Relative Difference Sets Associated with a Pair of Subgroups* (in Chinese), J. Math. (Wuhan) 12 (1992), 473-478.