Access Balancing in Storage Systems by Labelling Steiner Systems

by

Dylan Lusi

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved November 2021 by the
Graduate Supervisory Committee:

Charles J. Colbourn, Chair
Andrzej Czygrinow
Georgios Fainekos
Andrea Richa

ARIZONA STATE UNIVERSITY

December 2021

ABSTRACT

A storage system requiring file redundancy and on-line repairability can be represented as a Steiner system, a combinatorial design with the property that every t-subset of its points occurs in exactly one of its blocks. Under this representation, files are the points and storage units are the blocks of the Steiner system, or vice-versa. Often, the popularities of the files of such storage systems run the gamut, with some files receiving hardly any attention, and others receiving most of it. For such systems, minimizing the difference in the collective popularity between any two storage units is nontrivial; this is the access balancing problem. With regard to the representative Steiner system, the access balancing problem in its simplest form amounts to constructing either a point or block labelling: an assignment of a set of integer labels (popularity ranks) to the Steiner system's point set or block set, respectively, requiring of the former assignment that the sums of the labelled points of any two blocks differ as little as possible and of the latter that the sums of the labels assigned to the containing blocks of any two distinct points differ as little as possible. The central aim of this dissertation is to supply point and block labellings for Steiner systems of block size greater than three, for which up to this point no attempt has been made. Four major results are given in this connection.

First, motivated by the close connection between the size of the independent sets of a Steiner system and the quality of its labellings, a Steiner triple system of any admissible order is constructed with a pair of disjoint independent sets of maximum cardinality. Second, the spectrum of resolvable Bose triple systems is determined in order to label some Steiner 2-designs with block size four. Third, several kinds of independent sets are used to point-label Steiner 2-designs with block size four. Finally, optimal and close to optimal block labellings are given for an infinite class of

1-rotational resolvable Steiner 2-designs with arbitrarily large block size by exploiting their underlying group-theoretic properties.

Dedicated to the memory of Mervin Stanley Getten

ACKNOWLEDGMENTS

I would like to thank my advisor Charles Colbourn for his guidance, for letting me do a computer science thesis with a heavy dose of mathematics, and for introducing me to design theory. I would also like to thank the three other members of my committee: Andrzej Czygrinow, Georgios Fainekos, and Andrea Richa, for being accommodating, for being excellent instructors, and for kindling my interest in mathematics and theoretical computer science. Finally, I would like to thank my family for all their support, especially my mother and father.

The work of this thesis was largely supported by the National Science Foundation under the grant CCF 1816913 (CJC).

TABLE OF CONTENTS

Page

CHAPTER

CHAPTER Page

Chapter 1

INTRODUCTION

Certain distributed storage systems (DSS) [25, 56], multiserver private information retrieval systems [26], and systems for batch coding [57], each for their own reason, require redundancy of their data items. Thus, they are often represented as t-(v, k, λ) designs. A t-(v, k, λ) *design* is a pair $(X, \mathcal{B})$ where X is a v-set of *points* and $\mathcal{B}$ is a collection k-subsets (*blocks*) such that every t-subset of X is contained in precisely λ blocks. A t-$(v, k, 1)$ design is a *Steiner system*, denoted by $S(t, k, v)$, and a *Steiner triple system* is an $S(2, 3, v)$ (STS(v) for short). Under this representation, data items are associated with points and storage units (e.g., disks or servers) with blocks, so that data is distributed uniformly over the storage units.

Let us focus on one such reason for redundancy in which t-(v, k, λ) designs prominently figure. The storage units of massive data storage systems are especially susceptible to failure. To prevent concomitant data loss, copies of each data item are distributed over multiple storage units; the Google File System and the Hadoop Distributed File System are two examples [14]. In the same vein, the storage systems of transaction processing firms require (1) uninterrupted operation, retrieving customer data even in the event of disk failure and (2) on-line repair of these failed disks. To optimize for (1) and (2), *exact Minimum Bandwidth Regenerating* (MBR) codes [25] and declustered-parity RAIDS (DPRAIDS) have been proposed [12, 34].

An MBR code is composed of an outer MDS code and an inner fractional repetition code (FRC) that provide redundancy and repairability, respectively. Formally, the DSS in which an MBR code operates is an (n, k, d)-DSS, with $k \leq d \leq n$, which consists of

n storage nodes such that a read can be done given access to any k nodes and a failed node can be recovered given access to any d nodes. A *fractional repetition code with repetition degree* ρ for an (n, k, d)-DSS is a collection $\mathcal{C}$ of n d-subsets $V_1, \ldots, V_n$ of a set V, $|V| = v$, with the property that each element of V belongs to exactly ρ distinct sets of the collection. The *rate* of the FRC is $\min_{I \subset [n], |I|=k} |\bigcup_{i \in I} B_i|$. To optimize the rate and guarantee correct repetition and repair, it is required that $|B_i \cap B_j| \leq 1$ whenever $i \neq j$. When $\rho = (v-1)/(d-1)$, such an FRC is an $S(2, d, v)$, where the set of (coded) file chunks V is the set of points and the collection of storage nodes $\{V_1, \ldots, V_n\}$ is the block set of the design.

A *DPRAID*, like a run-of-the-mill RAID ("redundant array of inexpensive disks"), handles disk failure via parity-encoded redundancy, whereby subsets of the stored data (*parity stripes*) are XORed to produce a single-error-correction code. But unlike RAIDS, all disks in a DPRAID collaborate in reconstructing all the data units on a failed disk. For this reason, it is efficacious to model a DPRAID as a t-(v, k, λ) design $(X, \mathcal{B})$, where X is the set of disks in the array and $\mathcal{B}$ is the set of all parity stripes. Then as desired, all disks partake in reconstructing a failed disk, since each disk occurs in the same number of parity stripes.

Myriad papers have been written that exclusively address the redundancy problem, but within this framework, little work has been done on *access balancing* [13]. One may view access balancing as a kind of analogue to load balancing in the domain of popularity. With the latter, the aim is to distribute as evenly as possible a set of jobs over a set of computing units. Similarly, the object of the former is to distribute as evenly as possible access requests over storage units. While it is simple enough to design from the ground up a DSS exclusively optimized for access balancing, it is not so clear how to access-balance a DSS explicitly designed for storage unit failure and repair without modifying its original properties; call this the *constrained access balancing problem*. As we have already seen, such storage systems may be modeled as Steiner systems, and Dau and Milenkovic [22] thus address the constrained access balancing problem by proposing a two-faceted combinatorial model:

1. In one facet, the points (files) of a Steiner system are assigned labels (popularity ranks) so that the sums of the labels assigned to a block (storage unit) are either not too small or large, or too different between any two blocks. Such an assignment is a *point labelling*.
2. In the second facet, the blocks of a Steiner system are assigned labels (popularity ranks) so that the sums of the labels assigned to all blocks containing a point are either not too small or large, or not too different from one another. Such an assignment is a *block labelling*, and this amounts to labelling the points of the dual design of a Steiner system, which also admits application in the design of distributed storage systems [26].

It is within this model that we have operated to produce the work of this thesis.

1.1 Summary of Contributions

The central aim of this thesis is to supply point and block labellings for classes of Steiner systems hitherto unlabelled in the literature; namely, those $S(t, k, v)$ with $t = 2$ and $k > 3$. Indeed, all existing work up to this point in the domain of Steiner systems has focused exclusively on supplying point and block labellings for Steiner triple systems. This is something of a microcosm of the entire body of work in general on Steiner systems, the majority of which centers on Steiner triple systems.

Specifically, our contributions are fourfold. First, motivated by our central aim, we construct Steiner triple systems having a pair of disjoint independent sets whose collective cardinality is as large as possible. The genesis of this work is the close connection between "good" point labellings of Steiner systems and the size of their independent sets. Second, we determine the spectrum of orders of a special class of Steiner triple systems, which we then use to construct $S(2,4,v)$s with quality labellings. Third, we give several point labellings of $S(2,4,v)$s using special block-free collections of points. Fourth, we give several block labellings for a special class of $S(2,k,v)$s for infinitely many $k \geq 3$.

1.2 Organization of the Thesis

In Chapter 2 we supply the reader with definitions of design-theoretic and labelling terms and concepts used throughout our main body of work, and also summarize some key results. In Chapter 3, an offshoot of the close connection between quality point labellings and independent sets of Steiner systems, we construct for all possible orders v an STS(v) with a pair of independent sets of maximum cardinality. In Chapter 4, we determine the spectrum of orders of a special class of Steiner triple systems which are then used to construct a large class of $S(2,4,v)$s with quality labellings. In Chapter 5, we principally construct $S(2,4,v)$s with large and special kinds of independent sets, for which certain point-labelling bounds are derived. In Chapter 6, we provide optimal and close to optimal block labellings of a special class of $S(2,k,v)$s for infinitely many $k \geq 3$. We close the thesis with Chapter 7 by summarizing its main themes and discussing some open problems and future research directions.

Chapter 2

BACKGROUND

Throughout this thesis, we use the notation $[m,n]$ with $m \leq n$ to denote the integral interval from m up to n; i.e., $[m,n] = \{m,\ldots,n\}$.

2.1 Design-theoretic Preliminaries

A *set system* $D = (X, \mathcal{B})$ is a set X (whose elements are *points*), together with a multiset $\mathcal{B}$ of subsets of X (whose elements are *blocks*). We have already mentioned two classes of set systems in the introduction: t-(v,k,λ) designs, and more specifically Steiner systems. The *dual* of an $S(t,k,v)$ $D = (V, \mathcal{B})$ is the set system $D' = (\mathcal{B}, V)$, where the dual point $B \in \mathcal{B}$ is "contained" in the dual block $x \in V$ if $x \in B$ in D. The *replication number* of an $S(t,k,v)$, denoted r, is the number of blocks in which any one of its points occurs. A *Steiner 2-design* is an $S(2,k,v)$. The necessary conditions for the existence of an $S(2,k,v)$ are (1) $vr = bk$ and (2) $r(k-1) = v-1$. An *order* v that satisfies (1) and (2) is *admissible*. The admissible orders of the two main Steiner systems studied in this thesis; namely, STS(v)s and $S(2,4,v)$s, are $v \equiv 1,3 \pmod 6$ and $v \equiv 1,4 \pmod{12}$, respectively. As shown in [37] and [32], these two necessary conditions on v for the case of STS(v)s and $S(2,4,v)$s are also sufficient, so that an STS(v) exists if and only if $v \equiv 1,3 \pmod 6$ and an $S(2,4,v)$ exists if and only if $v \equiv 1,4 \pmod{12}$.

A Steiner 2-design $(V, \mathcal{B})$ is *resolvable* if there exists a partition (*resolution*) of $\mathcal{B}$ into sets called *parallel classes*, each of which partitions V. The study of resolvable block designs is one of the central pursuits of design theory [28]. An $S(2,3,v)$ with a resolution is a *Kirkman triple system* of *order* v, or KTS(v), named after Reverend Kirkman [36]. A KTS(v) exists if and only if $v \equiv 3 \pmod 6$ [42, 46].

A third set-system-based design is also used throughout this thesis. A *group-divisible design of index* λ *and order* v ((K,λ)-GDD) is a triple $(X, \mathcal{G}, \mathcal{A})$, where X is a v-set of points, $\mathcal{G}$ is a partition of X into at least two nonempty subsets (*groups*), and $\mathcal{A}$ is a set of subsets of X (blocks) such that (1) $|A| \in K$ for all $A \in \mathcal{A}$, (2) $|G \cap A| \leq 1$ for all $G \in \mathcal{G}$ and $A \in \mathcal{A}$, and (3) every (unordered) pair of points from distinct groups is contained in exactly λ blocks. If $K = \{k\}$, then the (K,λ)-GDD is simply a (k,λ)-GDD, and if $\lambda = 1$, the (K,λ)-GDD is simply a K-GDD. If $v = t_1u_1 + t_2u_2 + \cdots + t_su_s$ and for $i \in [1,s]$ there are u_i groups of size t_i, then the (K,λ)-GDD is of *type* $t_1^{u_1}t_2^{u_2}\ldots t_s^{u_s}$; this is *exponential notation* for the GDD type. Here is a 3-GDD of type 2^4:

$$\text{groups}: \{1_0,1_1\},\{2_0,2_1\},\{3_0,3_1\},\{4_0,4_1\}$$

$$\text{blocks}: \begin{array}{ccccccc} 1_0 & 2_1 & 3_0 & \qquad & 1_1 & 2_0 & 3_1 \\ 1_0 & 2_0 & 4_1 & & 1_1 & 2_1 & 4_0 \\ 1_0 & 3_1 & 4_0 & & 1_1 & 3_0 & 4_1 \\ 2_0 & 3_0 & 4_0 & & 2_1 & 3_1 & 4_1 \end{array}$$

A k-GDD of type n^k is a *transversal design*, TD(k,n). A staple of design theory is Wilson's fundamental construction (WFC) [62], a recursive construction used to produce GDDs.

Wilson's Fundamental Construction (WFC). Suppose that $(X, \mathcal{G}, \mathcal{A})$ is a GDD (the *master* GDD). Let w be a positive integer (the *weight*) and let I be a set of size w (the *weights*). Suppose that $K \subseteq \{n \in \mathbb{Z} : n \geq 2\}$ and for each $A \in \mathcal{A}$, suppose that there is a GDD $(A \times I, \{\{x\} \times I : x \in A\}, \mathcal{B}_A)$ of type w^u, with $u \geq 1$, such that for each $B \in \mathcal{B}_A$, $|B| \in K$ (such a GDD is an *ingredient* GDD). Define $Y = X \times I$, $\mathcal{H} = \{G \times I : G \in \mathcal{G}\}$, and $\mathcal{B} = \bigcup_{A \in \mathcal{A}} \mathcal{B}_A$. Then $(Y, \mathcal{H}, \mathcal{B})$ is a GDD.

2.2 Labelling Preliminaries

A *point labelling* of a set system $\mathcal{S} = (V, \mathcal{B})$ is a bijection $\mathsf{rk} : V \to [0, |V| - 1]$; in the application investigated by Dau and Milenkovic in [22], this amounts to assigning a popularity rank to each point. A set system together with a point labelling is a *point-labelled set system.* The *reverse* $\overline{\mathsf{rk}}$ of a point labelling rk of $\mathcal{S}$ is the point labelling for which $\overline{\mathsf{rk}}(i) = |V| - 1 - \mathsf{rk}(i)$ for $i \in [0, |V| - 1]$. A *block labelling* of $\mathcal{S}$ is a bijection $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$, and a set system together with a block labelling is a *block-labelled* set system. A point labelling of the dual of a Steiner system can be thought of as a block labelling of the (primal) Steiner system; henceforth, we use the block labelling representation. Given a (point or block) labelling rk of $\mathcal{S}$, let $\mathsf{rk}^{-1}(A)$ denote the preimage of a subset A of labels under rk.

2.2.1 Labelling Metrics for Access Balancing

Given a point-labelled set system $(\mathcal{S} = (V, \mathcal{B}), \mathsf{rk})$, for each $B \in \mathcal{B}$, the *block sum* with respect to rk, denoted $\mathsf{sum}(B, \mathsf{rk})$, is $\sum_{x \in B} \mathsf{rk}(x)$. With access balancing in mind, Dau and Milenkovic propose a collection of metrics:

$$\begin{aligned}\mathsf{MinSum}(\mathcal{S},\mathsf{rk}) &= \min(\mathsf{sum}(B,\mathsf{rk}) : B \in \mathcal{B});\\ \mathsf{MaxSum}(\mathcal{S},\mathsf{rk}) &= \max(\mathsf{sum}(B,\mathsf{rk}) : B \in \mathcal{B});\\ \mathsf{DiffSum}(\mathcal{S},\mathsf{rk}) &= \mathsf{MaxSum}(\mathcal{S},\mathsf{rk}) - \mathsf{MinSum}(\mathcal{S},\mathsf{rk});\ \text{and}\\ \mathsf{RatioSum}(\mathcal{S},\mathsf{rk}) &= \mathsf{MaxSum}(\mathcal{S},\mathsf{rk})/\mathsf{MinSum}(\mathcal{S},\mathsf{rk}).\end{aligned}$$

Under this regime, access balancing is optimized by minimizing the $\mathsf{DiffSum}$ or $\mathsf{RatioSum}$; given their similarity, it is customary to focus on the $\mathsf{DiffSum}$. Maximizing the MinSum and minimizing the MaxSum are also of interest.

Example 1. The blocks (B_0 up to B_{11}) of the unique STS(9) D_9 are given columnwise in the first subtable of Table 2.1. Applying the labelling $\mathsf{rk} : \{\mathrm{a, b, c, d, e, f, g, h, i}\} \to [0, 8]$ given by $\mathsf{rk}(x) = i$, where x is the ith lexicographically least letter, we obtain the point-labelled STS(9) (D_9, rk) given in the second subtable of Table 2.1. Hence,

1. $\mathsf{MinSum}(D_9, \mathsf{rk}) = 3$ (attained by block B_0),
2. $\mathsf{MaxSum}(D_9, \mathsf{rk}) = 21$ (attained by block B_{11}),
3. $\mathsf{DiffSum}(D_9, \mathsf{rk}) = 18$, and
4. $\mathsf{RatioSum}(D_9, \mathsf{rk}) = 7$.

Let $\mathcal{R}_{\mathcal{S}}$ denote the set of all point labellings of $\mathcal{S}$. Making use of the equality $\mathsf{MaxSum}(\mathcal{S},\mathsf{rk}) = k(|V| - 1) - \mathsf{MinSum}(\mathcal{S},\overline{\mathsf{rk}})$, we define

$$\begin{aligned}\mathsf{MinSum}(\mathcal{S}) &= \max(\mathsf{MinSum}(\mathcal{S},\mathsf{rk}) : \mathsf{rk} \in \mathcal{R}_{\mathcal{S}}),\\ \mathsf{MaxSum}(\mathcal{S}) &= \min(\mathsf{MaxSum}(\mathcal{S},\mathsf{rk}) : \mathsf{rk} \in \mathcal{R}_{\mathcal{S}}) = k(|V| - 1) - \mathsf{MinSum}(\mathcal{S}),\ \text{and}\\ \mathsf{DiffSum}(\mathcal{S}) &= \min(\mathsf{DiffSum}(\mathcal{S},\mathsf{rk}) : \mathsf{rk} \in \mathcal{R}_{\mathcal{S}}).\end{aligned}$$

While one can obtain a design-specific labelling with optimal MinSum, MaxSum, or

Table 2.1: The unique STS(9) and the point-labelled STS(9)

B_0	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}
a	a	a	a	b	b	b	c	c	c	d	g
b	d	e	f	d	e	f	d	e	f	e	h
c	g	i	h	i	h	g	h	g	i	f	i

B_0	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}
0	0	0	0	1	1	1	2	2	2	3	6
1	3	4	5	3	4	5	3	4	5	4	7
2	6	8	7	8	7	6	7	6	8	5	8

$\mathsf{DiffSum}$ (over all labellings of that design), it is more interesting to instead derive an optimal labelling over an entire class of set systems. For example, let $\mathcal{D}_{t,k,v}$ denote the set of all $S(t,k,v)$s and $\mathcal{D}'_{t,k,v}$ the set of duals of all $S(t,k,v)$s. Then define

$$\mathsf{MinSum}(t,k,v) = \max(\mathsf{MinSum}(D) : D \in \mathcal{D}_{t,k,v}),$$

$$\mathsf{MinSum}'(t,k,v) = \max(\mathsf{MinSum}(D') : D' \in \mathcal{D}'_{t,k,v}),$$

$$\mathsf{MaxSum}(t,k,v) = \min(\mathsf{MaxSum}(D) : D \in \mathcal{D}_{t,k,v}),$$

$$\mathsf{MaxSum}'(t,k,v) = \min(\mathsf{MaxSum}(D') : D' \in \mathcal{D}'_{t,k,v}),$$

$$\mathsf{DiffSum}(t,k,v) = \min(\mathsf{DiffSum}(D) : D \in \mathcal{D}_{t,k,v}), \text{ and}$$

$$\mathsf{DiffSum}'(t,k,v) = \min(\mathsf{DiffSum}(D') : D' \in \mathcal{D}'_{t,k,v}).$$

Given a block labelling rk of a set system $\mathcal{S} = (V, \mathcal{B})$, for each $x \in V$, the *point sum* with respect to rk, denoted $\mathsf{psum}(x, \mathsf{rk})$, is $\sum_{\{B \in \mathcal{B} : x \in B\}} \mathsf{rk}(B)$. With this, given an $S(t,k,v)$ $D = (V, \mathcal{B})$, we can translate each of the four point-labelling metrics of the dual D' of D into equivalent block labelling metrics of D:

$$\begin{aligned}\mathsf{MinSum}(D,\mathsf{rk}) &= \min(\mathsf{psum}(x,\mathsf{rk}) : x \in V),\\ \mathsf{MaxSum}(D,\mathsf{rk}) &= \max(\mathsf{psum}(x,\mathsf{rk}) : x \in V),\\ \mathsf{DiffSum}(D,\mathsf{rk}) &= \mathsf{MaxSum}(D,\mathsf{rk}) - \mathsf{MinSum}(D,\mathsf{rk}), \text{ and}\\ \mathsf{RatioSum}(D,\mathsf{rk}) &= \mathsf{MaxSum}(D,\mathsf{rk})/\mathsf{MinSum}(D,\mathsf{rk}).\end{aligned}$$

(The point and block sum metric notations are syntactically indistinguishable, so it is important to emphasize what kind of labelling rk is (block or point)).

Example 2. Consider the block labelling $\mathsf{rk} : \{B_0, \ldots, B_{11}\} \to [0, 11]$ of the blocks of the STS(9) D_9 of Table 2.1 given by $\mathsf{rk}(B_i) = i$ for $i \in [0, 11]$. Then

1. $\mathsf{MinSum}(D_9, \mathsf{rk}) = 6$, since $\mathsf{psum}(\mathrm{a}, \mathsf{rk}) = 6$ is minimum;
2. $\mathsf{MaxSum}(D_9, \mathsf{rk}) = 28$, since $\mathsf{psum}(\mathrm{f}, \mathsf{rk}) = 28$ is maximum;
3. $\mathsf{DiffSum}(D_9, \mathsf{rk}) = 22$; and
4. $\mathsf{RatioSum}(D_9, \mathsf{rk}) = 14/3$.

Here are some bounds on the point-labelling metrics.

Theorem 1 ([22])**.** *When D is a Steiner system $S(t, k, v)$,*

$$\begin{aligned}\mathit{MinSum}(D) \le \mathit{MinSum}(t,k,v) &\le \frac{1}{2}(v(k-t+1)+k(t-2)),\\ \mathit{MaxSum}(D) \ge \mathit{MaxSum}(t,k,v) &\ge \frac{1}{2}(v(k+t-1)-kt),\\ \mathit{DiffSum}(D) \ge \mathit{DiffSum}(t,k,v) &\ge (v-k)(t-1), \text{ and}\\ \mathit{RatioSum}(D) \ge \mathit{RatioSum}(t,k,v) &\ge \frac{v(k+t-1)-kt}{v(k-t+1)+k(t-2)}.\end{aligned}$$

When $k = t+1$, $\mathit{MinSum}(D) \le (v-1)+\binom{t}{2}$, $\mathit{MaxSum}(D) \ge t(v-1)-\binom{t}{2}$, $\mathit{DiffSum}(D) \ge (t-1)(v-t-1)$, and $\mathit{RatioSum}(D) \ge \frac{t(v-1)-\binom{t}{2}}{(v-1)+\binom{t}{2}}$. When D is an STS(v), the stronger bounds $\mathit{DiffSum}(D) \ge v$ for $v < 13$ and $\mathit{DiffSum}(D) \ge v+1$ for $v \ge 13$ hold.

The MinSum, MaxSum, DiffSum, or RatioSum of a point-labelled Steiner system is *optimal* if it meets the corresponding bound of Theorem 1.

Within the domain of Steiner systems, point labellings have been devised only for Steiner triple systems. In [22], Dau and Milenkovic label those STS(v)s, $v \equiv 3 \pmod 6$, produced by the Bose construction (with the *Bose labelling*) and those STS(v)s, $v \equiv 1 \pmod 6$, produced by the Skolem construction [58] (with the *Skolem labelling*) to attain MinSum v for all admissible v, the best possible by Theorem 1. In [10], the construction of Schreiber and Wilson [54, 63] is used to produce an infinite (proper) subclass of STS(v)s having DiffSum at most $v+4$, and a modified version of the Schreiber-Wilson construction is used to produce for all admissible v an STS(v) with DiffSum at most $v+7$.

Likewise, block labellings have been supplied only for Steiner triple systems. In [22], block labellings are provided for all admissible v of an STS(v) obtaining MinSum and DiffSum $O(v^3)$. In [15], Colbourn coins the term *egalitarian* block labellings to refer to block labellings attaining DiffSum 0 and constructs them for an infinite family of Steiner triple systems.

2.2.2 Point Labellings and Independent Sets of Steiner Systems

An *independent set* of an $S(t,k,v)$, $D=(V,\mathcal{B})$, is a subset $I \subseteq V$ with the property that no block of $\mathcal{B}$ is contained in I. The *independence number* $\alpha(D)$ of an $S(t,k,v)$, D, is $\max(|I| : I$ is an independent set of $D)$.

There is a close connection between the independence number of a Steiner system and the quality of its labellings.

Theorem 2 ([10])**.** *For a Steiner system $S(t,k,v)$ D to meet the MinSum bound of*

Theorem 1, it is required that

$$\alpha(D) \geq \frac{v(k-t+1)}{2k} + \frac{k+t-3}{2}.$$

For D to meet the $\mathsf{DiffSum}$ *bound of Theorem 1, it must have disjoint independent sets of sizes* $(\frac{v(k-t+1)}{2k} + \frac{k+t}{2} - 1, \frac{v(k-t+1)}{2k} + \frac{k+t}{2} - 1)$.

Thus, by Theorem 3 below, it is guaranteed that an arbitrary Steiner system cannot be meet the MinSum and $\mathsf{DiffSum}$ bounds of Theorem 1.

Theorem 3 ([44, 51])**.** *For some positive constant c, there exists an $S(t,k,v)$ D for which*

$$\alpha(D) \leq c v^{\frac{k-t}{k-1}} (\log v)^{\frac{1}{k-1}}.$$

Indeed, an immediate corollary of Theorem 3 is that in the case of Steiner triple systems, $\alpha_{\min}(v) \leq c\sqrt{v \log v}$; it is easy to see that this falls (asymptotically) short of the required independent set sizes of Theorem 2 for $S(2,3,v)$s.

Independent sets themselves can also be used to construct point labellings of Steiner systems.

Lemma 1 ([10])**.** *When an $S(t,k,v)$ D has two disjoint independent sets of sizes α and β, then $\mathsf{MinSum}(D) \geq \alpha + \binom{k-1}{2}$ and $\mathsf{MaxSum}(D) \leq k(v-1) - \binom{k-1}{2} - \beta$, so that $\mathsf{DiffSum}(D) \leq k(v+2-k) - \alpha - \beta - 2$.*

Proof. Any point labelling assigning labels $[0, \alpha - 1]$ to the points of the independent set of size α and labels $[v-\beta, v-1]$ to the points of the independent set of size β meets the given bounds. $\square$

2.3 Related Work

Other work has been done on the access balancing problem. In [64], an alternative to the Dau and Milenkovic model is proposed to label fractional repetition codes that are not equivalent to Steiner systems. In [2], infinitely many Kirkman triple systems are labelled to attain optimal MinSum.

The problem of labelling, or equivalently (totally) ordering, the blocks of Steiner systems predates the application of access balancing. In [18], with an application to erasure codes for disk arrays, the problem is considered of ordering the blocks of a partial Steiner triple system such that any m consecutive triples are pairwise disjoint. An entire monograph [23] has even been dedicated ordering the blocks of designs, motivated by a range of applications from group testing to tournament scheduling.

The problem of labelling graphs, which themselves are nothing more than set systems, is a significant sub-field of graph theory. Two types of labellings are of interest. The first are *magic labellings*, introduced in [55], in which the edges of the graph are labelled by the first m positive integers such that the sum of the labels of the edges incident with a vertex x and the sum of the labels of the edges incident with any other vertex y are the same. Such labellings are closely related to the block labellings studied in this thesis. The second are *graceful labellings* [52]: an assignment of the set of labels $[0, n-1]$ to the vertices of an undirected graph of order n such that the induced edge labels are distinct; that is, the absolute difference between the labels of the endvertices of an edge.

Chapter 3

THE MAXIMUM DOUBLE INDEPENDENCE NUMBER OF STEINER TRIPLE SYSTEMS

Given an $S(t, k, v)$ D with disjoint independent sets I_1 and I_2, Lemma 1 constructs a point labelling of D to derive an upper bound on $\mathsf{DiffSum}(D)$ that decreases as $|I_1| + |I_2|$ increases. One is thereby motivated to find as large a pair of disjoint independent sets as possible. Define

$$\alpha_{\max}(v) = \max(\alpha(D) : D \text{ is an STS}(v)).$$

Sauer and Schönheim determined $\alpha_{\max}(v)$:

Theorem 4 ([53])**.** *For all admissible v,* $\alpha_{\max}(v) = \begin{cases} (v+1)/2 & \text{if } v \equiv 3, 7 \pmod{12} \\ (v-1)/2 & \text{if } v \equiv 1, 9 \pmod{12}. \end{cases}$

In this chapter we extend Theorem 4 to pairs of disjoint independent sets of maximum total cardinality. The *double independence number* $\alpha_d(D)$ of an STS(v), D, is

$$\max(|I_1 \cup I_2| : I_1 \text{ and } I_2 \text{ are disjoint independent sets of } D).$$

Let $\alpha_{d,\max}(v)$ denote $\max(\alpha_d(D) : D \text{ is an STS}(v))$. Our main result is a determination of $\alpha_{d,\max}(v)$ for all admissible orders v. Of course, even if it were possible that some admissible v existed for which $\alpha_{d,\max}(v) = v$, the best labelling that one could get out of Lemma 1 would have DiffSum at most $2v - 5$, which is no improvement over the state of the art [10]. Regardless, we find the subject of this chapter of sufficient theoretical interest in the domain of classical design theory to justify its existence.

Here is the main result of this chapter:

Theorem 5. *For all admissible v,*

$$\alpha_{d,\max}(v) = \begin{cases} 4v/5 & \text{if } v \equiv 15, 25 \pmod{30}, \\ (4v+1)/5 & \text{if } v \equiv 1, 21 \pmod{30}, \\ (4v+2)/5 & \text{if } v \equiv 7, 27 \pmod{30}, \\ (4v+3)/5 & \text{if } v \equiv 3, 13 \pmod{30}, \\ (4v+4)/5 & \text{if } v \equiv 9, 19 \pmod{30}, \end{cases}$$

or equivalently, $\alpha_{d,\max}(v) = \lceil 4v/5 \rceil$.

We establish that the quantities given in Theorem 5 are upper bounds in Section 3.1. Then in Section 3.2 we develop constructions to show that they are also lower bounds.

3.1 Upper bounds for $\alpha_{d,\max}$

Haddad and Rödl [30] establish indirectly that $\alpha_{d,\max}(v) \leq \lfloor \frac{4}{5}v \rfloor + 1 = \lfloor \frac{4v+5}{5} \rfloor$, in the context of studying sizes of colour classes in c-colourings of Steiner triple systems. Theorem 5 requires a slightly stronger bound, $\lceil 4v/5 \rceil = \lfloor \frac{4v+4}{5} \rfloor$. These two bounds agree except when $v \equiv 15, 25 \pmod{30}$. We prove the bound in order to explore the sizes of the two independent sets required.

Lemma 2. *Suppose that an STS(v), $D = (V, \mathcal{B})$, has a 3-partition $\{A_1, A_2, C\}$ of V in which A_1 and A_2 are independent sets, and $|A_1| = \alpha_1$, $|A_2| = \alpha_2$, and $|C| = \gamma$. Then $\gamma \geq \frac{\alpha_1^2+\alpha_2^2-\alpha_1\alpha_2}{\alpha_1+\alpha_2} - 1$. When $|\alpha_1 - \alpha_2| \leq 1$, the bound on γ is the minimum, $\gamma \geq \lceil (v-4)/5 \rceil$.*

Proof. Let $\mathcal{B}_A \subseteq \mathcal{B}$ be the triples contained in $A_1 \cup A_2$, and $G_A = (A_1 \cup A_2, E_A)$ be the graph with edge set $E_A = \{\{p, p'\} \subseteq A_1 \cup A_2 : \{p, p'\} \subset B \in \mathcal{B}_A\}$. Because A_1 and A_2 are independent, every triple of $\mathcal{B}_A$ must contain two pairs having one end in A_1 and the other in A_2. Hence $|\mathcal{B}_A| \leq \frac{1}{2}\alpha_1\alpha_2$ and $|E_A| \leq \frac{3}{2}\alpha_1\alpha_2$. The complement graph $\overline{G_A}$ has at least $\binom{\alpha_1+\alpha_2}{2} - \frac{3\alpha_1\alpha_2}{2} = \frac{\alpha_1^2+\alpha_2^2-\alpha_1\alpha_2-\alpha_1-\alpha_2}{2}$ edges, and hence average degree at least $\delta = \frac{\alpha_1^2+\alpha_2^2-\alpha_1\alpha_2}{\alpha_1+\alpha_2} - 1$. Choose $x \in A_1 \cup A_2$ having maximum degree in $\overline{G_A}$. For each edge $\{x, y\}$ of $\overline{G_A}$, the triple containing $\{x, y\}$ contains a different element of C. Hence $\gamma \geq \delta$.

Now $(\gamma+1)(\alpha_1+\alpha_2) \geq (\alpha_1+\alpha_2)^2 - 3\alpha_1\alpha_2$. This is minimized when α_1 and α_2 are as equal as possible. If $\alpha_1 = \alpha_2$, write $\gamma = v - 2\alpha_1$. Then $(\gamma+1)(v-\gamma) \geq \frac{(v-\gamma)^2}{4}$, and hence $\gamma \geq \frac{1}{4}(v-\gamma) - 1$; thus $\gamma \geq \lfloor (v-4)/5 \rfloor$. If $\alpha_1 = \alpha_2 + 1$, write $\gamma = v - 2\alpha_1 + 1$. Then $(\gamma+1)(v-\gamma) \geq \frac{(v-\gamma)^2}{4} + \frac{3}{4}$. Hence $\gamma \geq \frac{1}{4}(v-\gamma) - 1 + \frac{3}{4(v-\gamma)}$, and thus $\gamma \geq \lceil (v-4)/5 \rceil$. □

Lemma 2 establishes the upper bounds on $\alpha_{d,\max}(v)$ in Theorem 5, and its proof suggests that systems with largest double independence number should have the two disjoint independent sets close in size. For example, Lemma 2 ensures that $\alpha_{d,\max}(30s+19) \leq \lceil \frac{4\cdot(30s+19)}{5} \rceil = 24s+16$. But it says more: When the two disjoint independent sets have sizes $12s+8-\tau$ and $12s+8+\tau$, we must have $6s+3 \geq \frac{(12s+8+\tau)^2+(12s+8-\tau)^2-(12s+8+\tau)(12s+8-\tau)}{24s+16} - 1$. Then $6s+4 \geq \frac{(12s+8)^2+3\tau^2}{24s+16}$ so $\tau^2 \leq 0$, and the bound could only be realized by disjoint independent sets of the same size. Similar calculations give the same conclusion for $30s+9$; when $v \equiv 3, 13 \pmod{30}$, they establish that the two independent sets must differ in size by exactly 1.

In certain congruence classes, however, there can be different choices for the sizes of the two independent sets. For example, by Lemma 2, $\alpha_{d,\max}(30s+15) \leq \lceil \frac{4\cdot(30s+15)}{5} \rceil = 24s+12$. When the two disjoint independent sets have sizes $12s+6-\tau$ and $12s+6+\tau$,

$6s+4 \geq \frac{(12s+6)^2+3\tau^2}{24s+12} = 6s+3+\frac{\tau^2}{8s+4}$ so $\tau \leq 2\sqrt{2s+1}$. The same bound holds for $30s+25$.

Although the independent sets need not have sizes as equal as possible to meet the bound in this congruence class, they cannot be far apart. Despite the possibility of the two independent sets differing in size by two or more, all of our constructions produce two independent sets that are as equal in size as possible.

3.2 The constructions

In order to establish the lower bounds on $\alpha_{d,\max}(v)$ in Theorem 5, we employ a number of related designs. We introduce these first, and then provide the necessary constructions for the maximum double independence number in Section 3.2.2 when $v \equiv 9, 19 \pmod{30}$; Section 3.2.3 when $v \equiv 7, 27 \pmod{30}$; and Section 3.2.4 when $v \equiv 1, 3, 13, 15, 21, 25 \pmod{30}$.

For quick reference by the reader, Table 3.1 lists cases to be settled, giving the sizes of the two independent sets (α_1 and α_2), the number of remaining points (γ), and the number of the theorem/lemma/corollary in which the required STS is constructed. In order to treat all $v \geq 7$, each case is to be settled for all $s \geq 1$.

Case	v	γ	α_1	α_2	Construction(s)		
					$s = 1$	$s = 2$	$s \geq 3$
C1	$30s + 1$	$6s$	$12s + 1$	$12s$	(5)	(3)	
C2	$30s + 3$	$6s$	$12s + 2$	$12s + 1$	(3)		
C3	$30s - 23$	$6s - 5$	$12s - 9$	$12s - 9$	(1)	(11)	
C4	$30s - 21$	$6s - 5$	$12s - 8$	$12s - 8$	(10)		
C5	$30s - 17$	$6s - 4$	$12s - 6$	$12s - 7$	(5)	(3)	
C6	$30s - 15$	$6s - 3$	$12s - 6$	$12s - 6$	(1)	(3)	
C7	$30s - 11$	$6s - 3$	$12s - 4$	$12s - 4$	(10)		
C8	$30s - 9$	$6s - 2$	$12s - 3$	$12s - 4$	(5)	(6)	(3)
C9	$30s - 5$	$6s - 1$	$12s - 2$	$12s - 2$	(5)	(2)	(3)
C10	$30s - 3$	$6s - 1$	$12s - 1$	$12s - 1$	(11)		

Table 3.1: Roadmap for the Constructions

A *partial triple system* PTS(v) is a pair $(V, \mathcal{B})$, where V is a v-set of *points* and $\mathcal{B}$ is a set of 3-subsets of V (*blocks*) with the property that each unordered pair of points occurs in at most one block of $\mathcal{B}$. An *incomplete triple system* of *order* v with a *hole* of size w (ITS(v, w)) is a PTS(v) $(V, \mathcal{B})$ with the property that for some w-subset $W \subset V$, if $x, y \in W$, no triple of $\mathcal{B}$ contains $\{x, y\}$, and if $x \in V \setminus W$ and $y \in V$, exactly one triple of $\mathcal{B}$ contains $\{x, y\}$. We employ the *Doyen-Wilson theorem*:

Theorem 6 ([24])**.** *An ITS*(v, w) *exists whenever* $w \equiv 1, 3 \pmod 6$ *or* $w = 0$, $v \equiv 1, 3 \pmod 6$, *and* $v \geq 2w + 1$.

When $w \equiv 1, 3 \pmod 6$, the hole of an ITS(v, w) can be filled with an STS(w); then the STS(w) is a *subsystem* of the STS(v), a *sub-STS*(w).

We employ two well-known results on 3-GDDs.

Theorem 7 (see [66], for example)**.** *A* 3*-GDD of type* m^u *exists if and only if* $u \geq 3$, $(u - 1)m \equiv 0 \pmod 2$, *and* $u(u - 1)m^2 \equiv 0 \pmod 6$.

Theorem 8 ([17]). *Let g, u, and m be nonnegative integers. A 3-GDD of type $g^u m^1$ exists if and only if the following all hold:*

1. *if $g > 0$, then $u \geq 3$, or $u = 2$ and $m = g$, or $u = 1$ and $m = 0$, or $u = 0$;*
2. *$m \leq g(u-1)$ or $gu = 0$;*
3. *$g(u-1) + m \equiv 0 \pmod 2$ or $gu = 0$;*
4. *$gu \equiv 0 \pmod 2$ or $m = 0$; and*
5. *$\frac{1}{2}g^2u(u-1) + gum \equiv 0 \pmod 3$.*

A *k-MGDD* of *type* $m \times n$ is a quadruple $(V, \mathcal{G}, \mathcal{H}, \mathcal{B})$, where $V = \{x_{ij} : 0 \leq i < m, 0 \leq j < n\}$ is a set of mn *points*; $\mathcal{G} = \{G_i = \{x_{ij} : 0 \leq j < n\} : 0 \leq i < m\}$ is a set of *first groups*; $\mathcal{H} = \{H_j = \{x_{ij} : 0 \leq i < m\} : 0 \leq j < n\}$ is a set of *second groups*; and $\mathcal{B}$ is a set of k-subsets (blocks) of V, so that every 2-subset of V appears either in a first or second group, or in exactly one block of $\mathcal{B}$, but not both.

Theorem 9 ([1, 19]). *Let $m, n \geq 3$. A 3-MGDD of type $m \times n$ exists if and only if* $\gcd(n-2, m-2, 6) = 1$.

3.2.1 A $2v + 1$ Construction

In order to make a few examples, we employ a specific $2v + 1$ *construction* from [19] and examine the disjoint independent sets produced.

Lemma 3. *Suppose that an STS(v) exists with disjoint independent sets of sizes α_1 and α_2. Then an STS$(2v+1)$ exists with disjoint independent sets of sizes $2\alpha_1$ and $2\alpha_2$.*

Proof. Let $(X, \mathcal{B})$ be an STS(v) having disjoint independent sets $A_1, A_2 \subset X$. Form the STS$(2v + 1)$ on points $(X \times \{1, 2\}) \cup \{\infty\}$. For each $B \in \mathcal{B}$, include the triples of a 3-GDD of type 2^3 (from Theorem 7) on $B \times \{1,2\}$, aligning groups on $\{\{x\} \times \{1,2\} : x \in B\}$. Then for each $x \in X$, include the triple $\{\infty, (x,1), (x,2)\}$. In the resulting STS($2v+1$), $A_1 \times \{1,2\}$ and $A_2 \times \{1,2\}$ are disjoint independent sets. □

Corollary 1. *The unique STS(7) exists having two disjoint independent sets, both of size 3. An STS(15) exists having two disjoint independent sets, both of size 6.*

Proof. The unique STS(7) can be written with points $\{0, \ldots, 6\}$ and blocks

$$\{\{i, i+1, i+3\} : 0 \le i \le 6\},$$

with addition performed modulo 7. Then $\{0,1,4\}$ and $\{2,3,6\}$ are disjoint independent sets. To obtain the STS(15), apply Lemma 3 to this STS(7). □

3.2.2 A GDD/ITS Construction

We address the cases $v \equiv 9, 19 \pmod{30}$ in this subsection.

Theorem 10. *Let A_1, A_2, C be disjoint sets with $|C| = \gamma \equiv 1, 3 \pmod 6$ and $|A_1| = |A_2| = 2\gamma + 2$. Then there exists an STS($5\gamma + 4$) on $A_1 \cup A_2 \cup C$ with A_1 and A_2 independent.*

Proof. Let X_1, X_2, X_3, and X_4 be four disjoint sets of size $\gamma + 1$, so that $A_1 = X_1 \cup X_2$ and $A_2 = X_3 \cup X_4$. Construct the block set of the required STS($5\gamma + 4$) as follows. First include the blocks of a 3-GDD of type $(\gamma+1)^4$ having groups X_1, X_2, X_3, and X_4, from Theorem 7. Next, for $i \in \{1,2,3,4\}$, include the blocks of an ITS($2\gamma+1, \gamma$) (from Theorem 6) on $X_i \cup C$ with hole C. Finally, place an STS(γ) on C.

By an elementary counting argument, each triple of an ITS($2\gamma+1, \gamma$) has exactly one point from the hole. Hence A_1 and A_2 are independent sets of the STS($5\gamma+4$). □

When $\gamma = 6s - 5$, Theorem 10 constructs the STS($30s - 21$) needed in Theorem 5 for all $s \geq 1$. When $\gamma = 6s - 3$, it constructs the STS($30s - 11$) for all $s \geq 1$.

3.2.3 An MGDD Construction

We address the cases $v \equiv 7, 27 \pmod{30}$ in this subsection.

Theorem 11. *Let A_1, A_2, C be disjoint sets with $|C| = \gamma \equiv 1, 5 \pmod{6}$ and $|A_1| = |A_2| = 2\gamma + 1$. Then there exists an STS$(5\gamma + 2)$ on $A_1 \cup A_2 \cup C$ with A_1 and A_2 independent.*

Proof. Corollary 1 handles the case with $\gamma = 1$, so assume that $\gamma \geq 5$. Let C, X_1, X_2, X_3, and X_4 be five disjoint sets of size γ. Let a_1 and a_2 be two other elements, and set $A_1 = X_1 \cup X_2 \cup \{a_1\}$ and $A_2 = X_3 \cup X_4 \cup \{a_2\}$. To construct the blocks of the STS$(5\gamma + 2)$, first include the blocks of a 3-MGDD of type $4 \times \gamma$ (from Theorem 9) having first groups X_1, X_2, X_3, X_4 and second groups $Y_1, \ldots, Y_\gamma$. Let $\{x_{ij}\} = X_i \cap Y_j$ for $1 \leq i \leq 4$ and $1 \leq j \leq \gamma$. Next, for every second group $Y_j = \{x_{1j}, x_{2j}, x_{3j}, x_{4j}\}$, include the triples $\{a_1, x_{1j}, x_{3j}\}, \{a_1, x_{2j}, x_{4j}\}$, $\{a_2, x_{1j}, x_{4j}\}$, and $\{a_2, x_{2j}, x_{3j}\}$. Then place an STS$(\gamma + 2)$ on $C \cup \{a_1, a_2\}$.

The pairs on $A_1 \cup A_2$ that are not yet in triples are

$$\{\{x_{ij}, x_{i\ell}\} : 1 \leq i \leq 4, 1 \leq j < \ell \leq \gamma\} \cup \{\{x_{1j}, x_{2j}\}, \{x_{3j}, x_{4j}\} : 1 \leq j < \ell \leq \gamma\};$$

each must appear in a triple whose third element is in C. These pairs form two copies of the Cartesian product $K_\gamma \Box K_2$, a regular graph of degree γ. This graph admits a 1-factorization [19, Lemma 1.17]; attach each of the γ 1-factors to a point of C to form triples. Then A_1 and A_2 are disjoint independent sets. $\Box$

When $\gamma = 6s - 5$, Theorem 11 constructs the STS$(30s - 23)$ needed in Theorem 5 for all $s \geq 1$. When $\gamma = 6s - 1$, it constructs the STS$(30s - 3)$ for all $s \geq 1$. In addition, it produces a solution for a further order:

Corollary 2. *An STS*(55) *exists with disjoint independent sets of sizes* 22 *and* 22.

Proof. Theorem 11 yields an STS(27) with disjoint independent sets of sizes 11 and 11. Apply Lemma 3. □

3.2.4 A GDD Construction

We employ a variant of Wilson's fundamental construction (WFC) to treat the remaining congruence classes. First, we produce a key ingredient.

Table 3.2: The latin square L for Lemma 4.

3	5	1	4	2
5	4	3	2	1
1	3	2	5	4
4	2	5	1	3
2	1	4	3	5

Lemma 4. *When* $|X| = 3$, *a* 3-*GDD*

$$(X \times \{1,2,3,4,5\}, \{\{g\} \times \{1,2,3,4,5\} : g \in X\}, \mathcal{B})$$

of type 5^3 *exists in which* $X \times \{1,2\}$ *and* $X \times \{3,4\}$ *are disjoint independent sets, each of size 6.*

Proof. Let $L = (\ell_{ij})$ be the latin square in Table 3.2 and let $X = \{x_1, x_2, x_3\}$. Form blocks $\mathcal{B} = \{\{(x_1, i), (x_2, j), (x_3, \ell_{ij})\} : 1 \leq i, j \leq 5\}$. The verification is routine. □

We also require explicit solutions for some small orders.

Lemma 5. *There is an STS(v) having disjoint independent sets of sizes α_1 and α_2 when* $(v, \alpha_1, \alpha_2) \in \{(13, 6, 5), (21, 9, 8), (25, 10, 10), (31, 13, 12)\}$.

Proof. An STS(13) whose point set partitions into independent sets of sizes 6, 5, and 2 is given in [27]. Table 3.3 provides the remaining STSs. All were generated by simulated annealing. □

Theorem 12. *Suppose that a 3-GDD of type $g_1^{u_1} \dots g_\ell^{u_\ell}$ exists. Further suppose that $f = 0$ or $f \equiv 1, 3 \pmod 6$, $f = f_1 + f_2 + f_3$ with $f_1, f_2, f_3 \geq 0$, and, for each $1 \leq i \leq \ell$, an STS($5g_i + f$) exists that (1) contains a sub-STS(f) when $f > 0$, and (2) has two disjoint independent sets of sizes $2g_i + f_1$ and $2g_i + f_2$ containing f_1 and f_2 points from the sub-STS(f) (if present), respectively. Then there exists an STS($f + 5\sum_{i=1}^{\ell} u_i g_i$) having disjoint independent sets of sizes $f_1 + 2\sum_{i=1}^{\ell} u_i g_i$ and $f_2 + 2\sum_{i=1}^{\ell} u_i g_i$.*

Proof. Start with a 3-GDD $D = (X, \mathcal{G}, \mathcal{B})$ of type $g_1^{u_1} \dots g_\ell^{u_\ell}$. Let $\mathcal{G} = \{G_1, \dots, G_{\sum_{i=1}^{\ell} u_i}\}$. We construct the STS($f + 5\sum_{i=1}^{\ell} u_i g_i$) on points $V = (X \times \{1, 2, 3, 4, 5\}) \cup F$, where $F = \{p_1, \dots, p_f\}$ and $F \cap (X \times \{1, 2, 3, 4, 5\}) = \emptyset$. Its blocks are determined as follows. First, for each group $G \in \mathcal{G}$ with $|G| = g_i$, place a copy of an STS($5g_i + f$) on $(G \times \{1, 2, 3, 4, 5\}) \cup F$ so that $(G \times \{1, 2\}) \cup \{p_1, \dots, p_{f_1}\}$ and $(G \times \{3, 4\}) \cup \{p_{f_1+1}, \dots, p_{f_1+f_2}\}$ are both independent; omit all triples in the sub-STS(f) *except* when $G = G_1$. Secondly, for each $B \in \mathcal{B}$, form a copy of the 3-GDD of type 5^3 from Lemma 4 on $B \times \{1, 2, 3, 4, 5\}$, aligning groups on $\{\{x\} \times \{1, 2, 3, 4, 5\} : x \in B\}$.

Consider any two points $x, y \in V$. If $\{x, y\} \subset F$, there is one triple containing $\{x, y\}$, and it is of the first type (when $G = G_1$). If $x \in F$ and $y = (g, i) \in X \times \{1, 2, 3, 4, 5\}$, exactly one group $G \in \mathcal{G}$ contains g, and hence exactly one triple contains $\{x, y\}$, also of the first type. If $x, y \in (X \times \{1, 2, 3, 4, 5\})$, write $x = (g, i)$ and $y = (h, j)$. Then if $\{g, h\} \subseteq G$ for some group G, exactly one triple contains $\{x, y\}$, of

Table 3.3: STS(v) for $v \in \{21, 25, 31\}$. Commas and braces are omitted. Lower case letters are used for one independent set, upper case letters for the other, and digits for the remainder.

STS(21) with a sub-STS(7) on `a,b,c,A,B,0,1`:

```
abA ac0 aB1 bcB b01 cA1 AB0 ad3 aeH afD agE ah2 aiF aCG bdF
beE bf3 bg2 bhH biC bDG cdD ce2 cfH cgG chE ci3 cCF de0 dfG
dgA dhC diB dEH d12 ef1 egC eh3 eiG eAF eBD fgF fh0 fi2 fAC
fBE ghD gi0 gBH g13 hi1 hAG hBF iAH iDE AD3 AE2 BC2 BG3 CD1
CE0 CH3 DF0 DH2 EF3 EG1 FG2 FH1 GH0 023
```

STS(25):

```
abF ac0 adD ae1 afG ag3 ah2 aiJ aj4 aAB aCI aEH bc4 bdE beG
bf1 bg0 bhA biI bjD bBJ bC2 bH3 cd3 ceA cfH cgJ chC ciD cj2
cB1 cEF cGI de4 df2 dgG dhH di0 dj1 dAF dBC dIJ efJ egE ehI
ei2 ejB eCH eDF e03 fg4 fhF fi3 fj0 fAE fBI fCD ghB giC gjI
gAD gFH g12 hi4 hj3 hDG hEJ h01 ijE iAG iBH iF1 jAC jFJ jGH
AH4 AI1 AJ0 A23 BD3 BE2 BF4 BG0 CE3 CF0 CG4 CJ1 DE0 DH1 DI2
DJ4 EG1 EI4 FG2 FI3 GJ3 HI0 HJ2 024 134
```

STS(31):

```
ab4 acD ad1 aeH afF agL ah5 ai2 ajC ak0 alI am3 aAG aBE aJK
bc3 bd5 be2 bf0 bgF bhK biC bjE bk1 blA bmJ bBD bGH bIL cdJ
ce0 cf4 cgK chB ciL cj1 ckH cl2 cmC cAF cEI cG5 de3 dfH dgC
dhG diD dj2 dkA dl4 dmE dBF dI0 dKL ef1 egE ehF ei5 ejA ek4
elK emL eBJ eCD eGI fg2 fh3 fiG fjI fkK fl5 fmB fAC fDJ fEL
ghI gi0 gj5 gk3 glD gm4 gAH gB1 gGJ hi4 hjJ hk2 hl1 hmA hCE
hDH hL0 ijF ikB il3 im1 iAK iEJ iHI jkG jl0 jmD jBK jHL j34
klJ km5 kCI kDE kFL lmH lBL lCG lEF mFG mIK m02 AB5 AD3 AE4
AI2 AJ0 AL1 BC2 BG0 BH3 BI4 CF4 CH0 CJ1 CK5 CL3 DF0 DG1 DI5
DK4 DL2 EG3 EH2 EK0 E15 FH5 FI1 FJ2 FK3 GK2 GL4 HJ4 HK1 IJ3
JL5 013 045 124 235
```

the first type; otherwise $\{g, h\} \subseteq B$ for some block B, and exactly one triple contains $\{x, y\}$, of the second type.

By construction, $(X \times \{1, 2\}) \cup \{p_1, \ldots, p_{f_1}\}$ and $(X \times \{3, 4\}) \cup \{p_{f_1+1}, \ldots, p_{f_1+f_2}\}$ are disjoint independent sets of the required sizes. $\square$

	Value(s) of s	STSs	3-GDDs	(f, f_1, f_2)
C1	2	STS(21)	4^3	$(1, 1, 0)$
	≥ 3	STS(31)	6^s	$(1, 1, 0)$
C2	≥ 2	STS(13)	2^{3s}	$(3, 2, 1)$
C5	≥ 2	STS(13)	2^{3s-2}	$(3, 2, 1)$
C6	≥ 2	STS(15)	3^{2s-1}	$(0, 0, 0)$
C8	3	STS(21)	4^4	$(1, 1, 0)$
	≥ 4	STS(21), STS(31)	$6^{s-1}4^1$	$(1, 1, 0)$
C9	≥ 3	STS(15), STS(25)	$3^{2s-1}5^1$	$(0, 0, 0)$

Table 3.4: Ingredient STSs and 3-GDDs.

Corollary 3. *Suppose that $v \geq 13$, $v \equiv 1, 3 \pmod 6$, $v \notin \{51, 55\}$, and $s \geq 1$. In each of the cases from Table 3.1 listed here,*

Case	v	γ	α_1	α_2
C1	$30s + 1$	$6s$	$12s + 1$	$12s$
C2	$30s + 3$	$6s$	$12s + 2$	$12s + 1$
C5	$30s - 17$	$6s - 4$	$12s - 6$	$12s - 7$
C6	$30s - 15$	$6s - 3$	$12s - 6$	$12s - 6$
C8	$30s - 9$	$6s - 2$	$12s - 3$	$12s - 4$
C9	$30s - 5$	$6s - 1$	$12s - 2$	$12s - 2$

there exists an STS(v) whose point set admits a partition $\{A_1, A_2, C\}$, where $|A_1| = \alpha_1$, $|A_2| = \alpha_2$, and $|C| = \gamma$, and A_1 and A_2 are both independent sets.

Proof. Apply Lemma 5 when $v \in \{13, 21, 25, 31\}$, and Corollary 1 when $v = 15$. Ingredients to apply Theorem 12 for the six cases are listed in Table 3.4. The 3-GDDs are from Theorem 7 or Theorem 8. □

Corollary 3 establishes the lower bound on $\alpha_{d,\max}(v)$ in Theorem 5 when $v \equiv 1, 3, 13, 15, 21, 25 \pmod{30}$ except when $v \in \{51, 55\}$. For the STS(55), see Corollary 2. Lemma 6 handles the final case.

Lemma 6. *There is an STS*(51) *with disjoint independent sets of sizes* 21 *and* 20.

Proof. We form the STS(51) on elements $(\{1,\ldots,15\} \times \{1,2,3\}) \cup \{p_1,\ldots,p_6\}$ with block set $\mathcal{B}$ and independent sets $(\{1,\ldots,6\}\times\{1,2,3\})\cup\{p_1,p_2,p_3\}$ and $(\{7,\ldots,12\}\times\{1,2,3\}) \cup \{p_4,p_5\}$. Start with the latin square L from Table 3.2. Replace each entry σ in L by the 3×3 latin square $\begin{pmatrix} 3\sigma & 3\sigma-1 & 3\sigma-2 \\ 3\sigma-2 & 3\sigma & 3\sigma-1 \\ 3\sigma-1 & 3\sigma-2 & 3\sigma \end{pmatrix}$ to form a 15×15 latin square $M = (m_{ij})$.

Include in $\mathcal{B}$ the blocks $\{\{(i,1),(j,2),(m_{ij},3)\} : 1 \le i,j \le 15\}$ *except for* the block $\{15\} \times \{1,2,3\}$. Next, for $j \in \{1,2,3\}$, on $(\{1,\ldots,15\} \times \{j\}) \cup \{p_1,\ldots,p_6\}$ align the points of the STS(21) from Table 3.3 so that the sub-STS(7) is on points $\{(15,j),p_1,\ldots,p_6\}$, and independent sets are on $(\{1,\ldots,6\} \times \{j\}) \cup \{p_1,p_2,p_3\}$ and $(\{7,\ldots,12\} \times \{j\}) \cup \{p_4,p_5\}$; once so aligned, include in $\mathcal{B}$ all blocks *not in* the sub-STS(7). Finally, include in $\mathcal{B}$ the blocks of an STS(9) on $(\{15\}\times\{1,2,3\})\cup\{p_1,\ldots,p_6\}$ in which $\{p_1,p_2,p_3\}$ and $\{p_4,p_5\}$ are independent sets. The verification is routine. □

Chapter 4

THE SPECTRUM OF RESOLVABLE BOSE TRIPLE SYSTEMS

The Bose construction produces a Steiner triple system of order $3n$ from a symmetric, idempotent latin square of order n whenever n is odd. It is an especially useful construction for devising quality point labellings. Dau and Milenkovic [22], for example, supply MinSum $3n$ (the best possible per Theorem 1) labellings of Bose-constructed Steiner triple systems for all odd n. In order to produce $S(2,4,v)$s with good MinSum (see Section 5.4), we determine in this chapter the spectrum of resolvable Bose-constructed STSs.

4.1 Preliminaries

A *latin square* of *order* n is an $n \times n$ array $L = (L_{x,y})$ in which every row is a permutation of an n-set S (the *symbol set* of L) and every column is a permutation of S. Let Q be a finite set of size n, and let $\circ$ be a binary operation on Q. The pair $(Q, \circ)$ is a *quasigroup of order* n provided that it satisfies (1) For every $x, y \in Q$, the equation $x \circ z = y$ has a unique solution $z \in Q$, and (2) For every $x, y \in Q$, the equation $z \circ x = y$ has a unique solution $z \in Q$. The *operation table* of $(Q, \circ)$ is the $|Q| \times |Q|$ array $A = (A_{x,y})$, where $A_{x,y} = x \circ y$. A quasigroup $(Q, \circ)$ is *idempotent* if $x \circ x = x$ for all $x \in Q$, and *symmetric* if $x \circ y = y \circ x$ for all $x, y \in Q$. A symmetric and idempotent quasigroup of order n exists if and only if n is odd [60]. The binary operation

$$x \circ y = 3(x + y) \pmod 5$$

Table 4.1: A symmetric idempotent quasigroup of order 5

$\circ$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

defines a symmetric idempotent quasigroup on $\mathbb{Z}_5$. It is given in Table 4.1. Quasigroups and latin squares are related, in that $(Q, \circ)$ is a quasigroup if and only if its operation table is a latin square [16].

Although rows and columns of a latin square could be indexed by different sets of size n, henceforth we take the index sets for rows, columns, and symbols to be the symbol set S. Any two such latin squares L and L' with symbol sets S and S', respectively, are *isomorphic* if there exists a bijection $\phi : S \to S'$ such that $\phi(L_{x,y}) = L'_{\phi(x),\phi(y)}$. An ordered triple $(i, j, L_{i,j})$ is a *cell* of latin square L whose row is i, column is j, and *entry* is $L_{i,j}$. If $c = (x, y, z)$ is a cell of L, denote by $c_{\{\}}$ the set $\{x, y, z\}$; if C is a set of cells of L, define $C_{\{\}} = \{c_{\{\}} : c \in C\}$.

Let L be an idempotent, symmetric latin square L of order n with symbol set S so that $n = |S| \equiv 0 \pmod 3$. A *partial latin square parallel class* (PLSPC) of L is a set $\mathcal{P}$ of cells of L so that whenever $c, c' \in \mathcal{P}$ and $c \neq c'$, we have $c_{\{\}} \cap c'_{\{\}} = \emptyset$. A *latin square parallel class* (LSPC) of L is a PLSPC $\mathcal{P}$ with $|\mathcal{P}| = n/3$; for an LSPC $\mathcal{P}$, $\bigcup_{c\in\mathcal{P}} c_{\{\}} = S$. An *upper triangular resolution* of L is a partition of the set of all cells above the main diagonal into LSPCs. When L has order 3ℓ, such an upper triangular resolution consists of $\frac{3}{2}(3\ell - 1)$ LSPCs.

Let L be a latin square with symbol set $S = \{0, \ldots, n-1\}$. For each $k \in S$, the *k-diagonal* of L is the set of cells $\{(i, i + k, L_{i,i+k}) : 0 \leq i < n - k\}$. When $0 < k \leq \lfloor n/2 \rfloor]$, the *k-diagonal pair* of L is the union of (the cells of) its k- and

$(n-k)$-diagonals. $C_k(L)$ denotes the set of cells of the k-diagonal pair of L, and k is the *index* of $C_k(L)$. When L is clear from the context, we abbreviate this to C_k.

The *averaging latin square* $B = (B_{i,j})$ of order n, n odd, is the latin square with symbol set $S = \{0, \ldots, n-1\}$ such that for all $x, y \in S$, $B_{x,y} = \frac{n+1}{2}(x+y) \pmod{n}$. B is thus the operation table of the quasigroup $Q_B = ([0, n-1], \circ)$, where $x \circ y = \frac{n+1}{2}(x+y) \pmod{n}$, and Q_B is both symmetric and idempotent [60]. A *Bose resolution* of B is either (1) an upper triangular resolution of B or (2) a partition of the set of cells of B above the main diagonal into LSPCs and a set $P = \{P_1, \ldots, P_p\}$ of $p \leq n$ proper PLSPCs for which there exists a partition $\pi = \{\pi_1, \ldots, \pi_q\}$ of $[0, n-1]$ into q sets and a bijection $\rho : P \to \pi$ such that $P_{i_{\{\}}} \cup \rho(P_i)$ is a partition of $[0, n-1]$ for all $i \in [1, p]$.

4.2 The Bose Construction

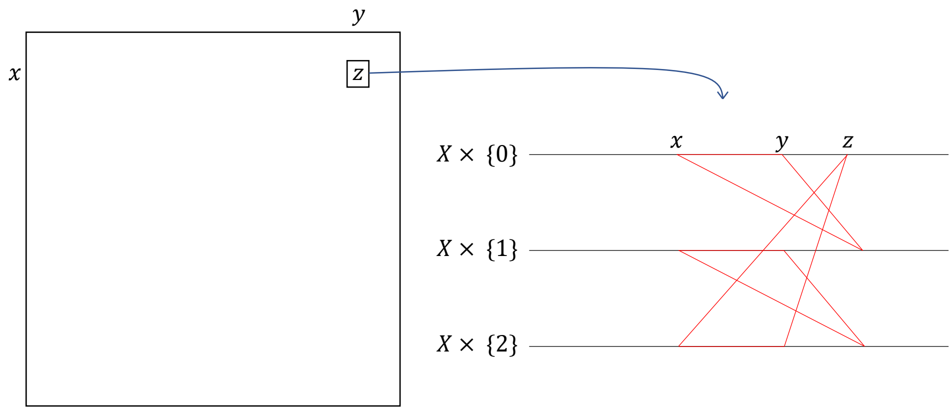
THE BOSE CONSTRUCTION. Let $L = (L_{i,j})$ be the operation table of a symmetric idempotent quasigroup of order n having symbol set $S = [0, n-1]$, and put $V = S \times \mathbb{Z}_3$. For every $x \in [0, n-1]$ define the block $A_x = \{(x, 0), (x, 1), (x, 2)\}$. Then for every pair of distinct elements $x, y \in [0, n-1]$, define a block $C_{x,y,i} = \{(x, i), (y, i), (L_{x,y}, i + 1 \pmod{3})\}$. Set

$$\mathcal{B} = \{A_x : x \in [0, n-1]\} \cup \{C_{x,y,i} : x, y \in S, x < y, i \in \mathbb{Z}_3\}.$$

Then $(V, \mathcal{B})$ is an STS$(3n)$, a *Bose triple system* of order $3n$. An illustration of the blocks of type $C_{x,y,i}$, taken from [60], is given in Figure 4.1.

Because a symmetric idempotent quasigroup of order n exists precisely when n is odd, a Bose triple system of order v exists precisely when $v \equiv 3 \pmod{6}$. If L is the averaging latin square, $(V, \mathcal{B})$ is the *Bose-averaging triple system* of order $3n$.

Figure 4.1: The Bose Construction



Now we establish that Bose resolutions of the averaging latin square of order n yield resolutions of the Bose-averaging triple system.

Theorem 13. *Let B be the averaging latin square of order n and D the Bose-averaging triple system of order $3n$ constructed from B. Then any Bose resolution of B induces a resolution of D.*

Proof. Let $C_{x,y,i}$ and A_x denote the two block types of D. Suppose that the Bose resolution is an upper triangular resolution with LSPCs $\{\mathcal{L}_1, \ldots, \mathcal{L}_{(3n-3)/2}\}$. Then

$$\mathcal{P}_j = \bigcup_{(x,y,z)\in\mathcal{L}_j, i\in\mathbb{Z}_3} C_{x,y,i}$$

is a parallel class of D for all $j \in [1, (3n-3)/2]$. The set $\mathcal{A} = \bigcup_{x\in[0,n-1]} A_x$ is a parallel class of D, and thus $\{\mathcal{P}_1, \ldots, \mathcal{P}_{(3n-3)/2}, \mathcal{A}\}$ is a resolution of D.

Now suppose that the Bose resolution of B is of the second kind, and let $\mathcal{L} = \{\mathcal{L}_1, \ldots, \mathcal{L}_p\}$ denote its set of LSPCs and $P = \{P_1, \ldots, P_q\}$ its set of all proper PLSPCs having a partition $\pi = \{\pi_1, \ldots, \pi_q\}$ of $[0, n-1]$ and a bijection $\rho : P \to \pi$

such that $P_{i_{\{\}}} \cup \rho(P_i)$ is a partition of $[0, n-1]$ for all $i \in [1, q]$. Then both

$$\mathcal{P}_j = \bigcup_{(x,y,z)\in\mathcal{L}_j, i\in\mathbb{Z}_3} C_{x,y,i}$$

and

$$\mathcal{P}'_k = \left(\bigcup_{(x,y,z)\in P_j, i\in\mathbb{Z}_3} C_{x,y,i} \right) \bigcup \left(\bigcup_{x\in\rho(P_j)} A_x \right)$$

are parallel classes of D for all $j \in [1, p]$ and all $k \in [1, q]$ and thus

$$\mathcal{R} = \left(\bigcup_{j\in[1,p]} \mathcal{P}_j \right) \bigcup \left(\bigcup_{k\in[1,q]} \mathcal{P}'_k \right)$$

is a resolution of D. □

Not every operation table of a symmetric idempotent quasigroup admits a Bose resolution.

Theorem 14. *If a Bose triple system of order* $3n$ *is resolvable, then* $n \equiv 3 \pmod 6$.

Proof. Suppose that $\mathcal{P}$ is a parallel class of the Bose triple system $\mathcal{D} = (V, \mathcal{B})$ on $V = [0, n-1] \times \mathbb{Z}_3$. There are four possible configurations of a block $B \in \mathcal{B}$ depending on the second coordinates of its points:

1. $B = \{(x, 0), (y, 0), (z, 1)\}$,
2. $B = \{(x, 1), (y, 1), (z, 2)\}$,
3. $B = \{(x, 2), (y, 2), (z, 0)\}$, or
4. $B = \{(x, 0), (y, 1), (z, 2)\}$;

represent the number of each type in $\mathcal{P}$ as A, B, C, and D, respectively. Then we have:

$$\begin{cases} A+B+C+D=n \\ 2A+C+D=n \\ A+2B+D=n \\ B+2C+D=n, \end{cases}$$

where the first equation counts the triples in $\mathcal{P}$ and the rest count the points in $[0,n-1]\times\{i\}$ for $i\in\mathbb{Z}_3$. Solve this system to get $A=B=C=\frac{n-D}{3}$; it follows that $D\equiv n \pmod 3$.

When $n\equiv 1 \pmod 6$, $D\geq 1$ and thus $\mathcal{D}$ has at most n disjoint parallel classes. But $\mathcal{D}$ requires $\frac{3n-1}{2}$ disjoint parallel classes to be resolvable, and thus no resolution exists. When $n\equiv 5 \pmod 6$, $D\geq 2$ and thus $\mathcal{D}$ would have at most $\frac{n-1}{2}$ disjoint parallel classes. $\square$

Our aim is to prove that the necessary condition of Theorem 14 is sufficient for the class of Bose-averaging triple systems.

4.3 Constructing Bose Resolutions

4.3.1 Bose Square Properties

To construct Bose resolutions, we employ several properties of the averaging latin square B. Henceforth, unless otherwise stated, n denotes the order of the averaging latin square B and C_k denotes the cells of the k-diagonal pair of B.

Property 1. *The set of symbols of $C_k(B)$ is equal to $[0,n-1]$.*

Proof. Suppose that $c = (0, a, b) \in C_k(B)$. Then $b \equiv a \cdot \frac{n+1}{2} \pmod{n}$. For all $i \in [0, n-1]$, $\frac{n+1}{2}(i+(a+i)) \equiv \frac{n+1}{2}(a+2i) \pmod{n} \equiv a\frac{n+1}{2} + (n+1)i \pmod{n} \equiv b+i \pmod{n}$, and hence $(i, a+i, b+i) \pmod{n} \in C_k(B)$ if $i \in [0, n-k]$ and $(a+i, i, b+i) \pmod{n} \in C_k(B)$ if $i \in [n-k+1, n-1]$. That is, $C_k(B)$ is obtained by additively developing c over $\mathbb{Z}_n$ (and permuting the first two coordinates of $c+i \pmod{n}$ for all $i \in [n-k+1, n-1]$).

□

Let $\{i, j\} = \{k, n-k\}$, and consider a cell $c = (x, y, z) \in C_k(B)$ belonging to the j-diagonal of B. The *next adjacent cell of* c, denoted $c \oplus_n 1$, is the cell $(x+1, y+1, z+1) \pmod{n}$ if $y < n-1$ or the cell $(0, x+1, z+1) \pmod{n} = (0, i, z+1) \pmod{n}$ if $y = n-1$. In plain English, the next adjacent cell after the bottom-most cell of the j-diagonal is the topmost cell of the i-diagonal. Extend $\oplus_n$ to all $\alpha \in \mathbb{N}$, defining $c \oplus_n 0 = c$ and $c \oplus_n \alpha = (c \oplus_n 1) \oplus (\alpha - 1)$ if $\alpha \geq 2$. We call $\oplus_n$ the *diagonal pair traversal operator* for B. When the averaging latin square is clear from the context, we simply write $\oplus$.

A triple $T = \{a, b, c\} \subset \mathbb{Z}_n$ is a *d-regular triple* if its elements can be permuted such that the second element minus the first element is equivalent to the third element minus the second element modulo n. For example, if $b - a \equiv c - b \equiv d \pmod{n}$, then arranging T as (a, b, c) certifies that T is d-regular. Any d-regular triple $\{a, b, c\}$ is also $(n-d)$-regular, since if $b - a \equiv c - b \equiv d \pmod{n}$, then $a - b \equiv b - c \equiv n - d \pmod{n}$, so that permuting T to get (c, b, a) certifies that T is $(n-d)$-regular. For each $d \in [1, n-1]$, define

$$\mathcal{T}_d = \{T_d : T_d \in \binom{[0, n-1]}{3} \text{ and } T_d \text{ is } d\text{-regular}\}.$$

Property 2. *For all* $k \in [1, (n-1)/2]$, $\mathcal{T}_{k-k\frac{n+1}{2}} = \{c_{\{\}} : c \in C_k(B)\}$.

Proof. Because $(0, k, \ell) \in C_k(B)$ when $\ell \equiv k \cdot (\frac{n+1}{2}) \pmod{n}$,

$$2\ell \equiv k(n+1) \pmod{n} \iff 2\ell \equiv k \pmod{n} \iff \ell \equiv k - \ell \pmod{n}. \quad (4.2)$$

Hence $\{0, \ell, k\}$ is ℓ-regular; developing it over $\mathbb{Z}_n$ gives $\mathcal{T}_\ell$ and

$$\begin{aligned} C_\ell(B) =& \{(i, k+i, \ell+i) : i \in [0, n-k-1]\} \\ & \cup\{(k+j, j, \ell+j) : j \in [n-k, n-1]\}, \end{aligned} \quad (4.3)$$

where addition is performed modulo n.

□

Property 3. *Let $C_k(B)$ denote an arbitrary diagonal pair with $c_0 = (0, k, \ell) \in C_k(B)$. Then for all $c \in C_k(B)$, $c_{\{\}}$ is d-regular only if $d \equiv \pm\ell \pmod{n}$.*

Proof. Suppose to the contrary that for some $d \in [1, n-1] \setminus \{\ell, -\ell\} \pmod{n}$ and some $c \in C_k(B)$, $c_{\{\}}$ is d-regular. Write $c_{\{\}} = \{x, x+d, x+2d\} \pmod{n}$ for some $x \in [0, n-1]$. By Property 2, some $c' \in C_k(B)$ has $c'_{\{\}} = \{0, d, 2d\}$. Because cells in a diagonal pair occur above the main diagonal of B, there are three possible permutations of $c'_{\{\}}$, namely $(0, d, 2d)$, $(0, 2d, d)$, and $(d, 2d, 0)$. However, the first is not feasible, because $d(n+1)/2 \equiv 2d \pmod{n} \iff d \equiv 0 \pmod{n}$. The third is not feasible, because $3d(n+1)/2 \equiv 0 \pmod{n} \iff d \equiv 0 \pmod{n}$. Finally, the second is not feasible, since otherwise $d = \ell$.

□

For each $k \in [1, (n-1)/2]$ define $\delta(C_k(B)) = \min\{\ell \pmod{n}, n - \ell \pmod{n}\}$, with $(0, k, \ell) \in C_k(B)$, so that $\delta(C_k(B))$ is the unique element of $[1, (n-1)/2]$ such that for all $c \in C_k(B)$, $c_{\{\}}$ is $\delta(C_k(B))$-regular. Then we say that $\delta(C_k(B))$ is the *regular difference* of $C_k(B)$.

Property 4. *For distinct* $k_1, k_2 \in [1, (n-1)/2]$, $\delta(C_{k_1}(B)) \neq \delta(C_{k_2}(B))$.

Proof. Suppose to the contrary that $d = \delta(C_{k_1}(B)) = \delta(C_{k_2}(B)) \pmod{n}$. Then by Property 2, some permutation of $T = \{0, d, 2d\}$ is a cell of C_{k_1} and some (other) permutation of T is a cell of C_{k_2}. As the cells of both diagonal pairs occur above the main diagonal of B, there are three possible permutations of T that yield a cell (in C_{k_1} or C_{k_2}), namely $(0, d, 2d)$, $(0, 2d, d)$, and $(d, 2d, 0)$. As shown in the proof of Property 3, the first and third are not feasible. Hence, the second must occur in two distinct diagonal pairs of B, which is impossible.

□

Property 5. *If* $\delta(C_k(B)) = d$, *then* $k = 2d$.

Proof. By (4.2) of Property 2, $(0, 2d, d) \in C_k(B)$. □

Property 6. *For all* $d \in [0, (n-1)/2]$ *and any* $T_d \in \binom{[0,n-1]}{3}$ *that is d-regular, there exists exactly one cell c above the main diagonal of B such that* $c_{\{\}} = T_d$.

Proof. This follows from Properties 3 and 4.

□

Property 7. *Let* $n \equiv 0 \pmod 3$ *and* $c \in C_k(B)$. *Then if* $k \equiv 0 \pmod 3$, *the elements of c are pairwise equivalent modulo 3; otherwise, the elements of c are pairwise inequivalent modulo 3.*

Proof. By (4.2) of Property 2, $(0, k, \ell) \in C_k$ has the stated property. Hence, each $c \in C_k$ also does because C_k is obtained additively over $\mathbb{Z}_n$.

□

Property 8. *Given a cell* $(0, k, \ell) \in C_k$, $\ell = k/2$ *if k is even and* $\ell = (n+k)/2$ *if k is odd.*

Proof. If k is even,

$$\begin{aligned}\ell &\equiv k\left(\frac{n+1}{2}\right) \pmod n \\ &\equiv (k/2)(n+1) \pmod n \\ &\equiv k/2 \pmod n.\end{aligned}$$

As $k/2 \le n-1$, $\ell = k/2$. If k is odd,

$$\begin{aligned} & k \equiv k \pmod n \\ \iff\ & kn + k \equiv n + k \pmod n \\ \iff\ & k(n+1) \equiv n + k \pmod n \\ \iff\ & k\left(\frac{n+1}{2}\right) \equiv \frac{n+k}{2} \pmod n.\end{aligned}$$

Thus, since $(n+k)/2 \le n-1$, $\ell = (n+k)/2$. □

4.3.2 Recursive construction for orders $n \equiv 9 \pmod{18}$

Henceforth, we assume that all arithmetic is performed modulo n.

Lemma 7. *If $n \equiv 3 \pmod 6$ and $k \not\equiv 0 \pmod 3$, C_k can be partitioned into three LSPCs.*

Proof. By (4.2) of Property 2, write $c = (0, 2d\gamma/3, d\gamma/3)$ such that $2d\gamma/3 \equiv k \pmod n$, $\gamma \mid n$ (so that $0 \le \gamma < n$), and $d \not\equiv 0 \pmod 3$. Consider the set of cells $\mathcal{B}$ of C_k

$$\mathcal{B} = \bigcup_{i \in [0, \gamma/3 - 1]} \{(i, 2d\gamma/3 + i, d\gamma/3 + i)\}.$$

Then

$$\mathcal{L}_1 = \bigcup_{c \in \mathcal{B}} \bigcup_{i \in [0, n/\gamma - 1]} c \oplus i\gamma, \tag{4.4}$$

is an LSPC, which holds by $|\mathcal{L}_1| = \gamma/3 \cdot n/\gamma = n/3$, $\gamma \equiv 0 \pmod 3$, and Property 7. The set of symbols of the cells of $\mathcal{L}_1$ is

$$\bigcup_{i \in [0, \gamma/3 - 1]} \{d\gamma/3 + i, d\gamma/3 + \gamma + i, \ldots, d\gamma/3 + n - \gamma + i\}.$$

Hence,

$$\mathcal{L}_2 = \bigcup_{c \in \mathcal{L}_1} c \oplus \gamma/3, \text{ and}$$

$$\mathcal{L}_3 = \bigcup_{c \in \mathcal{L}_1} c \oplus 2\gamma/3$$

are LSPCs such that the sets of symbols of the cells of $\mathcal{L}_1$, $\mathcal{L}_2$, and $\mathcal{L}_3$ are pairwise disjoint. Thus, by Property 1, the $\mathcal{L}_i$'s partition C_k.

□

Theorem 15. *If the averaging latin square of order* n *has a Bose resolution whenever* $n \equiv 3, 15 \pmod{18}$, *then the averaging latin square of order* n *has a Bose resolution whenever* $n \equiv 9 \pmod{18}$.

Proof. The recursion proceeds as follows. Define $K = \{k \in [0, (n-1)/2] : k \not\equiv 0 \pmod 3\}$. Then for each $k \in K$, partition the cells of $C_k(B)$ into three LSPCs by applying Lemma 7. Now the remaining set of cells

$$\bigcup_{j \in [0,(n-1)/2] \cap \overline{K}} C_j$$

partitions into three row-column-symbol disjoint latin subsquares L_0, L_1, and L_2 such that the symbol set, row index set, and column index set of L_i are each equal to

$\{x \in [0, n-1] : x \equiv i \pmod 3\}$, and each L_i is isomorphic to the averaging latin square of order $n/3$. If $n/3 \equiv 3, 15 \pmod{18}$, merge the putative Bose resolutions of these three subsquares to obtain a Bose resolution for B. Otherwise, $n/3 \equiv 9 \pmod{18}$, so recurse on each of the subsquares.

□

4.3.3 Constructions for orders $n \equiv 3, 15 \pmod{18}$

We employ more elaborate methods to organize the cells of diagonal pairs $C_k(B)$ for which $k \equiv 0 \pmod 3$ into LSPCs. For any set of integers S, define $S + j = \{s + j : s \in S\}$.

Lemma 8. *Suppose that B is the averaging latin square of order $n \equiv 3, 15 \pmod{18}$. If $k \equiv 0 \pmod 3$, $(0, k, \ell) \in C_k(B)$, $\gamma = \gcd(k, n)$, and $m' \equiv \lfloor n/(3\gamma) \rfloor^{-1} \cdot \ell/\gamma \pmod{n/\gamma}$, then gcd$(m', n/\gamma) = 1$.*

Proof. We first compute $\lfloor n/(3\gamma) \rfloor^{-1}$ modulo n/γ:

$$\begin{aligned} \lfloor n/(3\gamma) \rfloor x &\equiv 1 \pmod{n/\gamma} \\ \iff x(n/\gamma - r)/3 &\equiv 1 \pmod{n/\gamma}, \text{ where } r \in \{1, 2\} \\ \iff x(n/\gamma - r) &\equiv 3 \pmod{n/\gamma} \\ \iff -xr &\equiv 3 \pmod{n/\gamma} \\ \iff x &\equiv -3r^{-1} \pmod{n/\gamma}. \end{aligned}$$

Thus, $m' \equiv -3r^{-1} \cdot \ell/\gamma \pmod{n/\gamma}$. Now $\gcd(3, n/k) = 1$ and if $r = 1$, then $\gcd(r^{-1}, \gamma) = 1$. If $r = 2$, then $r^{-1} \equiv \frac{1}{2}(n/\gamma + 1) \pmod{n/\gamma}$ and since $\gcd(n/\gamma, n/\gamma + 1) = 1$, again $\gcd(r^{-1}, n/k) = 1$. Finally, we claim that $\gcd(\ell/\gamma, n/\gamma) = 1$, implying that $\gcd(m', n/\gamma) = 1$, as desired. By Property 8, $\gcd(\ell/\gamma, n/\gamma) = \gcd(k/(2\gamma), n/\gamma) = 1$ if k is even and $\ell/\gamma = \frac{1}{2}(n/\gamma + k/\gamma)$ if k is odd. Suppose the latter holds and that there exists some $d > 1$ such that $d \mid \ell/\gamma$ and $d \mid n/\gamma$. Then $d \mid k/\gamma$, contradicting that $\gcd(n/\gamma, k/\gamma) = 1$, and thus $\gcd(\ell/\gamma, n/\gamma) = 1$.

□

Lemma 8 allows us to construct a class of PLSPCs.

Lemma 9. *Suppose that B is the averaging latin square of order $n \equiv 3, 15 \pmod{18}$, and that $C_k(B)$ is a diagonal pair with cell $c = (0, k, \ell)$, $k \equiv 0 \pmod 3$. Put $\gamma = \gcd(k, n)$. Then for $m \equiv 3m' \pmod{3n/\gamma}$, where $m' \equiv \ell/\gamma\lfloor n/(3\gamma)\rfloor^{-1} \pmod{n/\gamma}$, and any $d \not\equiv 0 \pmod 3$, $j \in \mathbb{Z}_3$, and $\alpha \in [0, \gamma/3 - 1]$ the set*

$$P_{k,d,j,\alpha} = \bigcup_{h \in [0, \lfloor n/(3\gamma)\rfloor - 1], i \in \mathbb{Z}_3} c \oplus (\alpha + \gamma/3(hm + id) + j\ell) \tag{4.5}$$

is a PLSPC of size $3\lfloor n/(3\gamma)\rfloor$ such that for distinct $j, j' \in \mathbb{Z}_3$, $P_{k,d,j,\alpha} \cap P_{k,d,j',\alpha} = \emptyset$.

Proof. By Property 8, $\ell = k/2$ if k is even and $\ell = (n+k)/2$ if k is odd. In either case, $k, \ell \equiv 0 \pmod{\gamma/3}$, and thus for all $\alpha \in [0, \gamma/3 - 1]$, the union of the rows, columns, and symbols comprising the cells of

$$\bigcup_{h \in [0, 3n/\gamma - 1]} c \oplus (\alpha + h\gamma/3)$$

is precisely the elements of $[0, n-1]$ congruent to α modulo $\gamma/3$. Hence, it suffices to prove the result for $P_{k,d,j,0}$. We claim that the set $P'_j \subset P_{k,d,j,0}$ given by

$$P'_j = \bigcup_{h \in [0, \lfloor n/(3\gamma)\rfloor - 1]} c \oplus (hm\gamma/3 + j\ell)$$

is a PLSPC. To establish this, consider a solution m' to the system of equations:

$$\begin{cases} \ell/\gamma \equiv m'\lfloor n/(3\gamma)\rfloor \pmod{n/\gamma} & (4.6a) \\ k/\gamma \equiv 2m'\lfloor n/(3\gamma)\rfloor \pmod{n/\gamma} & (4.6b) \end{cases}$$

with the constraint that $\gcd(m', n/\gamma) = 1$, so that m' generates $\mathbb{Z}_{n/\gamma}$. Then putting $m \equiv 3m' \pmod{3n/\gamma}$, the multiples of $m\gamma/3$ modulo n are pairwise distinct and thus if

$$S_\ell = \{\lfloor n/(3\gamma)\rfloor m\gamma/3 = \ell, (\lfloor n/(3\gamma)\rfloor + 1)m\gamma/3, \ldots, (2\lfloor n/(3\gamma)\rfloor - 1)m\gamma/3\},$$

then $S_\ell + j$ gives the set of symbols of the cells of P'_j, while the remaining multiples of $m\gamma/3$ modulo n, plus j give the rows and columns. The system (4.6) appears to be overdetermined, but subtracting the first equation from the second, and noting that $\ell \equiv k - \ell \pmod{n}$ by (4.2) of Property 2, $\ell/\gamma \equiv k/\gamma - \ell/\gamma \equiv m'\lfloor n/(3\gamma)\rfloor \pmod{n/\gamma}$; applying Lemma 8 gives the desired m'. Hence, P'_j is a PLSPC as claimed and thus because $\gamma d/3 \not\equiv 0 \pmod{3}$, then by Property 7, $P_{k,d,j,0}$ is also a PLSPC.

Finally, suppose that there exists some $(x_1, x_2, x_3) \in P_{k,d,j,0} \cap P_{k,d,j',0}$, with $j, j' \in \{0, 1, 2\}$ and $j > j'$, and suppose without loss of generality that $x_3 \equiv 0 \pmod{3}$. Then there exist $(y_1, y_2, y_3), (z_1, z_2, z_3) \in P'_0$ (and hence $y_3, z_3 \in S_\ell$) such that $x_3 \equiv y_3 + j\ell \equiv z_3 + j'\ell \pmod{n}$. Because $(j - j')\ell \equiv z_3 - y_3 \pmod{n}$, either

$$z_3 - y_3 \equiv \lfloor n/(3\gamma)\rfloor m\gamma/3 \pmod{n}, \text{ or}$$
$$z_3 - y_3 \equiv 2\lfloor n/(3\gamma)\rfloor m\gamma/3 \pmod{n}.$$

But neither $\lfloor n/(3\gamma)\rfloor m\gamma/3$ nor $2\lfloor n/(3\gamma)\rfloor m\gamma/3$ is a possible difference of any two elements of S_ℓ.

□

Given $n \equiv 3, 15 \pmod{18}$, $k, \beta \in [1, (n-1)/2]$, and a PLSPC $P \subset C_k$, a β-*completing set* for P is a set $S \subset C_\beta$ such that $P \cup S$ is an LSPC. More generally, given $\gamma = \gcd(k, n)$, $\alpha \in [0, \gamma/3 - 1]$, and

$$U_\alpha = \bigcup_{h \in [0, 3n/\gamma - 1]} (c \oplus (\alpha + h\gamma/3)),$$

a PLSPC $P \subset U_\alpha$ is (α, β)-*completable* if there exists some subset $S \subset C_\beta$, $|S| = n/\gamma - |P|$, such that $P' = P \cup S$ is a PLSPC satisfying

$$\bigcup_{c \in P'} c_{\{\}} = \{x \in [0, n-1] : x \equiv \alpha \pmod{\gamma/3}\}.$$

Such a set S is an (α, β)-*completing set* for P.

The proof of Lemma 10 describes a method, completely determined by the single parameter $d \not\equiv 0 \pmod 3$ in the lemma statement, of partitioning any C_k, $k \not\equiv 0 \pmod 3$, together with an LSPC of C_β, into four LSPCs. This procedure is the *standard method of handling* C_k *with parameter* d, and C_β the *completing diagonal pair* for C_k.

Lemma 10. *Suppose that* $n \equiv 3, 15 \pmod{18}$ *with* $n > 15$, $k \equiv 0 \pmod 3$, $\gamma = \gcd(k, n)$, $3n/\gamma > 15$, $\hat{c} = (0, k, \ell) \in C_k$, *and fix* $d \not\equiv 0 \pmod 3$, $\beta = \min\{\pm 2d\gamma/3 \pmod n\}$. *Then there exists a partition* π_k *of* C_k *into four PLSPCs and a partition* π_β *into four PLSPCs of some LSPC* $\mathcal{L}$ *of* C_β *of type (4.4) of Lemma 7, such that for each* $S_k \in \pi_k$, *there exists a unique* $S_\beta \in \pi_\beta$ *such that* S_β *is a* β*-completing set for* S_k.

Proof. For each $\alpha \in [0, \gamma/3 - 1]$ and $j \in \mathbb{Z}_3$, form the PLSPC $P_{k,d,j,\alpha}$ as in (4.5). Set

$$U_\alpha = \bigcup_{h \in [0, 3n/\gamma - 1]} \left(\hat{c} \oplus (\alpha + h\gamma/3)\right),$$

and $N_\alpha = U_\alpha \setminus \bigcup_{j \in \mathbb{Z}_3} P_{k,d,j,\alpha}$. For $j \in \mathbb{Z}_3$ define $\mathcal{Y}_j = \bigcup_{c \in P_{k,d,j,\alpha}} c_{\{\}}$, and set $Y = \bigcup_{j \in \mathbb{Z}_3} P_{k,d,j,\alpha}$ and $R_\alpha = \{x \in [0, n-1] : x \equiv \alpha \pmod{\gamma/3}\}$. Then $\mathcal{N}_j = R_\alpha \setminus \mathcal{Y}_j$ partitions into three sets $\mathcal{N}_{j,0}, \mathcal{N}_{j,1}$, and $\mathcal{N}_{j,2}$ such that $|\mathcal{N}_{j,0}| = |\mathcal{N}_{j,1}| = |\mathcal{N}_{j,2}|$ and $\mathcal{N}_{j,i}$ is the set of all elements of $\mathcal{N}_j$ congruent to i modulo 3. Suppose that $x \in \mathcal{N}_{j,\alpha \pmod 3}$; we claim that $x + hd\gamma/3 \pmod n \in \mathcal{N}_{j,\alpha + hd\gamma/3 \pmod 3}$ for all $h \in \{1, 2\}$. Suppose instead that $x + hd\gamma/3 \pmod n \in \mathcal{Y}_j$ for some $h \in \{1, 2\}$; then there exists some $i \in [0, \lfloor n/(3\gamma) \rfloor - 1]$ such that the cell $\hat{c} \oplus (\alpha + \gamma/3(hd + im) + j\ell)$ has $x + hd\gamma/3$

(mod n) as one of its coordinates. But then the cell $c = \hat{c} \oplus (\alpha + im\gamma/3 + j\ell)$ satisfies $c \in P_{k,d,j,\alpha}$ and has x as one of its coordinates, implying that $x \in \mathcal{Y}_j$, a contradiction. Now by Property 5, if the regular difference $\delta(C_{k'}) = \min\{d\gamma/3 \pmod n, -d\gamma/3 \pmod n\}$, then $k' = \beta$. Thus, by (4.3) of Property 2,

$$\begin{aligned} S_{\alpha,j} =& \{(x, x + 2d\gamma/3, x + d\gamma/3) : x \in \mathcal{N}_{j,\alpha \,(\mathrm{mod}\ 3)} \text{ and } x < x + 2d\gamma/3\} \\ &\cup \{(x + 2d\gamma/3, x, x + d\gamma/3) : x \in \mathcal{N}_{j,\alpha \,(\mathrm{mod}\ 3)} \text{ and } x > x + 2d\gamma/3\} \end{aligned}$$

is an (α, β)-completing set for $P_{k,d,j,\alpha}$.

Next we derive an (α, β)-completing set S_{N_α} for N_α. We treat two cases.

Case 1: $3n/\gamma \equiv 3 \pmod{18}$. Then $n/\gamma \equiv 1 \pmod 6$, and so

$$\begin{aligned} |Y| &= 9\lfloor n/(3\gamma) \rfloor \\ &= 9(n/\gamma - 1)/3 \\ &= 3n/\gamma - 3. \end{aligned}$$

Thus, $|N_\alpha| = 3$. Moreover, since $d\gamma/3 \not\equiv 0 \pmod 3$ and $m \equiv 0 \pmod 3$, we may write $N_\alpha = \{c_0, c_1, c_2\}$ such that the row, column, and symbol of cell c_i are equivalent to i modulo 3 for $i \in \mathbb{Z}_3$. Hence, $N_{d,\alpha}$ is a PLSPC. Additionally, we claim that $c_{i+\alpha \,(\mathrm{mod}\ 3)} = c_{\alpha \,(\mathrm{mod}\ 3)} \oplus id\gamma/3$ for $i \in \{1, 2\}$. For suppose to the contrary that $c_{\alpha \,(\mathrm{mod}\ 3)} \oplus id\gamma/3 \in Y$ for some $i \in \{1, 2\}$. Then there must exist some $h \in [0, \lfloor 3n/\gamma \rfloor - 1]$ and $j \in \mathbb{Z}_3$ such that

$$c_{\alpha \,(\mathrm{mod}\ 3)} \oplus id\gamma/3 = \hat{c} \oplus (\alpha + \gamma/3(hm + id) + j\ell).$$

But then $c_{\alpha \,(\mathrm{mod}\ 3)} \in Y$, since $c_{\alpha \,(\mathrm{mod}\ 3)} = \hat{c} \oplus (\alpha + hm\gamma/3 + j\ell)$, a contradiction. Hence, defining the set of 3-tuples

$$\begin{aligned} T_{\alpha,3} = & \{(x, x + 2d\gamma/3, x + d\gamma/3) : x \in c_{\alpha \,(\mathrm{mod}\ 3)_{\{\}}} \text{ and } x < x + 2d\gamma/3\} \\ & \cup \{(x + 2d\gamma/3, x, x + d\gamma/3) : x \in c_{\alpha \,(\mathrm{mod}\ 3)_{\{\}}} \text{ and } x > x + 2d\gamma/3\}, \end{aligned}$$

we have that $\bigcup_{c\in T_{\alpha,3}} c_{\{\}} = \bigcup_{c'\in N_\alpha} c'_{\{\}}$.

Case 2: $3n/\gamma \equiv 15 \pmod{18}$. Then $n/\gamma \equiv 5 \pmod 6$, and so

$$\begin{aligned}|Y| &= 9\lfloor n/(3\gamma)\rfloor \\ &= 9(n/\gamma - 2)/3 \\ &= 3n/\gamma - 6.\end{aligned}$$

Thus, $|N_\alpha| = 6$. Since $d\gamma/3 \not\equiv 0 \pmod 3$ and $m \equiv 0 \pmod 3$, we may write

$$N_\alpha = \{c_{0,0}, c_{0,1}, c_{1,0}, c_{1,1}, c_{2,0}, c_{2,1}\}$$

such that the row, column, and symbol of the cell $c_{i,j}$ are equivalent to i modulo 3 for all $i \in \mathbb{Z}_3$ and $j \in \{0,1\}$. Using the same argument as in the previous case, without loss of generality $c_{\alpha+i \,(\mathrm{mod}\ 3),j} = c_{\alpha\,(\mathrm{mod}\ 3),j} \oplus id\gamma/3$ for all $i \in \{1,2\}$, $j \in \{0,1\}$. In turn, the set of 3-tuples

$$\begin{aligned}T_{\alpha,15} = \{&(y, y+2d\gamma/3, y+d\gamma/3) : y \in c_{\alpha\,(\mathrm{mod}\ 3),0_{\{\}}} \cup c_{\alpha\,(\mathrm{mod}\ 3),1_{\{\}}} \text{ and } y < y+2d\gamma/3\} \\ &\cup \{(y+2d\gamma/3, y, y+d\gamma/3) : y \in c_{\alpha\,(\mathrm{mod}\ 3),0_{\{\}}} \cup c_{\alpha\,(\mathrm{mod}\ 3),1_{\{\}}} \text{ and } y > y+2d\gamma/3\}\end{aligned}$$

satisfies $\bigcup_{c\in T_{\alpha,15}} c_{\{\}} = \bigcup_{c'\in N_\alpha} c'_{\{\}}$.

R_α has size $3n/\gamma$, and since $\gamma/3 \not\equiv 0 \pmod 3$, it partitions into three sets $R_{\alpha,0}, R_{\alpha,1}$, and $R_{\alpha,2}$, such that $|R_{\alpha,0}| = |R_{\alpha,1}| = |R_{\alpha,2}|$ and $R_{\alpha,i}$ is the set of all elements of R_α congruent to i modulo 3. Thus, using (4.3) of Property 2,

$$\begin{aligned}\mathcal{P}_\alpha = &\{(x, x+2d\gamma/3, x+d\gamma/3) : x \in R_{\alpha,\alpha\,(\mathrm{mod}\ 3)} \text{ and } x < x+2d\gamma/3\} \\ &\cup\{(x+2d\gamma/3, x, x+d\gamma/3) : x \in R_{\alpha,\alpha\,(\mathrm{mod}\ 3)} \text{ and } x > x+2d\gamma/3\}\end{aligned}$$

is a PLSPC such that $\mathcal{P}_\alpha \subset C_\beta$ and $\bigcup_{c\in\mathcal{P}_\alpha}\{c_{\{\}}\}$ is a partition of R_α. Hence, whether $n \equiv 3 \pmod{18}$ or $n \equiv 15 \pmod{18}$, $S_{N_\alpha} = \mathcal{P}_\alpha \setminus T_{\alpha,3}$ or $S_{N_\alpha} = \mathcal{P}_\alpha \setminus T_{\alpha,15}$ is an (α,β)-completing set for N_α, respectively.

Define $\mathcal{Y} = \bigcup_{c \in N_\alpha} c_{\{\}}$ and $\mathcal{N} = R_\alpha \setminus \mathcal{Y}$. By Lemma 9, $|\mathcal{Y}_j| = 9\lfloor n/(3\gamma) \rfloor$ and if $3n/\gamma \equiv 3 \pmod{18}$, then $|\mathcal{Y}| = 9$; on the other hand, if $n \equiv 15 \pmod{18}$, then $|\mathcal{Y}| = 18$. In either case, $|\mathcal{Y}_j| + |\mathcal{Y}| > 3n/\gamma$ and thus by the pigeonhole principle, $R_\alpha = \mathcal{Y}_j \cup \mathcal{Y}$, so that $\mathcal{N}_j \cap \mathcal{N} = \emptyset$ for all $j \in \mathbb{Z}_3$. Now suppose there exists some $x \in R_\alpha$ such that $x \notin \mathcal{N}_0 \cup \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}$. Then $x \in \mathcal{Y}_0 \cap \mathcal{Y}_1 \cap \mathcal{Y}_2 \cap \mathcal{Y}$, which is impossible since by Property 1, x can only occur in at most three cells of C_k. Hence, R_α admits a partition into sets $\mathcal{N}_0, \mathcal{N}_1, \mathcal{N}_2$, and $\mathcal{N}$, and thus, since for each $j \in \mathbb{Z}_3$ the symbol of each cell of $S_{\alpha,j}$ belongs to $R_{\alpha,\alpha+d\gamma/3 \pmod 3}$, it must be that $S_{\alpha,0} \cup S_{\alpha,1} \cup S_{\alpha,2} \cup S_{N_\alpha} = \mathcal{P}_\alpha$.

We claim that $\mathcal{L} = \bigcup_{\alpha \in [0,\gamma/3-1]} \mathcal{P}_\alpha$ is an LSPC of C_β of type (4.4) of Lemma 7. As the cells of $\mathcal{P}_\alpha$, treated as 3-sets, partition R_α, $\mathcal{L}$ is an LSPC. Suppose that $z \in [0, \gamma/3 - 1]$. Then for each $j \in [0, n/\gamma - 1]$, since $\gamma \equiv 0 \pmod 3$, $z + j\gamma \equiv z \pmod 3$; this and the fact that $z + j\gamma \equiv z \pmod{\gamma/3}$ imply that $z + j\gamma \in R_{z,z \pmod 3}$. Thus, $d\gamma/3 + z + j\gamma$ is a symbol of some cell of $\mathcal{P}_z$.

Finally, putting

$$\pi_k = \bigcup_{j \in \mathbb{Z}_3} \left\{ \bigcup_{\alpha \in [0,\gamma/3-1]} P_{k,d,j,\alpha} \right\} \cup \left\{ \bigcup_{\alpha \in [0,\gamma/3-1]} N_\alpha \right\}$$

and

$$\pi_\beta = \bigcup_{j \in \mathbb{Z}_3} \left\{ \bigcup_{\alpha \in [0,\gamma/3-1]} S_{\alpha,j} \right\} \cup \left\{ \bigcup_{\alpha \in [0,\gamma/3-1]} S_{N_\alpha} \right\}$$

gives us the desired pair of partitions, where $\bigcup\limits_{\alpha \in [0,\gamma/3-1]} S_{\alpha,j} \in \pi_\beta$ is a completing set for $\bigcup_{\alpha \in [0,\gamma/3-1]} P_{k,d,j,\alpha} \in \pi_k$ for each $j \in \mathbb{Z}_3$ and $\bigcup\limits_{\alpha \in [0,\gamma/3-1]} S_{N_\alpha} \in \pi_\beta$ is a completing set for $\bigcup\limits_{\alpha \in [0,\gamma/3-1]} N_\alpha \in \pi_k$.

□

Let us demonstrate the standard method with a small example, reusing the notation in the proof of Lemma 10.

Example 3. Suppose that $n = 21$ and $k = 3$ so that $(0, 3, 12) \in C_3$ with $\ell = 12$. Put $d = 1$. Then $\gamma = \gcd(k, n) = 3$,

$$m' \equiv \ell/\gamma \lfloor n/(3\gamma) \rfloor^{-1} \equiv 4 \lfloor 21/9 \rfloor^{-1} \equiv 2 \pmod{7},$$

$m \equiv 6 \pmod{21}$, and $\beta = \min\{\pm 2d\gamma/3 \pmod{n}\} = 2$. Hence,

$$P_{3,1,0,0} = \{(0,3,12), (1,4,13), (2,5,14), (6,9,18), (7,10,19), (8,11,20)\},$$

$$P_{3,1,0,1} = \{(12,15,3), (13,16,4), (14,17,5), (0,18,9), (1,19,10), (2,20,11)\}, \text{ and}$$

$$P_{3,1,0,2} = \{(3,6,15), (4,7,16), (5,8,17), (9,12,0), (10,13,1), (11,14,2)\}.$$

Thus,

$$\mathcal{Y}_0 = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,18,19,20\},$$

$$\mathcal{Y}_1 = \{0,1,2,3,4,5,9,10,11,12,13,14,15,16,17,18,19,20\}, \text{ and}$$

$$\mathcal{Y}_2 = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17\}.$$

Since $R_0 = \bigcup_{i \in [0, 3n/\gamma - 1]} i\gamma/3 = [0, 20]$,

$$\mathcal{N}_0 = R_0 \setminus \mathcal{Y}_0 = \{15, 16, 17\},$$

$$\mathcal{N}_1 = R_0 \setminus \mathcal{Y}_0 = \{6, 7, 8\}, \text{ and}$$

$$\mathcal{N}_2 = R_0 \setminus \mathcal{Y}_0 = \{18, 19, 20\}.$$

Thus,

$$S_{0,0} = \{(15, 17, 16)\},$$

$$S_{0,1} = \{(6, 8, 7)\}, \text{ and}$$

$$S_{0,2} = \{(18, 20, 19)\}$$

are $(0,2)$-completing sets for $P_{3,1,0,0}$, $P_{3,1,0,1}$, and $P_{3,1,0,2}$, respectively. Next, $U_0 = C_3$, and thus $N_0 = U_0 \setminus \bigcup_{j\in\mathbb{Z}_3} P_{k,d,j,a} = \{(15,18,6),(16,19,7),(17,20,8)\}$. Thus,

$$T_{0,3} = \{(15,17,16),(18,20,19),(6,8,7)\}, \text{ and}$$
$$\mathcal{P}_0 = \{(0,2,1),(3,5,4),(6,8,7),(9,11,10),(12,14,13),(15,17,16),(18,20,19)\};$$

hence, $S_{N_0} = \mathcal{P}_0 \backslash T_{0,3} = \{(0,2,1),(3,5,4),(9,11,10),(12,14,13)\}$ is a $(0,2)$-completing set for N_0. By inspection

$$\pi_3 = \{P_{3,1,0,0}, P_{3,1,0,1}, P_{3,1,0,2}, N_0\}, \text{ and}$$
$$\pi_2 = \{S_{0,0}, S_{0,1}, S_{0,2}, S_{N_0}\}$$

are the desired partitions of C_3 and C_2, respectively.

The only kind of diagonal pair C_k, $k \not\equiv 0 \pmod 3$, that is not handled by the standard method is one satisfying $3n/\gcd(k,n) = 15$; we now treat this exception.

Construction 1. We construct a Bose resolution of the second kind for the averaging latin square B of order 15. We give a Bose resolution of the second kind. The first part of the resolution is the collection of LSPCs:

$$\{(0,3,9),(1,7,4),(2,5,11),(12,14,13),(6,10,8)\}$$
$$\{(6,9,0),(7,13,10),(8,11,2),(3,5,4),(1,12,14)\}$$
$$\{(0,12,6),(2,14,8),(4,13,1),(9,11,10),(3,7,5)\}$$
$$\{(3,6,12),(4,10,7),(5,8,14),(0,2,1),(9,13,11)\}$$
$$\{(1,10,13),(9,12,3),(11,14,5),(6,8,7),(0,4,2)\}$$
$$\{(1,3,2),(4,6,5),(7,9,8),(10,12,11),(0,13,14)\}$$
$$\{(2,4,3),(5,7,6),(8,10,9),(11,13,12),(1,14,0)\}, \text{ and}$$
$$\{(3,6,4),(5,9,7),(8,12,10),(0,11,13),(3,14,1)\}.$$

Second, partition each of $C_1(B)$, $C_5(B)$, and $C_7(B)$ into LSPCs by applying Lemma 7 to get the remaining LSPCs of the resolution. Third, the remaining set of cells of B above the main diagonal partitions into five PLSPCs, each of size four. We now present these PLSPCs $\hat{P}_i$, adjoining to each a 3-set $\hat{T}_i$ of the points not covered by the corresponding PLSPC, such that the collection of these 3-sets gives a partition of $[0, 14]$:

$$\hat{P}_1 = \{(3,9,6),(4,7,13),(5,11,8),(10,14,12)\} \text{ and } \hat{T}_1 = \{0,1,2\};$$
$$\hat{P}_2 = \{(6,12,9),(7,10,1),(8,14,11),(2,13,0)\} \text{ and } \hat{T}_2 = \{3,4,5\};$$
$$\hat{P}_3 = \{(0,9,12),(2,11,14),(10,13,4),(1,5,3)\} \text{ and } \hat{T}_3 = \{6,7,8\};$$
$$\hat{P}_4 = \{(1,13,7),(3,12,0),(5,14,2),(4,8,6)\} \text{ and } \hat{T}_4 = \{9,10,11\};$$
$$\hat{P}_5 = \{(0,6,3),(1,4,10),(2,8,5),(7,11,9)\} \text{ and } \hat{T}_5 = \{12,13,14\}.$$

For any integer $x > 1$, write its prime factorization as $x = p_1 \cdot p_2 \cdot \cdots \cdot p_q$, and define the multiset $\mathsf{pf}(x) = \{p_1, \ldots, p_q\}$. If $x \in \{0, 1\}$, define $\mathsf{pf}(x) = \emptyset$. For any $n \equiv 3, 15 \pmod{18}$ and $m \equiv 0 \pmod 3$ such that $\mathsf{pf}(m/3) \subset \mathsf{pf}(n/3)$, let B_m and B_n be the averaging latin squares of orders m and n, respectively. (If $m = 0$, then B_m is the empty averaging square). The *diagonal pair indices of B_m in B_n*, denoted $D_m(B_n)$, is the empty set if $m = 0$ and otherwise the set $\{n/m, 2n/m, \ldots, (m-1)n/m\}$ of $(m-1)/2$ diagonal pair indices of B_n. For each $\alpha \in [0, n/m - 1]$, define the map $\varphi_\alpha : [0, m-1] \to \{\alpha, \alpha + n/m, \alpha + 2n/m, \ldots, \alpha + (m-1)n/m\}$, where $\varphi_\alpha(i) = in/m + \alpha$. Extend φ_α naturally to 3-tuples by applying the map to each component; i.e., if (x, y, z) satifies $x, y, z \in [0, m-1]$, then $\varphi_\alpha((x, y, z)) = (\varphi_\alpha(x), \varphi_\alpha(y), \varphi_\alpha(z))$. Further, for any $S \subset \{(x, y, z) : x, y, z \in [0, m-1]\}$, define $\varphi_\alpha(S) = \{\varphi_\alpha((x, y, z)) : (x, y, z) \in S\}$.

Lemma 11. *Let B_n be the averaging latin square of order $n \equiv 3, 15 \pmod{18}$, and B_m the averaging latin square of order m, $m \equiv 0 \pmod 3$, such that $\mathsf{pf}(m/3) \subset \mathsf{pf}(n/3)$.*

Then for each diagonal pair $C_{k'}(B_m)$, there exists a corresponding $k \in D_m(B_n)$ such that $C_k(B_n)$ partitions into n/m isomorphic copies of $C_{k'}(B_m)$.

Proof. For $k' \in [1,(m-1)/2]$ and $\alpha \in [0, n/m-1]$, define

$$U_{k',\alpha} = \bigcup_{i\in[0,m-1]} c_{n,k'n/m} \oplus_n (\alpha + in/m),$$

where $c_{n,k'n/m} = (0, k'n/m, \ell) \in C_{k'n/m}(B_n)$. Moreover, let $c_{m,k'} = (0, k', \ell') \in C_{k'}(B_m)$.

There are four cases in total: (1) k' is even and $i \in [0, m-k'-1]$, (2) k' is even and $i \in [m-k', m-1]$, (3) k' is odd and $i \in [0, m-k'-1]$, and (4) k' is odd and $i \in [m-k', m-1]$. If case (1) holds, then by (4.3) of Property 2 and Property 8,

$$\begin{aligned}\varphi_\alpha(c_{m,k'} \oplus_m i) &= \varphi_\alpha((i, k'+i, k'/2+i)) \\ &= (in/m+\alpha, n/m(k'+i)+\alpha, n/m(k'/2+i)+\alpha) \\ &= c_{n,k'n/m} \oplus_n (\alpha + in/m).\end{aligned}$$

Treating the remaining cases in like fashion, we see that $\varphi_\alpha(C_{k'}(B_m)) = U_{k',\alpha}$, so that the φ_α's are the desired isomorphisms.

□

Corollary 4. *Let B be the averaging latin square of order $n \equiv 3, 15 \pmod{18}$ such that $n > 15$ and $n = 15t$, and let B_{15} be the averaging latin square of order 15. Let $D_{15}(B)$ denote the diagonal pair indices of B_{15} in B, so that*

$$\begin{aligned}U &= \bigcup_{j\in D_{15}(B)} C_j(B) \\ &= \bigcup_{i\in[1,7]} C_{it}(B).\end{aligned}$$

Then there exists a partition of U into a set $\mathcal{L} = \{L_1, \ldots, L_{17}\}$ of LSPCs, and a set $\mathcal{P} = \{P_1, \ldots, P_5\}$ of PLSPCs of size $4n/15$ such that there exists a partition $\mathcal{T} = \{T_1, \ldots, T_{n/3}\}$ of $[0, n-1]$ into triples and a partition $\mathcal{T}' = \{T'_1, \ldots, T'_5\}$ of $\mathcal{T}$ into sets (of triples) of size $n/15$ such that for all $i \in [1, 5]$,

$$\bigcup_{c \in P_i} c_{\{\}} \cup \bigcup_{T \in T'_i} T = [0, n-1].$$

Proof. For each $\alpha \in [0, t-1]$, set

$$U_\alpha = \bigcup_{c \in \{(0, it, B_{0,it}) : i \in [1,7]\}, j \in [0,14]} c \oplus (\alpha + jt).$$

Then by Lemma 11,

$$\varphi_\alpha \left(\bigcup_{k \in [1,7]} C_k(B_{15}) \right) = U_\alpha.$$

By Property 8, for all even $i \in [1, 7]$, $B_{0,it} = it/2$ and for all odd $i \in [1, 7]$, $B_{0,it} = (n + it)/2$. In either case, $it \equiv B_{0,it} \equiv 0 \pmod{t}$. Therefore, the union of the cells (treated as 3-sets) of U_α is

$$R_\alpha = \{x \equiv \alpha \pmod{t} : x \in [0, n-1]\}.$$

Let $\hat{\mathcal{L}} = \{\hat{L}_1, \ldots, \hat{L}_{17}\}$, $\hat{\mathcal{P}} = \{\hat{P}_1, \ldots, \hat{P}_5\}$, and $\hat{\mathcal{T}} = \{\hat{T}_1, \ldots, \hat{T}_5\}$ be the 17 LSPCs, the 5 PLSPCs (each of size 4), and the 5 triples (which partition [0,14]), respectively, that comprise the Bose resolution of B_{15} given in Construction 1.

Let us now partition U. For each $i \in [1, 17]$, put

$$L_i = \bigcup_{\alpha \in [0, t-1]} \varphi_\alpha(\hat{L}_i).$$

The union of the cells of each $\varphi_\alpha(\hat{L}_i)$ is equal to R_α, and thus L_i is an LSPC (of B). For each $j \in [1,5]$, put

$$P_j = \bigcup_{\alpha\in[0,t-1]} \varphi_\alpha(\hat{P}_j), \text{ and}$$
$$T'_j = \bigcup_{\alpha\in[0,t-1]} \varphi_\alpha(\hat{T}_j).$$

As

$$\bigcup_{c\in\varphi_\alpha(\hat{P}_j)} c_{\{\}} \cup \varphi_\alpha(\hat{T}_j) = R_\alpha,$$

the result follows.

□

Define $K = \{k \in [1,(n-1)/2] : k \equiv 0 \pmod 3\}$. Given distinct diagonal pairs $C_k, C_{k'}$, with $k, k' \in K$, suppose we apply the standard method to C_k and $C_{k'}$ with parameters d and d', respectively, such that $d \gcd(k,n) \equiv d' \gcd(k',n) \pmod n$. Then C_k and $C_{k'}$ share the same completing diagonal pair; in fact, the same LSPC of that completing diagonal pair is used by the standard method to complete the four PLSPCs of C_k and the four PLSPCs of $C_{k'}$ to LSPCs. We call this a *collision between C_k and $C_{k'}$*. To produce a Bose resolution for B_n when $5 \nmid n$, we wish to apply the standard method to each diagonal pair of $S = \{C_k : k \in K'\}$, such that there is no collision between any two $C_k, C_{k'} \in S$. To produce a Bose resolution for B_n when $5 \mid n$, we wish to apply the standard method to each diagonal pair of $S = \{C_k : k \in K \setminus D_{15(B_n)}\}$ such that there is no collision between any two $C_k, C_{k'} \in S$.

We accomplish this by applying Hall's marriage theorem. A *transversal* for $\mathcal{M}$ is an injective function $\rho : \mathcal{M} \to U$ such that $\rho(S) \in S$ for all $S \in \mathcal{M}$, and $\mathcal{M}$ satisfies the *marriage condition* if for each submultiset $\mathcal{H} \subseteq \mathcal{M}$, $|\mathcal{H}| \leq \left|\bigcup_{H\in\mathcal{H}} H\right|$.

Theorem 16 (Hall's marriage theorem [31])**.** *Suppose that $\mathcal{M}$ is a multiset of finite subsets of some universe U. Then $\mathcal{M}$ has a transversal if and only if it satisfies the marriage condition.*

Let $K = \{k \in [1,(n-1)/2] : k \equiv 0 \pmod 3\}$ and for each $k \in K$, write $\mu_k = \gcd(k,n)/3$. If q is a positive integer, then a subset N of the least residue system modulo q is *negative-free modulo* q if for any $x \in N$, $-x \pmod q \notin N$. For any integer m such that $3 \mid m$ and $\mathsf{pf}(m) \subset \mathsf{pf}(n)$ with B_m the averaging latin square of order m, recall that $D_m(B_n)$ is the set of diagonal pair indices of B_m in B_n. Let

$$T_{\mu_k,D_m(B_n)} = \{d \in [1, n/\mu_k - 1] : d \not\equiv 0 \pmod 3, d \notin D_m(B_n)\},$$

so that the set $S = \{d\mu_k : d \in T_{\mu_k,D_m(B)}\}$ gives all the multiples of μ_k modulo n not congruent to 0 modulo 3, minus those in $D_m(B)$. As $n/\mu_k \equiv 0 \pmod 3$, for any $d \in T_{\mu_k,D_m(B_n)}$, $n/\mu_k - d \not\equiv 0 \pmod 3$. Hence, $-d \pmod{n/\mu_k} \in T_{\mu_k,D_m(B_n)}$, and thus

$$T'_{\mu_k,D_m(B_n)} = \{d \in [1,(n/\mu_k - 1)/2] : d \not\equiv 0 \pmod 3, d \notin D_m(B_n)\}$$

is a maximal subset of $T_{\mu_k,D_m(B_n)}$ that is negative-free modulo n/μ_k. Consequently, $F_k^{-D_m(B_n)} = \{d\mu_k : d \in T'_{\mu_k,D_m(B_n)}\}$ is a maximal subset of S that is negative-free modulo n. Therefore, by Property 3, $F_k^{-D_m(B_n)}$ gives precisely the set of all regular differences of all the distinct completing diagonal pairs, excluding those indexed by $D_m(B_n)$, which we may use in the standard method of handling C_k. That is, for each $d\mu_k \in F_k^{-D_m(B_n)}$, if one handles C_k using the standard method with parameter d, the resulting completing diagonal pair is $C_{2d\mu_k}$, since the regular difference of $C_{2d\mu_k}$ is $\delta(C_{2d\mu_k}) = d\mu_k$. Accordingly, we call $F_k^{-D_m(B_n)}$ the *completing candidate set for k with forbidden diagonal pairs $D_m(B_n)$*. The *family of all completing candidate sets with forbidden diagonal pairs $D_m(B_n)$* is the set family $\mathcal{F}^{-D_m(B_n)} = \bigcup_{k \in K \setminus D_m} F_k^{-D_m(B_n)}$. If

$D_m(B_n) = \emptyset$, we simply write F_k to denote the completing candidate set for k and $\mathcal{F}$ to denote the family of all completing candidate sets.

For any $\mathcal{H} = \{F_{k_1}^{-D_m(B_n)}, \ldots, F_{k_m}^{-D_m(B_n)}\} \subseteq \mathcal{F}^{-D_m(B_n)}$, the *multiple closure of* $\mathcal{H}$ *over* K *minus* $D_m(B_n)$, denoted $\mathsf{mcl}_{K \setminus D_m(B_n)}(\mathcal{H})$, is the subset of $\mathcal{F}^{-D_m(B_n)}$ given by

$$\mathsf{mcl}_{K \setminus D_m(B_n)}(\mathcal{H}) = \{F_k^{-D_m(B_n)} \in \mathcal{F}^{-D_m(B_n)} : \mu_{k_i} \mid \mu_k \text{ for some } i \in [1, m]\},$$

or equivalently,

$$\mathsf{mcl}_{K \setminus D_m(B_n)}(\mathcal{H}) = \bigcup_{j \in [1,m]} \{F_{3i\mu_{k_j}}^{-D_m(B_n)} : i \in [1, \lfloor n/(6\mu_{k_j}) \rfloor], 3i\mu_{k_j} \notin D_m(B_n)\}. \quad (4.7)$$

In words, $\mathsf{mcl}_{K \setminus D_m(B_n)}(\mathcal{H})$ gives us every completing candidate set of $\mathcal{F}^{-D_m(B_n)}$ that is subscripted by a multiple of μ_{k_j} in $K \setminus D_m(B_n)$ for each $j \in [1, m]$. If $\mathcal{H} = \{F_k^{-D_m(B_n)}\}$, we write $\mathsf{mcl}_{K \setminus D_m(B_n)}(F_k^{-D_m(B_n)})$. $\mathcal{H} \subseteq \mathcal{F}^{-D_m(B_n)}$ is *multiple-closed over* K *minus* $D_m(B_n)$ if $\mathsf{mcl}_{K \setminus D_m(B_n)}(\mathcal{H}) = \mathcal{H}$.

We now verify that each candidate set $F_k^{-D_m(B_n)} \in \mathcal{F}^{-D_m(B_n)}$ excludes the regular differences of the diagonal pairs indexed by $D_m(B_n)$.

Lemma 12. *Suppose that* $n \equiv 3, 15 \pmod{18}$ *and* $m \equiv 0 \pmod 3$*, such that* $\mathsf{pf}(m/3) \subset \mathsf{pf}(n/3)$*. Let* B_n *and* B_m *be the averaging latin squares of orders* n *and* m*, respectively, and let* $D_m(B_n)$ *be the diagonal pair indices of* B_m *in* B_n*. If* $D'_m(B_n)$ *is the set of all diagonal pair indices of* $D_m(B_n)$ *not congruent to* 0 *mod* 3*, then* $\{C_i(B_n) : i \in D'_m(B_n)\} = \{C_{\delta(C_i)}(B_n) : i \in D'_m(B_n)\}$.

Proof. Recall that $D_m(B_n) = \bigcup_{i \in [1,(m-1)/2]} in/m$, so that

$$D'_m(B_n) = \bigcup_{i \in [1,(m-1)/2], i \not\equiv 0 \pmod 3} in/m.$$

By (4.2) of Property 2 and Property 3, the desired result holds provided that there exists a map $f : D'_m(B_n) \to \{\pm 2^{-1} \pmod{n}\}$ such that

$$\bigcup_{xn/m \in D'_m(B_n)} f(xn/m) \cdot xn/m \,(\text{mod } n) = D'_m(B_n),$$

or equivalently, a map $g : [1, (m-1)/2] \to \{\pm 2^{-1} \pmod{m}\}$ such that

$$\bigcup_{x \in [1,(m-1)/2]} g(x) \cdot x \,(\text{mod } m) = [1, (m-1)/2].$$

Let us then derive such a g. First, suppose that $xn/m \in D'_m(B_n)$ such that x is even. Then

$$\begin{aligned} 2^{-1} \cdot xn/m &\equiv (n+1)/2 \cdot xn/m \,(\text{mod } n) \\ &\equiv x/2 \cdot (n+1) \cdot n/m \,(\text{mod } n) \\ &\equiv x/2 \cdot n/m \,(\text{mod } n); \end{aligned}$$

thus, $2^{-1} \cdot x \equiv x/2 \pmod{m}$. Second, if $xn/m \in D'_m(B_n)$ such that x is odd, then

$$\begin{aligned} -2^{-1} \cdot xn/m &\equiv -1 \cdot 2^{-1} \cdot xn/m \,(\text{mod } n) \\ &\equiv 2^{-1} \cdot -x \cdot n/m \,(\text{mod } n) \\ &\equiv (n+1)/2 \cdot (n-x) \cdot n/m \,(\text{mod } n) \\ &\equiv (n-x)/2 \cdot n/m \,(\text{mod } n); \end{aligned}$$

thus, $-2^{-1} \cdot x \equiv (m-x)/2 \pmod{m}$. Now put $E = \{x \in [1, (m-1)/2] : x \text{ even}\}$ and $O = \{x \in [1, (m-1)/2] : x \text{ odd}\}$, and let $g(x) = 2^{-1} \pmod{m}$ if $x \in E$ $g(x) = -2^{-1} \pmod{m}$ if $x \in O$. Consequently,

$$\begin{aligned} \bigcup_{x \in E} g(x) \cdot x \,(\text{mod } m) &= \bigcup_{x \in E} x/2 \,(\text{mod } m) \\ &= [1, |E|], \end{aligned}$$

while

$$\begin{aligned}\bigcup_{x\in O} g(x)\cdot x \pmod{m} &= \bigcup_{x\in O}(m-x)/2 \pmod{m}\\ &= [|E+1|,(m-1)/2].\end{aligned}$$

□

Given a multiset S and any element $x \in S$, let $m_S(x)$ the *multiplicity of x in S* is the number of times that x occurs in S. For any two multisets S_1 and S_2, the *multiset union of S_1 and S_2* is the multiset for which each element has multiplicity equal to the maximum of its multiplicities in S_1 and S_2. For any two integers $x, y > 1$, the intersection of the set of multiples of x and the set of multiples of y is the set of multiples of the product of the elements of the multiset union of $\mathsf{pf}(x)$ and $\mathsf{pf}(y)$.

Henceforth, we assume that $n \equiv 3, 15 \pmod{18}$, $m \equiv 0 \pmod 3$, $\mathsf{pf}(m/3) \subset \mathsf{pf}(n/3)$, B_n is the averaging latin square of order n, $K = \{k \in [1,(n-1)/2] : k \equiv 0 \pmod 3\}$, and $\mu_k = \gcd(k,n)/3$ for $k \in K$.

Lemma 13. *For any divisor d of n satisfying $3 \nmid d$, $\lfloor n/(6d)\rfloor = (n-3d)/(6d)$.*

Proof. Because $n/6 = (n-3)/6 + 1/2$, where $(n-3)/6$ is an integer,

$$\begin{aligned}\lfloor n/(6d)\rfloor &= \lfloor (n/d-3)/6+1/2\rfloor\\ &= (n/d-3)/6\\ &= n/(6d)-3/6\\ &= (n-3d)/(6d).\end{aligned}$$

□

Lemma 14. *For $k \in K$, $\bigcup_{F_j \in \mathsf{mcl}_K(F_k)} F_j = F_k$.*

Proof. If $F_j \in \mathsf{mcl}_K(F_k)$, by definition $\mu_k \mid \mu_j$, and thus $F_j \subset F_k$. □

Lemma 15. *For $k \in K$, suppose that $F_k \in \mathcal{F}$ is the completing candidate set for k. Then*

$$2 \cdot |\mathsf{mcl}_K(F_k)| + 1 = \left| \bigcup_{F_j \in \mathsf{mcl}_K(F_k)} F_j \right|.$$

Proof. By Lemma 14 $|\bigcup_{F_j \in \mathsf{mcl}_K(F_k)} F_j| = |F_k| = n/(3\mu_k)$. By (4.7), $\mathsf{mcl}_K(F_k) = \{F_{3i\mu_k} : i \in [1, \lfloor n/(6\mu_k) \rfloor]\}$. Hence, by Lemma 13, $|\mathsf{mcl}_K(F_k)| = (n - 3\mu_k)/(6\mu_k)$.

□

Lemma 16. *For any pair of completing candidate sets $F_j^{-D_m(B_n)}, F_k^{-D_m(B_n)} \in \mathcal{F}^{-D_m(B_n)}$ with forbidden diagonal pairs $D_m(B_n)$ such that $\mu_j, \mu_k > 1$ and $\mathsf{pf}(\mu_k) \cup \mathsf{pf}(\mu_j) \neq \mathsf{pf}(n/3)$,*

$$\mathsf{mcl}_{K \setminus D_m(B_n)}(F_j^{-D_m(B_m)}) \cap \mathsf{mcl}_{K \setminus D_m(B_n)}(F_k^{-D_m(B_n)}) = \mathsf{mcl}_{K \setminus D_m(B_n)}(F_\ell^{-D_m(B_n)}),$$

where $F_\ell^{-D_m(B_n)} \in \mathcal{F}^{-D_m(B_n)}$ and μ_ℓ is the product of the elements of the multiset union of $\mathsf{pf}(\mu_k)$ and $\mathsf{pf}(\mu_j)$.

Proof. Let $h \in \{j, k\}$. By (4.7),

$$\mathsf{mcl}_{K \setminus D_m(B_n)}(F_h^{-D_m(B_n)}) = \{F_{3i\mu_h}^{-D_m(B_n)} : i \in [1, \left\lfloor \frac{n}{6\mu_h} \right\rfloor], 3i\mu_h \notin D_m(B_n)\},$$

or equivalently, letting p be the product of the elements of the multiset union of $\mathsf{pf}(\mu_k)$ and $\mathsf{pf}(\mu_j)$,

$$\mathsf{mcl}_{K \setminus D_m(B_n)}(F_h^{-D_m(B_n)}) = \{F_{3ip}^{-D_m(B_n)} : i \in [1, \frac{\mu_h}{p} \left\lfloor \frac{n}{6\mu_h} \right\rfloor], 3ip \notin D_m(B_n)\}.$$

Applying Lemma 13,

$$\mathsf{mcl}_{K \setminus D_m(B_n)}(F_h^{-D_m(B_n)}) = \{F_{3ip}^{-D_m(B_n)} : i \in [1, \frac{n - 3\mu_h}{6p}], 3ip \notin D_m(B_n)\}.$$

Now $3p \mid n$ and by assumption p is sufficiently small that there must exist some $\ell \in K \setminus D_m(B_n)$ such that $p = \mu_\ell = \gcd(\ell, n)/3$. Hence,

$$\begin{aligned}
&\mathsf{mcl}_{K\setminus D_m(B_n)}(F_j^{-D_m(B_n)}) \cap \mathsf{mcl}_{K\setminus D_m(B_n)}(F_k^{-D_m(B_n)}) \\
&= \{F_{3i\mu_\ell}^{-D_m(B_n)} : i \in \left[1, \min\left\{\frac{n-3\mu_j}{6\mu_\ell}, \frac{n-3\mu_k}{6\mu_\ell}\right\}\right], 3i\mu_\ell \notin D_m(B_n)\} \\
&= \{F_{3i\mu_\ell}^{-D_m(B_n)} : i \in [1, \frac{n-3\mu_\ell}{6\mu_\ell}], 3i\mu_\ell \notin D_m(B_n)\} \\
&= \mathsf{mcl}_{K\setminus D_m(B_n)}(F_\ell^{-D_m(B_n)}),
\end{aligned}$$

where the second-to-last equality follows from the fact that $\frac{n-3\mu_\ell}{6\mu_\ell} \leq \min\left\{\frac{n-3\mu_j}{6\mu_\ell}, \frac{n-3\mu_k}{6\mu_\ell}\right\}$ and the subscripting set $[1, \frac{n-3\mu_\ell}{6\mu_\ell}]$ is the minimum-sized set that yields every multiple of μ_ℓ in K.

□

Lemma 17. *Suppose $D_m(B_n) \neq \emptyset$, and for $k \in K \setminus D_m(B_n)$, that $F_k^{-D_m(B_n)} \in \mathcal{F}^{-D_m(B_n)}$ is the completing candidate set for k with forbidden diagonal pairs $D_m(B_n)$. Then*

$$2 \cdot |\mathit{mcl}_{K\setminus D_m(B_n)}(F_k^{-D_m(B_n)})| = \left| \bigcup_{H \in \mathit{mcl}_{K\setminus D_m(B_n)}(F_k^{-D_m(B_n)})} H \right|.$$

Proof. Let $F_k \in \mathcal{F}$ be the completing candidate set for k (with no forbidden diagonal pairs). By definition, $D_m(B_n) = \bigcup_{i\in[1,(m-1)/2]} in/m$. Moreover,

$$(m-1)/2 \cdot n/m = n/2 - n/(2m) < (n-1)/2, \text{ while}$$

$$(m+1)/2 \cdot n/m = n/2 + n/(2m) > (n-1)/2.$$

Hence, $F_{3n/m} \in \mathcal{F}$ such that $\mathsf{mcl}_K(F_{3n/m}) \subset \bigcup_{i\in D_m(B_n)}\{F_i\}$, implying

$$\begin{aligned}
\mathsf{mcl}_K(F_k) \cap \bigcup_{i\in D_m(B_n)} \{F_i\} &= \mathsf{mcl}_K(F_k) \cap \mathsf{mcl}_K(F_{3n/m}) \\
&= \mathsf{mcl}_K(F_\ell),
\end{aligned}$$

where by Lemma 16, $F_\ell \in \mathcal{F}$ with μ_ℓ being the product of the elements of $\mathsf{pf}(\mu_k) \cup \mathsf{pf}(\mu_{3n/m} = n/m)$. By Lemma 14,

$$\bigcup_{F_j \in \mathsf{mcl}_K(F_k)} F_j \cap D_m(B_n) = F_k \cap D_m(B_n) = F_\ell.$$

Next,

$$\mathsf{mcl}_{K \setminus D_m(B_n)}(F_k^{-D_m(B_n)}) = \{M \setminus D_m(B_n) : M \in \mathsf{mcl}_K(F_k)\} \setminus \bigcup_{i \in D_m(B_n)} \{F_i \setminus D_m(B_n)\},$$

implying both

$$\begin{aligned}|\mathsf{mcl}_{K \setminus D_m(B_n)}(F_k^{-D_m(B_n)})| &= |\mathsf{mcl}_K(F_k)| - |\mathsf{mcl}_K(F_k) \cap \bigcup_{i \in D_m(B_n)} \{F_i\}| \\ &= |\mathsf{mcl}_K(F_k)| - |\mathsf{mcl}_K(F_\ell)|,\end{aligned}$$

and, together with Lemma 14,

$$\left| \bigcup_{H \in \mathsf{mcl}_{K \setminus D_m(B_n)}(F_k^{-D_m(B_n)})} H \right| = F_k \setminus D_m(B_n) = |F_k| - |F_\ell|.$$

Applying Lemma 15 twice, we have that

$$\begin{aligned}&2|\mathsf{mcl}_K(F_k)| + 1 - (2|\mathsf{mcl}_K(F_\ell)| + 1) = |F_k| - |F_\ell| \\ \iff\ &2(|\mathsf{mcl}_K(F_k)| - |\mathsf{mcl}_K(F_\ell)|) = |F_k| - |F_\ell|,\end{aligned}$$

as desired.

□

Lemma 18. *For any collection* $\mathcal{H} = \{F_{k_1}^{-D_m(B_n)}, \ldots, F_{k_m}^{-D_m(B_n)}\} \subseteq \mathcal{F}^{-D_m(B_n)}$ *of completing candidate sets for* k *with forbidden diagonal pairs* $D_m(B_n)$,

$$|mcl_{K \setminus D_m(B_n)}(\mathcal{H})| \leq \left| \bigcup_{H \in mcl_{K \setminus D_m(B_n)}(\mathcal{H})} H \right|.$$

Proof. First, suppose there exists some $i \in [1, m]$ such that $\mu_{k_i} = 1$. Then

$$\begin{aligned}
|\mathsf{mcl}_{K \setminus D_m(B_n)}(\mathcal{H})| &\leq |K \setminus D_m(B_n)| \\
&= \lfloor (n-1)/6 \rfloor - \lfloor (m-1)/6 \rfloor \\
&\leq (n-m)/3 \\
&= |F_{k_i}^{-D_m(B_n)}| \leq \left| \bigcup_{H \in \mathsf{mcl}_{K \setminus D_m(B_n)}(\mathcal{H})} H \right|.
\end{aligned}$$

Otherwise, we compute the size of $\mathsf{mcl}_{K \setminus D_m(B_n)}(\mathcal{H})$ using the inclusion-exclusion principle:

$$\begin{aligned}
&|\mathsf{mcl}_{K \setminus D_m(B_n)}(\mathcal{H})| \\
&= \left| \bigcup_{i=1}^{m} \mathsf{mcl}_{K \setminus D_m(B_n)}(F_{k_i}^{-D_m(B_n)}) \right| \\
&= \sum_{i=1}^{m} (-1)^{i+1} \left(\sum_{1 \leq h_1 < \cdots < h_i \leq m} |\mathsf{mcl}_{K \setminus D_m(B_n)}(F_{k_{h_1}}^{-D_m(B_n)}) \cap \cdots \cap \mathsf{mcl}_{K \setminus D_m(B_n)}(F_{k_{h_i}}^{-D_m(B_n)})| \right).
\end{aligned}$$

For each $i \in [1, m]$ and for each i-subset $S = \{F_{k_{h_1}}^{-D_m(B_n)}, \ldots, F_{k_{h_i}}^{-D_m(B_n)}\} \subseteq \mathcal{H}$, either (1) we can "collapse" the intersections of the inclusion-exclusion expression by (repeated) application of Lemma 16 to yield

$$\bigcap_{j=1}^{i} \mathsf{mcl}_{K \setminus D_m(B_n)}(F_{k_{h_j}}^{-D_m(B_n)}) = \mathsf{mcl}_{K \setminus D_m(B_n)}(F_{\sigma(S)}^{-D_m(B_n)}),$$

where $F_{\sigma(S)}^{-D_m(B_n)} \in \mathcal{F}$ is the candidate set for $\sigma(S)$ with forbidden diagonal pairs $D_m(B_n)$ such that $\mu_{\sigma(S)}$ is the product of the elements of the multiset union $\bigcup_{j \in [1,i]} \mathsf{pf}(\mu_{k_{h_j}})$, or (2)

$$\bigcap_{j=1}^{i} \mathsf{mcl}_{K \setminus D_m(B_n)}(F_{k_{h_j}}^{-D_m(B_n)}) = \emptyset,$$

which occurs precisely when $\bigcup_{j\in[1,i]} \mathsf{pf}(\mu_{k_{h_j}}) = \mathsf{pf}(n/3)$. Let $\mathcal{S}$ be the set of all subsets of $\mathcal{H}$ that satisfy case (1). Then there exists a map $\tau : \mathcal{S} \to \{-1, 1\}$ such that

$$|\mathsf{mcl}_{K\setminus D_m(B_n)}(\mathcal{H})| = \sum_{S\in\mathcal{S}} \tau(S)|\mathsf{mcl}_{K\setminus D_m(B_n)}(F_{\sigma(S)}^{-D_m(B_n)})|,$$

and since $\bigcup_{F_j\in\mathsf{mcl}_K(F_k)} F_j = F_k$ for any $k \in K$,

$$\left|\bigcup_{H\in\mathsf{mcl}_{K\setminus D_m(B_n)}(\mathcal{H})} H\right| = \sum_{S\in\mathcal{S}} \tau(S)|F_{\sigma(S)}^{-D_m(B_n)}|.$$

Hence, by Lemmas 15 and 17,

$$\sum_{S\in\mathcal{S}} \tau(S)|F_{\sigma(S)}| \geq 2 \cdot \sum_{S\in\mathcal{S}} \tau(S)|\mathsf{mcl}_K(F_{\sigma(S)})|.$$

□

Corollary 5. *For any collection $\mathcal{H} \subseteq \mathcal{F}^{-D_m(B_n)}$ of completing candidate sets with forbidden diagonal pairs $D_m(B_n)$ that is not multiple-closed over K, $|\mathcal{H}| \leq \left|\bigcup_{H\in\mathcal{H}} H\right|$.*

Proof. Suppose to the contrary that there exists some $\mathcal{H} \subseteq \mathcal{F}^{-D_m(B_n)}$ such that $|\mathcal{H}| > \left|\bigcup_{H\in\mathcal{H}} H\right|$. But $|\bigcup_{G\in\mathsf{mcl}_{K\setminus D_m(B_n)}(\mathcal{H})} G| = |\bigcup_{H\in\mathcal{H}} H|$; also $|\mathsf{mcl}_{K\setminus D_m(B_n)}(\mathcal{H})| \geq |\mathcal{H}|$. Thus, $|\mathsf{mcl}_{K\setminus D_m(B_n)}(\mathcal{H})| > |\bigcup_{G\in\mathsf{mcl}_{K\setminus D_m(B_n)}(\mathcal{H})} G|$, contradicting Lemma 18. □

Theorem 17. *The family $\mathcal{F}^{-D_m(B_n)}$ of all completing candidate sets with forbidden diagonal pairs $D_m(B_n)$ satisfies the marriage condition.*

Proof. Any $\mathcal{H} \subseteq \mathcal{F}^{-D_m(B_n)}$ is either multiple-closed over $K \setminus D_m(B_n)$, or it isn't. Hence, the result follows from Lemma 18 and Corollary 5.

□

We now have all the machinery to construct Bose resolutions.

Theorem 18. *For all $n \equiv 3, 15 \pmod{18}$ with $n > 15$, the averaging latin square B of order n admits a Bose resolution.*

Proof. There are two cases to treat.

Case 1: $5 \nmid n$. Define $K = \{k \in [1,(n-1)/2] : k \equiv 0 \pmod 3\}$, and for each $k \in K$, write $\mu_k = \gcd(k,n)/3$. Let $\mathcal{F} = \bigcup_{k\in K}\{F_k\}$ be the family of all completing candidate sets. Each $F_k \in \mathcal{F}$ gives the set of regular differences of all possible completing diagonal pairs for C_k. By Theorem 17, $\mathcal{F}$ meets the marriage condition, and so by Theorem 16, there exists a transversal $\rho : \mathcal{F} \to [1,(n-1)/2] \setminus K$ used to prevent a collision between two diagonal pairs $C_k, C_{k'}$.

Fix $k \in K$, and define $c_k = (0, k, B_{0,k}) \in C_k$ and $\beta_k = \min\{\pm 2\rho(F_k)\mu_k\}$. Apply the standard method with parameter $\rho(F_k)$ to handle C_k, giving us a partition $\pi_k = \{\mathcal{P}_{k,0}, \mathcal{P}_{k,1}, \mathcal{P}_{k,2}, \mathcal{P}_{k,3}\}$ of C_k into four PLSPCs, a partition π_{β_k} into four PLSPCs of some LSPC $\mathcal{L}_{\beta_k,0}$ of C_{β_k} of type (4.4) of Lemma 7, and an injective map $f_k : \pi_k \to \pi_{\beta_k}$ such that (the disjoint union) $\mathcal{P}_{k,i} \cup f_k(\mathcal{P}_{k,i})$ is an LSPC for $i \in [0,3]$. Next, apply Lemma 7 to partition C_{β_k} into three LSPCs $\mathcal{L}_{\beta_k,0}, \mathcal{L}_{\beta_k,1}$, and $\mathcal{L}_{\beta_k,2}$. The Bose resolution $\mathcal{R}$ of B is

$$\mathcal{R} = \bigcup_{k\in K}\left(\bigcup_{i\in[0,3]}\{\mathcal{P}_{k,i} \cup f_k(\mathcal{P}_{k,i})\} \cup \{\mathcal{L}_{\beta_k,1}, \mathcal{L}_{\beta_k,2}\}\right).$$

Case 2: $n = 15t$. Let $D_{15}(B)$ be the set of diagonal pair indices of the averaging latin square of order 15 in B_n. Put $U = \bigcup_{i\in[1,7]} C_{it}(B)$, and apply Corollary 4 to handle U to obtain part of the Bose resolution $\mathcal{R}'$ for B. Let $\mathcal{F}^{-D_{15}(B)} = \bigcup_{k\in K\setminus D_m} F_k^{-D_{15}(B)}$ be the family of all completing candidate sets with forbidden diagonal pairs $D_{15}(B)$. Each $F_k^{-D_{15}(B)} \in \mathcal{F}^{-D_{15}(B)}$ gives the set of regular differences of all possible completing diagonal pairs for C_k, excluding the diagonal pairs indexed by $D_{15}(B)$. By Theorem 17, $\mathcal{F}^{-D_{15}(B)}$ satisfies the marriage condition, and thus by Theorem 16, there exists a transversal $\rho' : \mathcal{F}^{-D_{15}(B)} \to [1,(n-1)/2] \setminus (K \cup D_{15}(B))$. To obtain the remainder of $\mathcal{R}'$, analogous to the first case, apply the standard method to each of the diagonal pairs indexed by $K \setminus D_{15}(B)$, using ρ' to prevent a collision between any two such diagonal pairs.

□

4.3.4 Main Result

Suppose that $n \equiv 3, 9, 15 \pmod{18}$, which by Theorem 14 is necessarily the only possible order of an averaging latin square with a Bose resolution. Applying Construction 1 when $n = 15$, Theorem 15 when $n \equiv 9 \pmod{18}$, and Theorem 18 otherwise, we obtain a Bose resolution to which we apply Theorem 13 to obtain a resolution of the corresponding Bose-averaging triple system, thus establishing our main result.

Theorem 19. *Every resolvable Bose triple system of order v has $v \equiv 9 \pmod{18}$ and the Bose-averaging triple system of order $v \equiv 9 \pmod{18}$ is resolvable.*

Chapter 5

MINSUM AND DIFFSUM BOUNDS FOR $S(2,4,v)$S

Applying Theorem 1, the optimal MinSum and DiffSum of an $S(2,4,v)$ are $3v/2$ and $v-4$, respectively. The general problem of producing point-labelled $S(2,4,v)$s with MinSum and DiffSum "close" to these optima appears to be much more difficult than the analogous problem for Steiner triple systems. The reasons, we suspect, are twofold. One, the great majority of constructions of $S(2,4,v)$s are recursive, and it is not clear how one might go about labelling the ingredients of a recursive construction such that the resulting design is well-labelled. Indeed, if we are especially demanding and define "well-labelled" to be within a constant summand of the optimal MinSum or DiffSum, then every well-labeled Steiner (triple) system in the literature is directly constructed. Two, the direct constructions that do exist are, to our knowledge, all based on difference families. While designs produced by difference families can admit good *block* labellings (see Chapter 6), it seems that some of their properties make it prohibitively difficult to point-label them well.

With these obstacles in mind, we take in this chapter an approach in the spirit of Lemma 1, constructing $S(2,4,v)$s with (special) large independent sets to derive bounds for the major point-labelling metrics.

5.1 Preliminaries

Two set systems $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ are *isomorphic (with isomorphism φ)* if there exists a bijection $\varphi : X \to Y$ such that

$$\{\varphi(A) : A \in \mathcal{A}\} = \mathcal{B},$$

where $\varphi(A)$ is the image of A under φ. An *automorphism* of a set system $(X, \mathcal{B})$ is an isomorphism from X onto itself. Moreover, an *automorphism group* of $\mathcal{B}$ is a group of automorphisms of $\mathcal{B}$; the *full* automorphism group of $\mathcal{B}$ is the group of all automorphisms of $\mathcal{B}$.

Given an $S(2, 4, v)$ $D = (V, \mathcal{B})$, a *blocking set* X of D is an independent set of D whose complement $V \setminus X$ is also an independent set of D. An *arc* of D is an independent set A of D with the property that no three points of A are contained in a block of $\mathcal{B}$. A *secant* of an arc A of D is a block which contains exactly two points of A, while a *tangent* of A is a block which contains exactly one point of A. An arc A is *complete* if any point in V is contained in at least one secant of A. Equivalently, a complete arc is an arc which cannot be (properly) contained in some other arc. If for each point of a complete arc A there exists a unique tangent of A containing x, then A is an *oval*. An arc in an $S(2, 4, v)$ with maximum size $\frac{v+2}{3} = r + 1$ is a *maximum arc* or *hyperoval*. A hyperoval H is *not* an oval, since every block intersects in either two or zero points with H [47]. Accordingly, a *maximum oval* is an oval with maximum size $(v - 1)/3$. The necessary condition for the existence of a hyperoval is $v \equiv 4 \pmod{12}$ [21], and was proved to be sufficient in [29] and independently in [41].

If $\{S_1, \ldots, S_n\}$ is a partition of a *symbol set* S, an $\{S_1, \ldots, S_n\}$-*Room frame* is an $|S| \times |S|$ array F, indexed by S, satisfying:

1. every cell of F is either empty or contains a 2-subset of S,

Table 5.1: A Room frame of type 2^5

				79	68		35	24	
		69	78			34			25
59	48							17	06
				16	07	58	49		
26						19	08		37
	27	18	09					36	
	39	04	15	28					
38					29			05	14
		57	46		13	02			
47	56			03			12		

2. the subarrays $S_i \times S_i$ are empty for $i \in [1, n]$ (these subarrays are *holes*),
3. each symbol $x \notin S_i$ occurs exactly once in each row s and exactly once in each column s for any $s \in S_i$, and
4. the 2-subsets of S occuring in F are those $\{s, t\}$, where $(s, t) \in (S \times S) \setminus \bigcup_{i=1}^{n}(S_i \times S_i)$.

The *type* of a Room frame F is the multiset $\{|S_i| : i \in [1, n]\}$. Exponential notation is used to give the type; that is, a Room frame has type $t_1^{u_1} t_2^{u_2} \ldots t_k^{u_k}$ if there are u_i S_js of size t_i for $i \in [1, k]$. A Room frame of type 2^5 on symbol set $[0, 9]$ is given in Table 5.1. A Room frame is *skew* if for any pair of cells (s, t) and (t, s) in $(S \times S) \setminus \bigcup_{i=1}^{n}(S_i \times S_i)$, precisely one is empty.

5.2 MinSum and DiffSum Bounds via Arcs

For blocksize $k > 3$, replacing "independent sets" with "arcs" in the statement of Lemma 1, and as in the proof of that lemma, assigning the lowest-valued set of labels to one arc and the highest-valued set of labels to the other arc, we get the following result.

Lemma 19. *When an $S(2,k,v)$ D with $k>3$ has two disjoint arcs of sizes α and β, then $\mathsf{MinSum}(D) \geq \alpha(k-2)+1$ and $\mathsf{MaxSum}(D) \leq 2v-3+(k-2)(v-\beta)-\binom{k-1}{2}$, so that*

$$\mathsf{DiffSum}(D) \leq 2v-3+(k-2)(v-\beta)-\binom{k-1}{2}-\alpha(k-2)-1.$$

To optimize the bounds of Lemma 19, we would like the arc sizes α and β to be as large as possible. To this end, we use the following result.

Lemma 20. *Given $v \equiv 1 \pmod{12}$, an arc A of size $\frac{v-1}{3}=r$ in an $S(2,4,v)$ $D=(V,\mathcal{B})$ is a maximum oval.*

Proof. As $v \equiv 1 \pmod{12}$, A must be a complete arc. Fix a point $x \in A$. Then for $y \in V \setminus \{x\}$, either $\{x,y\}$ occurs in a secant or a tangent of A. Hence, for $z \in A \setminus \{x\}$, $\{x,z\}$ must occur in exactly one secant of A, implying that x occurs in exactly $r-1$ secants of A, leaving $2r+1-2(r-1)=3$ points of $V \setminus A$ that do not occur together with x in a secant of A. These three points together with x constitute the unique tangent of A that contains x. □

In light of Lemmas 19 and 20, we propose two questions:

Q1. For $v \equiv 1 \pmod{12}$, does there exist an $S(2,4,v)$ with a pair of disjoint maximum ovals?

Q2. For $v \equiv 4 \pmod{12}$, does there exist an $S(2,4,v)$ with a pair of disjoint hyperovals?

The answer to Q1 is "yes", save for one possible exception. In [49, 50] Rodger et al. give for $v \equiv 1,4 \pmod{12}$ a construction, using certain skew Room frames as ingredients, for weakly 3-chromatic $S(2,4,v)$ designs. It turns out that with a cosmetic modification of the construction, we can produce for all $v \equiv 1 \pmod{12}$ with $v > 49$

an $S(2,4,v)$ with a pair of disjoint maximum ovals. First, though, we require a pair of results.

Theorem 20 ([11, 65]). *The necessary conditions for the existence of a skew Room frame of type t^u; namely, that $u \geq 4$ and $t(u-1)$ is even, are also sufficient except for $(t,u) \in \{(1,5),(2,4)\}$, and with possible exceptions:*

1. *$t \equiv 2 \pmod 4$ and $u = 4$;*
2. *$t \in \{17, 19, 23, 29, 31\}$.*

Lemma 21. *The unique $S(2,4,13)$ has a disjoint pair of maximum ovals.*

Proof. Inspecting the unique $S(2,4,13)$ of Table 5.2, $\{4,5,6,9\}$ and $\{8,\mathrm{a},\mathrm{b},\mathrm{c}\}$ are disjoint maximum ovals. □

We now present our light modification of the construction of Rodger et al.

Lemma 22. *For all $v \equiv 1 \pmod{12}$ with $v > 49$, there exists an $S(2,4,v)$ with a pair of disjoint maximum ovals.*

Proof. Write $v = 12s + 1$, and let F be a skew Room frame of type 2^s on symbol set $S = [1, 2s]$, which exists by Theorem 20. Let $\mathcal{H}$ be the set of holes of F. Form an $S(2,4,v)$ D on point set $V = (S \times [0,5]) \cup \{\infty\}$ and block set $\mathcal{B}$ consisting of two types of blocks:

1. For each $H \in \mathcal{H}$, let $\mathcal{B}$ contain a sub-$S(2,4,13)$ on points $(H \times [0,5]) \cup \{\infty\}$, naming the points such that $H \times \{0,3\}$ and $H \times \{1,4\}$ are (disjoint) maximum ovals, which is possible by Lemma 21.
2. For each $\{x,y\} \subset S$ with $\{x,y\} \neq H$ for all $H \in \mathcal{H}$, and for $j \in [0,5]$, define the block $\{(x,j),(y,j),(r,j+1),(c,j+4)\} \in \mathcal{B}$, where $\{x,y\}$ occurs in cell (r,c) of F, with addition in the second coordinate performed modulo 6.

Verifying that D is in fact an $S(2,4,v)$:

1. For each pair of points $P = \{(a,i),(b,i)\}$, $\{a,b\}$ occurs in exactly one cell of F.
2. For each pair of points $P = \{(a,i),(b,i+1)\}$, symbol a occurs exactly once in row b.
3. For each pair of points $P = \{(a,i),(b,i+3)\}$, F is skew, ensuring that exactly one of cells (a,b) and (b,a) is filled.
4. For each pair of points $P = \{(a,i),(b,i+4)\}$, symbol a occurs exactly once in column b.

Hence, every pair of points occurs in exactly one block of $\mathcal{B}$, as desired. Finally, $S \times \{0,3\}$ and $S \times \{1,4\}$ are (disjoint) hyperovals, for the multiset of second coordinates of any $B \in \mathcal{B}$ of type 2 intersects in two points with some set in $A = \{\{0,3\},\{1,4\},\{2,5\}\}$ and two points with some other set in A. The remaining blocks, each belonging to a sub-$S(2,4,13)$ with appropriately-named points, are either secants or tangents of $S \times \{0,3\}$ and $S \times \{1,4\}$. □

Lemma 23. *For all* $v \equiv 1 \pmod{12}$*, except possibly* $v = 37$*, there exists an* $S(2,4,v)$ *with a pair of disjoint maximum ovals.*

Proof. By Lemmas 21 and 22, it suffices to prove that there exists an $S(2,4,25)$ and $S(2,4,49)$, each having a pair of disjoint maximum ovals. The desired $S(2,4,25)$ is given in Table 5.2 (the first one in the list of all 18 nonisomorphic $S(2,4,25)$ designs given in [16]), having a pair of disjoint maximum ovals $\{0,1,3,4,6,7,\mathrm{l},\mathrm{n}\}$ and $\{9,\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{d},\mathrm{e},\mathrm{j},\mathrm{k}\}$.

We construct the desired $S(2,4,49)$ using WFC. The master GDD $(X,\mathcal{G},\mathcal{A})$ is the 4-GDD of type 3^5 that results from deleting point 0 and all the blocks that contain it

Table 5.2: The unique $S(2,4,13)$ and $S(2,4,16)$, and an $S(2,4,25)$

0000111223345
1246257364789
385a46b57689a
9c7ba8cb9cabc

00000111122223333456
147ad456945684567897
258be7b8cc79a98abbac
369cfadefefbddcfefed

00000 0 00 1 11111122222 2 233333 4 444555 5 66677 8 8 9 9aabbi l
13456 7 c e 3 4578cd34568 d e468bh 6 79f78a g 79b9a a b c ddecejm
298df b hk e a6g9kf7c9af k g5cgf i h dgi f ch i 8ejj c j d f hgfghkn
iaolgmjnmbohnljonblhmjjdlknmeklnekmkinlimimonooloo

from the unique $S(2,4,16)$ of Table 5.2, so that the array $M = (m_{i,j})$ with $i \in [1,5]$ and $j \in [1,3]$:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 5 \\ 8 & 7 & 9 \\ \mathrm{c} & \mathrm{a} & \mathrm{b} \\ \mathrm{d} & \mathrm{e} & \mathrm{f} \end{bmatrix}$$

is such that each of its rows is a group of $\mathcal{G}$ and each block of $\mathcal{A}$ intersects in precisely two points with two of its columns. The ingredient GDD is any 4-GDD of type 3^4 that results from deleting a point and all of its containing blocks from the unique $S(2,4,13)$; hence, for each $A \in \mathcal{A}$, there exists a 4-GDD

$$(A \times \{0,1,2\}, \{\{x\} \times \{0,1,2\} : x \in A\}, \mathcal{B}_A)$$

of type 3^4. Applying WFC with weight 3, the resulting 4-GDD of type 9^5 is $D = (Y, \mathcal{H}, \mathcal{B})$, where $Y = X \times \{0,1,2\}$, $\mathcal{H} = \{G \times \{0,1,2\} : G \in \mathcal{G}\}$, and $\mathcal{B} = \bigcup_{A \in \mathcal{A}} \mathcal{B}_A$.

It is routine to verify that $O_1 = \{0,1,2,5\}$ and $O_2 = \{3,4,7,9\}$ are maximum ovals of the unique $S(2,4,13)$ as presented in Table 5.2, say $D_{13} = (Z, \mathcal{B}_{13})$, such that the block $B = \{1,7,\mathrm{b},\mathrm{c}\} \in \mathcal{B}_{13}$ satisfies $B \cap O_1 = \{1\}$ and $B \cap O_2 = \{7\}$. Now for each $G \in \mathcal{G}$, write $G = \{m_{i,1}, m_{i,2}, m_{i,3}\}$, and let

$$\varphi_G : [0,9] \cup \{\mathrm{a},\mathrm{b},\mathrm{c}\} \to G \times \{0,1,2\} \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}$$

be a bijection with:

1. $\varphi_G(1) = \infty_1$, $\varphi_G(7) = \infty_2$, and $\varphi_G(\{\mathrm{b},\mathrm{c}\}) = \{\infty_3, \infty_4\}$;
2. $\varphi_G(O_1 \setminus \{1\}) = m_{i,1} \times \{0,1,2\}$; and
3. $\varphi_G(O_2 \setminus \{7\}) = m_{i,2} \times \{0,1,2\}$.

Then $(Y \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}, \mathcal{C})$ is an $S(2,4,49)$ with a pair of disjoint maximum ovals

$$\left(\bigcup_{i \in [1,5]} m_{i,1} \times \{0,1,2\} \right) \cup \{\infty_1\}, \text{ and}$$

$$\left(\bigcup_{i \in [1,5]} m_{i,2} \times \{0,1,2\} \right) \cup \{\infty_2\},$$

where

$$\mathcal{C} = \mathcal{B} \cup \bigcup_{G \in \mathcal{G}} \varphi_G(\mathcal{B}_{13}).$$

□

The answer to Q2 is “no”, save for the trivial $S(2,4,4)$.

Lemma 24. *For all $v \equiv 4 \pmod{12}$ with $v > 4$, no $S(2,4,v)$ contains a disjoint pair of hyperovals.*

Proof. Suppose to the contrary that for some $v \equiv 4 \pmod{12}$ with $v > 4$, there exists an $S(2,4,v)$ $D = (V, \mathcal{B})$ that contains a pair (A_1, A_2) of disjoint hyperovals, and put $C = V \setminus (A_1 \cup A_2)$ and $r = (v-1)/3$. Let Q_1 denote the number of blocks $B \in \mathcal{B}$ such that $|B \cap A_1| = |B \cap C| = 2$, Q_2 the number of blocks $B \in \mathcal{B}$ such that $|B \cap A_2| = |B \cap C| = 2$, and Q_3 the number of blocks $B \in \mathcal{B}$ such that $|B \cap C| = 4$. Then

$$\begin{aligned} 4Q_1 &= |A_1||C| = (r+1)(r-1), \\ 4Q_2 &= |A_2||C| = (r+1)(r-1), \text{ and} \\ Q_1 + Q_2 + 6Q_3 &= \binom{|C|}{2} = (r-1)(r-2)/2. \end{aligned}$$

Hence,

$$\begin{aligned} &(r^2-1)/2 + 6Q_3 = (r-1)(r-2)/2 \\ \iff &Q_3 = (1-r)/4, \end{aligned}$$

so that $Q_3 < 0$, which is absurd. □

However, the second-best state of affairs holds: For $v \equiv 4 \pmod{12}$, there exists an $S(2,4,v)$ with a disjoint hyperoval and arc of size $(v-1)/3$. This is a consequence of the following property of the $S(2,4,v)$ designs of [29, 41], the *Greig-Rosa-Ling* (or *GRL*) $S(2,4,v)$s:

Property 9. *Given a GRL $S(2,4,v)$ D, there exist three hyperovals H_1, H_2, and H_3 of D satisfying $H_1 \cap H_2 \cap H_3 = \{c\}$ such that every block of D containing c intersects in exactly one point with each H_i.*

For all but one admissible order of an $S(2,4,v)$, we are now equipped to give the strongest-possible application of Lemma 19.

Theorem 21. *For $v \equiv 1 \pmod{12}$, except possibly $v = 37$, there exists an $S(2,4,v)$ D with $\mathsf{MinSum}(D) \geq (2v+4)/3$ and $\mathsf{MaxSum}(D) \leq (10v-16)/3$, so that $\mathsf{DiffSum}(D) \leq (8v-20)/3$. For $v \equiv 4 \pmod{12}$, there exists an $S(2,4,v)$ D with $\mathsf{MinSum}(D) \geq (2v+7)/3$ and $\mathsf{MaxSum}(D) \leq (10v-16)/3$, so that $\mathsf{DiffSum}(D) \leq (8v-23)/3$.*

Proof. Apply Lemma 19 using the $S(2,4,v)$ designs of Lemma 23 and the GRL $S(2,4,v)$s, where each of the former has a pair of disjoint maximum ovals and each of the latter has a disjoint hyperoval and arc of size $(v-1)/3$. □

5.3 MinSum and DiffSum Bounds via Blocking Sets

Given an $S(2,4,v)$ $D = (V, \mathcal{B})$, a blocking set X of D is *equitable* if the size of X and its complement differ by at most 1. Then just as the strongest application of Lemma 19 occurs with a pair of disjoint hyperovals or maximum ovals, so the strongest application of Lemma 1 for DiffSum occurs with an equitable blocking set and its complement. Applying Lemma 1 as prescribed, we get:

Lemma 25. *When an $S(2,4,v)$ D has an equitable blocking set, then $\mathsf{MinSum}(D) \geq \lfloor v/2 \rfloor + 3$ and $\mathsf{MaxSum}(D) \leq 4(v-1) - 3 - \lceil v/2 \rceil$, so that $\mathsf{DiffSum}(D) \leq 3v - 10$.*

Thus, the sole fact that an equitable blocking set and its complement are each larger than a hyperoval (and a maximum oval) does not conduce to a better DiffSum bound than the ones of Theorem 21. But is there some way to merge the ideal property that no block can intersect in more than two points with an arc and the ideal property that an equitable blocking set has larger size than any arc to produce better bounds than those offered in Theorem 21? Indeed, these two properties can be integrated by applying with special ingredients a modificiation of the construction of Hoffman, Lindner, and Phelps [33], the original version of which is used to produce an $S(2,4,v)$ with an equitable blocking set for all $v \equiv 1, 4 \pmod{12}$ except $v \in \{37, 40, 73\}$.

A *nested* 3-GDD is a 3-GDD $D = (X, \mathcal{G}, \mathcal{A})$ equipped with a *nesting*, which is a map $\alpha : \mathcal{A} \to X$ such that

$$\bigcup_{A \in \mathcal{A}} \{A \cup \{\alpha(A)\}\}$$

is the block set of a $(4,2)$-GDD on X. This $(4,2)$-GDD is the *underlying* GDD of D. Henceforth, we identify D as a 4-tuple $(X, \mathcal{G}, \mathcal{A}, \alpha)$ and if U is the underlying GDD of D, we let $\mathfrak{A}(U)$ denote the full automorphism group of U.

Lemma 26. *Let $(X, \mathcal{G}, \mathcal{A}, \alpha)$ be a nested 3-GDD with underlying GDD U. Then for each $\sigma \in \mathfrak{A}(U)$, $(X, \mathcal{G}, \sigma(\mathcal{A}), \sigma \circ \alpha)$ is a nested 3-GDD.*

Proof. $D = (X, G, \sigma(\mathcal{A})^+)$, where $\sigma(\mathcal{A})^+ = \{\sigma(A) \cup \{\sigma(\alpha(A))\} : A \in \mathcal{A}\}$, is a $(4,2)$-GDD. Hence, it suffices to prove that $E = (X, \mathcal{G}, \sigma(\mathcal{A}))$ is a 3-GDD. Suppose to the contrary that E is not a 3-GDD. Then there exists a pair of points $P \subset X$ with $P \not\subseteq G$ for all $G \in \mathcal{G}$ such that P is not contained in any block of $\sigma(\mathcal{A})$. Thus, since $|\sigma(\mathcal{A})| = |\mathcal{A}|$, there must exist some other pair of points $P' \subset X$ such that P' is contained in at least two blocks of $\sigma(\mathcal{A})$, say B_1 and B_2, but then $|\sigma^{-1}(B_1) \cap \sigma^{-1}(B_2)| \geq 2$, contradicting that $(X, G, \mathcal{A})$ is a 3-GDD. □

Two distinct automorphisms of $\mathfrak{A}(U)$ may yield the "same" nested 3-GDD. To formalize this notion of "sameness", we define a binary relation $\sim_{\mathfrak{A}(U)}$ on $\mathfrak{A}(U)$, where $\sigma \sim_{\mathfrak{A}(U)} \tau$ (i.e., σ and τ are *nesting equivalent relative to* U) iff for each pair of blocks $S = \{x, y, z, \alpha(\{x, y, z\})\}$ and $T = \{a, b, c, \alpha(\{a, b, c\})\}$ of U such that $\sigma(S) = \tau(T)$, $\sigma(\alpha(\{x, y, z\})) = \tau(\alpha(\{a, b, c\}))$. Conversely, if $\sigma \not\sim_{\mathfrak{A}(U)} \tau$, then σ and τ are *nesting inequivalent relative to* U. By extension, if σ and τ are nesting equivalent

Figure 5.1: The Stinson ingredient GDD: A nested 3-GDD of Type 2^4. The adjoined point to each triple defined by the nesting occurs to the right of the vertical bar.

$$\text{groups}: \{1_0, 1_1\}, \{2_0, 2_1\}, \{3_0, 3_1\}, \{4_0, 4_1\}$$

$$\text{blocks}: \begin{array}{ccc|c} 1_0 & 2_1 & 3_0 & 4_1 \\ 1_0 & 2_0 & 4_1 & 3_1 \\ 1_0 & 3_1 & 4_0 & 2_1 \\ 2_0 & 3_0 & 4_0 & 1_0 \end{array} \qquad \begin{array}{ccc|c} 1_1 & 2_0 & 3_1 & 4_0 \\ 1_1 & 2_1 & 4_0 & 3_0 \\ 1_1 & 3_0 & 4_1 & 2_0 \\ 2_1 & 3_1 & 4_1 & 1_1 \end{array}$$

(nesting inequivalent) relative to U, then the nested 3-GDDs $(X, \mathcal{G}, \sigma(\mathcal{A}), \sigma \circ \alpha)$ and $(X, \mathcal{G}, \tau(\mathcal{A}), \tau \circ \alpha)$ are *nesting equivalent* (*nesting inequivalent*). Equivalently, two nested 3-GDDs $(X, \mathcal{G}, \mathcal{A}, \alpha)$ and $(X, \mathcal{G}, \mathcal{B}, \beta)$ are nesting equivalent if (1) they have the same underlying GDD, say U, and (2) for each block $B = \{w, x, y, z\}$ of U, $\{w, x, y\} \in \mathcal{A} \cap \mathcal{B}$, and hence $\alpha(\{w, x, y\}) = \beta(\{w, x, y\})$. Nesting equivalent nested 3-GDDs are thus, in every sense of the word, identical.

Lemma 27. *Let $D = (X, \mathcal{G}, \mathcal{A}, \alpha)$ be a nested 3-GDD with underlying GDD U. Then $\sim_{\mathfrak{A}(U)}$ is an equivalence relation.*

Proof. That $\sim_{\mathfrak{A}(U)}$ is both reflexive and symmetric is trivially true. Suppose to the contrary that $\sim_{\mathfrak{A}(U)}$ is not transitive; that is, suppose that for some $\sigma, \tau, \gamma \in \mathfrak{A}(U)$, $\sigma \sim_{\mathfrak{A}(U)} \tau$ and $\tau \sim_{\mathfrak{A}(U)} \gamma$, but $\sigma \not\sim_{\mathfrak{A}(U)} \gamma$. Then there exist two blocks $S = \{s_1, s_2, s_3, \alpha(\{s_1, s_2, s_3\})\}$ and $G = \{g_1, g_2, g_3, \alpha(\{g_1, g_2, g_3\})\}$ of U such that $B = \sigma(S) = \gamma(G)$ and $\sigma(\alpha(\{s_1, s_2, s_3\})) \neq \gamma(\alpha(\{g_1, g_2, g_3\}))$. But since $\sigma \sim_{\mathfrak{A}(U)} \tau$ and $\tau \sim_{\mathfrak{A}(U)} \gamma$, then in particular there exists a block $T = \{t_1, t_2, t_3, \alpha(\{t_1, t_2, t_3\})\}$ of U such that $\tau(T) = B$ and $\tau(\alpha(\{t_1, t_2, t_3\})) = \sigma(\alpha(\{s_1, s_2, s_3\})) = \gamma(\alpha(\{g_1, g_2, g_3\}))$, a contradiction. $\square$

The nested 3-GDD of Figure 5.1, the *Stinson ingredient GDD*, originates from [61]. Let U_ι be the underlying GDD of the Stinson ingredient GDD, and let R be a

Figure 5.2: The blocks of the underlying GDD of the Stinson ingredient GDD are the rows of $U = (u_{i,j})$, where $i \in [1, 8]$ and $j \in [1, 4]$. The eight nesting inequivalent nested 3-GDDs having underlying GDD defined by U are encoded in the sets $\mathscr{A}_1$ up to $\mathscr{A}_8$, insofar as that each $\mathscr{A}_i$ specifies which point of each row/block is the point adjoined by the i-th nesting to the remaining triple of points of that row/block.

$$U = \begin{bmatrix} 1_0 & 3_0 & 2_1 & 4_1 \\ 1_0 & 2_0 & 3_1 & 4_1 \\ 1_0 & 4_0 & 3_1 & 2_1 \\ 1_0 & 2_0 & 3_0 & 4_0 \\ 2_0 & 4_0 & 1_1 & 3_1 \\ 3_0 & 4_0 & 1_1 & 2_1 \\ 2_0 & 3_0 & 1_1 & 4_1 \\ 1_1 & 2_1 & 3_1 & 4_1 \end{bmatrix}$$

$$\begin{aligned}
\mathscr{A}_1 &= \{u_{1,1}, u_{2,2}, u_{3,3}, u_{4,4}, u_{5,3}, u_{6,4}, u_{7,2}, u_{8,4}\}, \\
\mathscr{A}_2 &= \{u_{1,2}, u_{2,1}, u_{3,4}, u_{4,4}, u_{5,4}, u_{6,3}, u_{7,1}, u_{8,4}\}, \\
\mathscr{A}_3 &= \{u_{1,4}, u_{2,2}, u_{3,1}, u_{4,3}, u_{5,2}, u_{6,4}, u_{7,3}, u_{8,3}\}, \\
\mathscr{A}_4 &= \{u_{1,3}, u_{2,1}, u_{3,2}, u_{4,3}, u_{5,1}, u_{6,3}, u_{7,4}, u_{8,3}\}, \\
\mathscr{A}_5 &= \{u_{1,2}, u_{2,4}, u_{3,1}, u_{4,2}, u_{5,4}, u_{6,2}, u_{7,3}, u_{8,2}\}, \\
\mathscr{A}_6 &= \{u_{1,1}, u_{2,3}, u_{3,2}, u_{4,2}, u_{5,3}, u_{6,1}, u_{7,4}, u_{8,2}\}, \\
\mathscr{A}_7 &= \{u_{1,3}, u_{2,4}, u_{3,3}, u_{4,1}, u_{5,1}, u_{6,2}, u_{7,2}, u_{8,1}\}, \text{ and} \\
\mathscr{A}_8 &= \{u_{1,4}, u_{2,3}, u_{3,4}, u_{4,1}, u_{5,2}, u_{6,1}, u_{7,1}, u_{8,1}\}.
\end{aligned}$$

complete set of representatives of the equivalence classes of $\mathfrak{A}(U_\iota)$ induced by $\sim_{\mathfrak{A}(U_\iota)}$. We have verified by computer that $|R| = 8$, and all eight nesting inequivalent nested 3-GDDs are given in Figure 5.2.

For $u \equiv 1 \pmod 4$ with $u \geq 5$, the *Stinson master GDD* $S_\mu = (Y, \mathcal{H}, \mathcal{B})$ is the 4-GDD obtained by deleting the common point of Property 9 in which three of the hyperovals of the GRL $S(2, 4, 3u + 1)$ intersect. Then Y partitions into three sets $\{Y_0, Y_1, Y_2\}$, the *hyperoval partition of* Y, with $|Y_0| = |Y_1| = |Y_2|$ such that by Property 9, $M \in \mathcal{B}$ is of precisely one of the three types:

(T_1) $|M \cap Y_0| = 2$ and $|M \cap Y_1| = 2$,

(T_2) $|M \cap Y_0| = 2$ and $|M \cap Y_2| = 2$, or

(T_3) $|M \cap Y_1| = 2$ and $|M \cap Y_2| = 2$.

Given the hyperoval partition $\{Y_0, Y_1, Y_2\}$ of Y, a *hyperoval-intervaled point ordering of* S_μ is a bijection $\mathsf{HOrd}_{S_\mu} : Y \to [0, |Y| - 1]$ such that $\mathsf{HOrd}_{S_\mu}(Y_i) = [i|Y|/3, (i+1)|Y|/3 - 1]$ for $i \in \{0, 1, 2\}$. Let HOrd_{S_μ} be a hyperoval-intervaled point ordering of S_μ, and $S_\iota = (X, \mathcal{G}, \mathcal{A}, \alpha)$ be the Stinson ingredient GDD, with $\mathcal{G} = \{\{1_0, 1_1\}, \{2_0, 2_1\}, \{3_0, 3_1\}, \{4_0, 4_1\}\}$ exactly as given in Figure 5.1. For each $B = \{b_1, b_2, b_3, b_4\} \in \mathcal{B}$, order its points as $(b_{i_1}, b_{i_2}, b_{i_3}, b_{i_4})$, $i_j \in [1, 4]$, such that $\mathsf{HOrd}_{S_\mu}(b_{i_1}) < \mathsf{HOrd}_{S_\mu}(b_{i_2}) < \mathsf{HOrd}_{S_\mu}(b_{i_3}) < \mathsf{HOrd}_{S_\mu}(b_{i_4})$. Then the *block placement map for* B *with respect to* HOrd_{S_μ} is the bijection $\sigma_{B,\mathsf{HOrd}_{S_\mu}} : X \to B \times \{0, 1\}$ satisfying:

1. $\sigma_{B,\mathsf{HOrd}_{S_\mu}}(1_0) = (b_{i_1}, 0)$ and $\sigma_{B,\mathsf{HOrd}_{S_\mu}}(1_1) = (b_{i_1}, 1)$;
2. $\sigma_{B,\mathsf{HOrd}_{S_\mu}}(2_0) = (b_{i_2}, 0)$ and $\sigma_{B,\mathsf{HOrd}_{S_\mu}}(2_1) = (b_{i_2}, 1)$;
3. $\sigma_{B,\mathsf{HOrd}_{S_\mu}}(3_0) = (b_{i_3}, 0)$ and $\sigma_{B,\mathsf{HOrd}_{S_\mu}}(3_1) = (b_{i_3}, 1)$; and
4. $\sigma_{B,\mathsf{HOrd}_{S_\mu}}(4_0) = (b_{i_4}, 0)$ and $\sigma_{B,\mathsf{HOrd}_{S_\mu}}(4_1) = (b_{i_4}, 1)$.

Finally, if U_ι is the underlying GDD of the Stinson ingredient GDD, a *choice map for* S_μ is a map $\kappa : \mathcal{B} \to \mathfrak{A}(U_\iota)$. We now present a generalization of the construction of Stinson in [61].

Generalized Stinson Construction. In essence, the construction is an application of WFC with master GDD a Stinson master GDD and ingredient GDD the Stinson ingredient GDD. For $u \equiv 1 \pmod 4$ with $u \geq 5$, let $S_\mu = (Y, \mathcal{H}, \mathcal{B})$ be the Stinson master GDD of type 3^u. We construct a nested 3-GDD D of type 6^u on points $Y \times \{0, 1\}$. Let $S_\iota = (X, \mathcal{G}, \mathcal{A}, \alpha)$ be the Stinson ingredient GDD, κ a choice map for S_μ, and HOrd_{S_μ} a hyperoval-intervaled point ordering of S_μ. For each $B \in \mathcal{B}$, place the nested 3-GDD

$$(B \times \{0,1\}, \sigma_{B,\mathsf{HOrd}_{S_\mu}}(\mathcal{G}), \sigma_{B,\mathsf{HOrd}_{S_\mu}}(\kappa(B)(\mathcal{A})), \sigma_{B,\mathsf{HOrd}_{S_\mu}} \circ \kappa(B) \circ \alpha), \tag{5.1}$$

where $\sigma_{B,\mathsf{HOrd}_{S_\mu}}$ is the block placement map for B with respect to HOrd_{S_μ}. The nesting of D is defined by the nestings of the placed copies of the Stinson ingredient GDD given by (5.1), and we write $D = \mathrm{GSC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$, determined as it is by these three parameters.

For any two applications of the generalized Stinson construction with fixed Stinson master GDD S_μ, the underlying GDDs, say U_1 and U_2, of the resulting two nested GDDs, say N_1 and N_2, of type 6^u are identical, so that $U = U_1 = U_2$. But under what conditions are N_1 and N_2 nesting equivalent?

Lemma 28. *Fix a Stinson master GDD $S_\mu = (Y, \mathcal{H}, \mathcal{B})$ of type 3^u and a hyperoval-intervaled point ordering HOrd_{S_μ} of S_μ, and suppose that GSC$(S_\mu, \kappa_1, \mathsf{HOrd}_{S_\mu}) = N_1$ and GSC$(S_\mu, \kappa_2, \mathsf{HOrd}_{S_\mu}) = N_2$, where $N_1 = (X, \mathcal{G}, \mathcal{A}_1, \alpha_1)$ and $N_2 = (X, \mathcal{G}, \mathcal{A}_2, \alpha_2)$ have common underlying GDD U. Suppose also that U_ι is the underlying GDD of the Stinson ingredient GDD. Then N_1 and N_2 are nesting equivalent if and only if $\kappa_1(B) \sim_{\mathfrak{A}(U_\iota)} \kappa_2(B)$ for all $B \in \mathcal{B}$.*

Proof. Both directions follow immediately from the fact that α_1 and α_2 are defined completely by the nestings of the copies of the Stinson ingredient GDD placed on the weighted blocks of S_μ. □

Let U_ι denote the underlying GDD of the Stinson ingredient GDD, and let R_ι be a complete set of representatives of the equivalence classes of $\mathfrak{A}(U_\iota)$ induced by $\sim_{\mathfrak{A}(U_\iota)}$. By consequence of Lemma 28, for a fixed Stinson master GDD S_μ with block set $\mathcal{B}$ and a hyperoval-intervaled point ordering HOrd_{S_μ} of S_μ, the set of all distinct (i.e., nesting-inequivalent) nested 3-GDDs of type 6^u that can possibly be produced by applying the generalized Stinson construction with S_μ and HOrd_{S_μ} as parameters is

$$\{\mathrm{GSC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu}) : \kappa(B) \in R_\iota \text{ for all } B \in \mathcal{B}\}.$$

The designs output by the generalized Stinson construction are ingredients of the principal construction of this section:

The 12u Construction. Fix $u \equiv 1 \pmod 4$ with $u \geq 5$, and let S_μ be the Stinson master GDD of type 3^u on point set Y, so that $E = (X, \mathcal{G}, \mathcal{A}, \alpha) = \mathrm{GSC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$ is a nested 3-GDD of type 6^u with nesting α. Put $V = X \times \{0, 1\}$ and for each pair of points $\{x, y\}$ intersecting with two different groups of $\mathcal{G}$, place the two blocks $\{(x, 0), (y, 0), (z, 0), (\alpha(A), 1)\}$ and $\{(x, 1), (y, 1), (z, 1), (\alpha(A), 0)\}$ in $\mathcal{B}$, where $A = \{x, y, z\} \in \mathcal{A}$. Then $(V, \mathcal{B})$ is a 4-GDD of type 12^u.

A 4-GDD D output by an application of the $12u$ construction is completely determined by the GDD E of type 6^u used in said application, and E, being a product of the generalized Stinson construction, is completely determined by some Stinson master GDD S_μ, choice map κ for S_μ, and hyperoval-intervaled point ordering of S_μ HOrd_{S_μ}. Accordingly, we write $D = \mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$, determined as it is by these three parameters. Our principal objective over the remainder of this section is to solve the optimization problem, thus: For fixed S_μ and HOrd_{S_μ}, which $\mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$ admits the best labelling, subject to certain constraints, with respect to the MinSum and DiffSum metrics?

Let rk be a point labelling of $D = \mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu}) = (Y, \mathcal{H}, \mathcal{B})$, where $\{Y_0, Y_1, Y_2\}$ is the hyperoval partition of the point set Y of the Stinson master GDD S_μ of type 3^u. Set $v = 12u$. We define two constraints on rk. First, rk is *HOrd_{S_μ}-faithful (with corresponding permutation σ)* iff there exists some permutation σ of $[0, 11]$ such that (1) for $i \in [0,2]$ and $j,k \in [0,1]$,

$$\mathsf{rk}(Y_i \times \{j\} \times \{k\}) = [\sigma(i+3j+6k)v/12, (\sigma(i+3j+6k)+1)v/12-1], \qquad (5.2)$$

and (2) $\mathsf{rk}(y_i,j,k) < \mathsf{rk}(y_i',j,k)$ iff $\mathsf{HOrd}_{S_\mu}(y_i) < \mathsf{HOrd}_{S_\mu}(y_i')$ for $y_i, y_i' \in Y_i$. In other words, if we think of a HOrd_{S_μ}-faithful labelling rk as an ordering of the points of $Y_i \times \{j\} \times \{k\}$ for $j,k \in [0,1]$, then the four copies of a point y of S_μ in D (i.e., $(y,0,0),(y,0,1),(y,1,0)$, and $(y,1,1)$) occupy the same position relative to the corresponding $Y_i \times \{j\} \times \{k\}$ that contains each one, and that position is precisely $\mathsf{HOrd}_{S_\mu}(y)$.

Next, rk is *worst of all possible worlds (with corresponding permutation σ)*, or WAPW for short, if (1) it is a HOrd_{S_μ}-faithful labelling with corresponding permutation σ and (2) for each type T_1 up to T_3, there exists a pair of distinct blocks M, M' of S_μ of that type such that if $|M' \cap Y_i| = |M \cap Y_i| = 2$, then

$$\mathsf{rk}((M \cap Y_i) \times \{0\} \times \{0\}) = [\sigma(i)v/12, \sigma(i)v/12+1], \text{ and}$$
$$\mathsf{rk}((M' \cap Y_i) \times \{0\} \times \{0\}) = [(\sigma(i)+1)v/12-2, (\sigma(i)+1)v/12-1].$$

Equivalently, rk is WAPW if for each block type and for fixed $i,j \in [0,1]$, there exists a block M of S_μ of that type such that $M \times \{i\} \times \{j\}$ has the lowest-valued possible labels and some other block M' of S_μ of the same type such that $M' \times \{i\} \times \{j\}$ has the greatest-valued possible labels. Accordingly, M and M' are *min-worst* and *max-worst* blocks of S_μ relative to rk, respectively.

As S_μ is a 4-GDD, there is at most one min-worst (max-worst) block of S_μ over all three types $\{T_1, T_2, T_3\}$ and thus a WAPW labelling of a GDD D output by the $12u$ construction cannot exist. However, we henceforth pretend that it does exist only for the sake of deriving bounds on the MinSum and $\mathsf{DiffSum}$ of D, for no *actual* point labelling of D can be any worse than a (pretend) WAPW labelling of it. Moreover, our understanding of the GRL $S(2,4,v)$ designs is not sufficient to guarantee that a min-worst or max-worst blocks relative to an arbitrary HOrd_{S_μ}-faithful labelling cannot exist; hence, we deal exclusively with WAPW labellings. But within an application of the generalized Stinson construction we still have a choice in how to place the Stinson ingredient GDD on the points of each weighted block of the Stinson master GDD. If two designs are *distinct* provided their block sets are not equal, then for a fixed Stinson master GDD S_μ with block set $\mathcal{B}$ and a hyperoval-intervaled point ordering of S_μ HOrd_{S_μ}, the set, denoted $\mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, of all distinct 4-GDDs of type 12^u that can possibly be produced by applying the $12u$ construction with S_μ and HOrd_{S_μ} as parameters is just the set of 4-GDDs

$$\mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu}) = \{\mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu}) : \kappa(B) \in R_\iota \text{ for all } B \in \mathcal{B}\},$$

where R_ι is a complete set of representatives of the equivalence classes of $\mathfrak{A}(U_\iota)$ induced by $\sim_{\mathfrak{A}(U_\iota)}$, and U_ι is the underyling GDD of the Stinson ingredient GDD. We emphasize that for any two choice maps κ, κ' for S_μ that do not map some $B \in \mathcal{B}$ to automorphisms in the same equivalence class, then $\mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$ and $\mathrm{TUC}(S_\mu, \kappa', \mathsf{HOrd}_{S_\mu})$ are distinct.

We thus have a pair of optimization problems, which we now pose in the form of a question. Given a fixed Stinson master GDD S_μ on point set Y, a hyperoval-intervaled point ordering of S_μ HOrd_{S_μ}, and a WAPW labelling rk of any $D \in \mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, for which D is $\mathsf{MinSum}(D, \mathsf{rk})$ the maximum, and for which D is $\mathsf{DiffSum}(D, \mathsf{rk})$ the minimum, over all $D \in \mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$? While the search space of these optimization problems grows arbitrarily large as the size of the point set of the Stinson master GDD grows, in fact to get the best result all we have to do is optimize how to place the Stinson ingredient blocks on the weighted min-worst and max-worst blocks. To establish this, we require some definitions. Given a Stinson master GDD S_μ on point set Y and a WAPW labelling rk of $D \in \text{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, let $m_w(S_\mu, \mathsf{rk})$ and $M_w(S_\mu, \mathsf{rk})$ denote the set of all min-worst and max-worst blocks of S_μ relative to rk, respectively. Further, for each $B \in m_w(S_\mu, \mathsf{rk}) \cup M_w(S_\mu, \mathsf{rk})$ let D_B denote the set of all blocks of D contained in $B \times \{0,1\} \times \{0,1\}$. Then D is *min-worst optimal with respect to* rk if for each $B \in m_w(S_\mu, \mathsf{rk})$ and $D' \in \text{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$,

$$\min(\mathsf{sum}(A, \mathsf{rk}) : A \in D_B) \geq \min(\mathsf{sum}(A, \mathsf{rk}) : A \in D'_B).$$

Conversely, D is *max-worst optimal with respect to* rk if for each $B \in M_w(S_\mu, \mathsf{rk})$ and $D' \in \text{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$,

$$\max(\mathsf{sum}(A, \mathsf{rk}) : A \in D_B) \leq \max(\mathsf{sum}(A, \mathsf{rk}) : A \in D'_B).$$

Finally, a choice map κ for $S_\mu = (Y, \mathcal{H}, \mathcal{B})$ is *min-worst consistent* with respect to a WAPW labelling rk of $D \in \text{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$ if, given the unique $B_i \in m_w(S_\mu, \mathsf{rk})$ of type T_i for $i \in [1,3]$, $\kappa(B_i) = \kappa(B)$ for every block $B \in B$ of type T_i. In essence, this means that D is constituted in such a way that whatever nested 3-GDD (among the collection of all eight nesting inequivalent nested 3-GDDs having the same underlying GDD as the Stinson ingredient GDD) is placed on the points of a weighted min-worst block of S_μ is also placed on all weighted blocks of S_μ of the same type T_i as that min-worst block.

Lemma 29. *Let $S_\mu = (X, \mathcal{G}, \mathcal{A})$ be a Stinson master GDD and rk a WAPW labelling of $D = TUC(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$, where κ is a choice map for S_μ that is min-worst consistent with respect to rk. Then*

$$\mathit{MinSum}(D, \mathit{rk}) = \min(\{\min(\mathit{sum}(A, \mathit{rk}) : A \in D_B) : B \in m_w(S_\mu, \mathit{rk})\}) \tag{5.3}$$

such that every block C of D with $\textsf{sum}(C, \textsf{rk}) = \textsf{MinSum}(D, \textsf{rk})$ satisfies $C \in D_B$, where $B \in m_w(S_\mu, \textsf{rk})$, and

$$\textsf{MaxSum}(D, \textsf{rk}) = \max(\{\max(\textsf{sum}(A, \textsf{rk}) : A \in D_B) : B \in M_w(S_\mu, \textsf{rk})\}) \tag{5.4}$$

such that every block C of D with $\textsf{sum}(C, \textsf{rk}) = \textsf{MaxSum}(D, \textsf{rk})$ satisfies $C \in D_B$, where $B \in M_w(S_\mu, \textsf{rk})$.

Proof. Let $B \in m_w(S_\mu, \textsf{rk})$ be the unique min-worst block of type T_i and let C be any other block of type T_i for $i \in \{1, 2, 3\}$. If $\sigma_{B,\textsf{HOrd}_{S_\mu}}$ and $\sigma_{C,\textsf{HOrd}_{S_\mu}}$ are the block placement maps for B and C, respectively, with respect to $\textsf{HOrd}_{S_\mu}$, then since $|B \cap C| \leq 1$, there exist at least three pairs (b, c) of the set

$$\{(b, c) : b \in B, c \in C, \text{ and } \sigma^{-1}_{B,\textsf{HOrd}_{S_\mu}}(b, 0) = \sigma^{-1}_{C,\textsf{HOrd}_{S_\mu}}(c, 0)\}$$

for which $\textsf{HOrd}_{S_\mu}(b) < \textsf{HOrd}_{S_\mu}(c)$. Hence, if $E = \text{GSC}(S_\mu, \kappa, \textsf{HOrd}_{S_\mu})$ has block set $\mathcal{E}$ and nesting α, then for any pair (F, G) of the set

$$\{(F, G) : F, G \in \mathcal{E}, F \in B \times \{0, 1\}, G \in C \times \{0, 1\} \text{ s.t. } \sigma^{-1}_{B,\textsf{HOrd}_{S_\mu}}(F) = \sigma^{-1}_{C,\textsf{HOrd}_{S_\mu}}(G)\},$$

where $F = \{f_1, f_2, f_3\}$ and $G = \{g_1, g_2, g_3\}$, then for $i \in \mathbb{Z}_2$

$$F'_i = \{(f_1, i), (f_2, i), (f_3, i), (\alpha(F), i + 1)\} \text{ and}$$
$$G'_i = \{(g_1, i), (g_2, i), (g_3, i), (\alpha(G), i + 1)\}$$

are blocks of D such that $\textsf{sum}(F'_i, \textsf{rk}) < \textsf{sum}(G'_i, \textsf{rk})$.

Applying a symmetric argument, let $B \in M_w(S_\mu, \textsf{rk})$ be the unique max-worst block of type T_i and let C be any other block of type T_i for $i \in \{1, 2, 3\}$. If $\sigma_{B,\textsf{HOrd}_{S_\mu}}$ and $\sigma_{C,\textsf{HOrd}_{S_\mu}}$ are the block placement maps for B and C, respectively, with respect to $\textsf{HOrd}_{S_\mu}$, then since $|B \cap C| \leq 1$, there exist at least three pairs (b, c) of the set

$$\{(b, c) : b \in B, c \in C, \text{ and } \sigma^{-1}_{B,\textsf{HOrd}_{S_\mu}}(b, 0) = \sigma^{-1}_{C,\textsf{HOrd}_{S_\mu}}(c, 0)\}$$

for which $\mathsf{HOrd}_{S_\mu}(b) > \mathsf{HOrd}_{S_\mu}(c)$. Hence, if $E = \text{GSC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$ has block set $\mathcal{E}$ and nesting α, then for any pair (F, G) of the set

$$\{(F,G) : F, G \in \mathcal{E}, F \in B \times \{0,1\}, G \in C \times \{0,1\} \text{ s.t. } \sigma^{-1}_{B,\mathsf{HOrd}_{S_\mu}}(F) = \sigma^{-1}_{C,\mathsf{HOrd}_{S_\mu}}(G)\},$$

where $F = \{f_1, f_2, f_3\}$ and $G = \{g_1, g_2, g_3\}$, then for $i \in \mathbb{Z}_2$

$$F'_i = \{(f_1, i), (f_2, i), (f_3, i), (\alpha(F), i+1)\} \text{ and}$$
$$G'_i = \{(g_1, i), (g_2, i), (g_3, i), (\alpha(G), i+1)\}$$

are blocks of D such that $\mathsf{sum}(F'_i, \mathsf{rk}) > \mathsf{sum}(G'_i, \mathsf{rk})$. □

Lemma 30. *Let S_μ be a Stinson master GDD and rk a WAPW labelling of $D \in$ TUCD$(S_\mu, \mathsf{HOrd}_{S_\mu})$. If D is min-worst optimal relative to rk and satisfies (5.3), then for any $D' \in$ TUCD$(S_\mu, \mathsf{HOrd}_{S_\mu})$, $\mathsf{MinSum}(D, \mathsf{rk}) \geq \mathsf{MinSum}(D', \mathsf{rk})$. If D is min-worst and max-worst optimal relative to rk, and satisfies both (5.3) and (5.4), then for any $D' \in$ TUCD$(S_\mu, \mathsf{HOrd}_{S_\mu})$, $\mathsf{DiffSum}(D, \mathsf{rk}) \leq \mathsf{DiffSum}(D', \mathsf{rk})$.*

Proof. For any $D' \in \text{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, put

$$\mathfrak{m}_{D'} = \min(\{\min(\mathsf{sum}(A, \mathsf{rk}) : A \in D'_B) : B \in m_w(S_\mu, \mathsf{rk})\}).$$

Then either $\mathsf{MinSum}(D', \mathsf{rk}) = \mathfrak{m}_{D'}$ or $\mathsf{MinSum}(D', \mathsf{rk}) \neq \mathfrak{m}_{D'}$. If the former obtains, then for any $D \in \text{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$ that is min-worst optimal relative to rk and satisfies (5.3), $\mathsf{MinSum}(D, \mathsf{rk}) \geq \mathsf{MinSum}(D', \mathsf{rk})$. If the latter obtains,

$$\mathsf{MinSum}(D', \mathsf{rk}) < \mathfrak{m}_{D'} \leq \mathfrak{m}_D = \mathsf{MinSum}(D, \mathsf{rk}).$$

Applying the above argument, *mutatis mutandis*, it follows that if D is max-worst optimal relative to rk and satisfies (5.4), then for any $D' \in \text{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, $\mathsf{MaxSum}(D, \mathsf{rk}) \leq \mathsf{MaxSum}(D', \mathsf{rk})$. Hence, if D is both max-worst and min-worst optimal relative to rk and satisfies both (5.3) and (5.4), then $\mathsf{DiffSum}(D, \mathsf{rk}) \leq \mathsf{DiffSum}(D', \mathsf{rk})$. □

In short, Lemmas 29 and 30 together imply that in order to compute the maximum MinSum over all $D \in \mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$ for a fixed WAPW point labelling rk of the point set of all designs of $\mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, we need only compute the minimum block sum over the set of blocks of a min-worst optimal $D' \in \mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$ (with respect to rk) contained in a weighted min-worst block (relative to rk). Exploiting this reduction, Algorithm 1 computes for a given Stinson master GDD S_μ and hyperoval-intervaled point ordering HOrd_{S_μ} of S_μ the maximum MinSum over all possible WAPW labellings of all $D \in \mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$. In Algorithm 1, the symbol $\mathfrak{D}$ appears on line 5; we now define it. Let U_ι denote the underlying GDD of the Stinson ingredient GDD, and R_ι a complete set of representatives of the equivalence classes of $\mathfrak{A}(U_\iota)$ induced by $\sim_{\mathfrak{A}(U_\iota)}$. For $i \in [1, 3]$, let K_i denote a (maximum) set of eight choice maps for S_μ with codomain restricted to R_ι with the property that for any distinct $\kappa, \kappa' \in K_i$, then for the min-worst block $B_i \in m_w(S_\mu, \mathsf{rk})$ of type T_i, where rk is the labelling of line 4, $\kappa(B_i) \neq \kappa'(B_i)$. Then

$$\mathfrak{D} = \{\mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu}) : \kappa \in \bigcup_{i \in [1,3]} K_i\}.$$

By running Algorithm 1, we get:

Lemma 31. *Let S_μ be the Stinson master GDD of type 3^u, with $u \equiv 1 \pmod 4$ and $u \geq 5$, and put $v = 12u$. Then there exists a WAPW labelling rk of some $D \in TUCD(S_\mu, \mathsf{HOrd}_{S_\mu})$ such that $\mathsf{MinSum}(D, \mathsf{rk}) = 13v/12 + 2$.*

By running a slightly modified version of Algorithm 1 that returns some $D \in \mathfrak{D}$ that realizes the optimal MinSum of $13v/12 + 2$, we obtain the 4-GDD described in Lemma 32:

Algorithm 1 Compute maximum MinSum (`MSBest`) for $12u$ construction

Let S_μ be a Stinson master GDD and HOrd_{S_μ} a hyperoval-intervaled point ordering of S_μ
`MSBest` $\leftarrow 0$
for each permutation σ of the set $[0, 11]$ **do**
    Let rk be a WAPW labelling of any design in $\mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$ with corresponding permutation σ
    for $D \in \mathfrak{D}$ **do**
        for each block type T_i **do**
            Let $B_i \in m_w(S_\mu, \mathsf{rk})$ be the min-worst block of type T_i
            $\mathtt{MS}_i \leftarrow$ minimum block sum over all blocks of D_{B_i}
        end for
        `MS` $\leftarrow$ minimum of all $\mathtt{MS}_i$'s
        if `MS` $>$ `MSBest` **then**
            `MSBest` $\leftarrow$ `MS`
        end if
    end for
end for
return `MSBest`

Lemma 32. *Let $S_\iota = (X, \mathcal{G}, \mathcal{A}, \alpha)$ denote the Stinson ingredient GDD and let S_μ denote the Stinson master 3-GDD of type 3^u. Put*

$$\sigma(0) = 10, \sigma(1) = 11, \sigma(2) = 9, \sigma(3) = 8, \sigma(4) = 7, \sigma(5) = 6,$$

$$\sigma(6) = 5, \sigma(7) = 0, \sigma(8) = 4, \sigma(9) = 1, \sigma(10) = 3, \sigma(11) = 2,$$

so that for any design in TUCD($S_\mu, \mathsf{HOrd}_{S_\mu}$), rk is a WAPW labelling with corresponding permutation σ. Further, for $i \in [1, 3]$, let $\mathcal{B}_i$ be the set of blocks of S_μ of type T_i; then define the choice map κ for S_μ such that:

1. *For each $B \in \mathcal{B}_1$, $\kappa(B) \circ \alpha$ gives the nesting determined by $\mathscr{A}_6$ of Figure 5.2;*
2. *for each $B \in \mathcal{B}_2$, $\kappa(B) \circ \alpha$ gives the nesting determined by $\mathscr{A}_6$ of Figure 5.2; and*
3. *for each $B \in \mathcal{B}_3$, $\kappa(B) \circ \alpha$ gives the nesting determined by $\mathscr{A}_1$ of Figure 5.2.*

Then if $D = TUC(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$, $\mathsf{MinSum}(D, \mathsf{rk}) = 13v/12 + 2$, where $v = 12u$.

If $D = \mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu}) = (V, \mathcal{G}, \mathcal{A})$, where S_μ is the Stinson master GDD of type 3^u, then we can obtain from D an $S(2,4,12u+1)$ and an $S(2,4,12u+4)$ on point sets $X \cup \{\infty\}$ and $X \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}$, respectively, by "filling in groups":

(C1) For each $G \in \mathcal{G}$, let $(G \cup \{\infty\}, G^*)$ be an $S(2,4,13)$. Then $D' = (V, \mathcal{A} \cup \bigcup_{G \in \mathcal{G}} G^*)$ is an $S(2,4,12u+1)$.

(C2) For each $G \in \mathcal{G}$, let $(G \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}, G^*)$ be an $S(2,4,16)$ with $\{\infty_1, \infty_2, \infty_3, \infty_4\} \in G^*$. Then $D' = (V, \mathcal{A} \cup \bigcup_{G \in \mathcal{G}} G^*)$ is an $S(2,4,12u+4)$.

Lemma 32 gives us a WAPW labelling rk of a particular $D \in \mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$; we now show that it is possible to, roughly speaking, "extend" rk to obtain a labelling rk^+ of D' such that $\mathsf{MinSum}(D', \mathsf{rk}^+) = \mathsf{MinSum}(D, \mathsf{rk})$. The trick is to carefully place the blocks of each sub-$S(2,4,16)$ (sub-$S(2,4,13)$). Before doing so, we require an auxiliary result.

Lemma 33. *Let $D = (X, \mathcal{G}, \mathcal{A}) \in TUCD(S_\mu, \mathsf{HOrd}_{S_\mu})$, where S_μ is the Stinson master GDD of type 3^u. Let rk be a WAPW labelling of D with corresponding permutation σ of $[0,11]$. Following (5.2), for $i \in [0,2]$ and $j,k \in [0,1]$, define*

$$I_{i,j,k} = [\sigma(i+3j+6k)v/12, (\sigma(i+3j+6k)+1)v/12 - 1],$$

where $v = 12u$. Then for each $G \in \mathcal{G}$ there exists a bijection $f_G : G \to \bigcup_{i \in [0,2], j,k \in [0,1]} \{I_{i,j,k}\}$ such that for each $g \in G$, $\mathsf{rk}(g) \in f_G(g)$.

Proof. Suppose that S_μ has point set Y, so that $X = Y \times \{0,1\} \times \{0,1\}$, and let $\{Y_0, Y_1, Y_2\}$ be the hyperoval partition of Y. Since $\mathsf{rk}(Y_i \times \{j\} \times \{k\}) = I_{i,j,k}$ for $i \in [0,2]$ and $j,k \in [0,1]$, then by Property 9 the result obtains. □

We must emphasize at the outset that the labellings of Theorem 22 below are fictional, since they are based on WAPW labellings, which, as we've already noted, cannot exist. However, they still can be used to derive a lower bound on the MinSum.

Theorem 22. *Let $v = 12u$ with $u \equiv 1 \pmod 4$ with $u \geq 5$. Then the following exist:*

1. *A labelling rk^+ of an $S(2,4,v+1)$ E such that $\mathsf{MinSum}(E, \mathsf{rk}^+) \geq 13v/12 + 3$, and*
2. *a labelling rk'^+ of an $S(2,4,v+4)$ E' such that $\mathsf{MinSum}(E', \mathsf{rk}'^+) \geq 13v/12 + 2$.*

Proof. Let σ and $D = \mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu}) = (V, \mathcal{G}, \mathcal{A})$ be the permutation of $[0, 11]$ and the 4-GDD of type 12^u, respectively, of Lemma 32. Let rk be a WAPW labelling of D with corresponding permutation σ. Now let rk^+ be the labelling of $V \cup \{\infty\}$ satisfying $\mathsf{rk}^+(\infty) = 0$ and $\mathsf{rk}^+(x) = \mathsf{rk}(x) + 1$ for all $x \in V$. As in (C1), construct an $S(2,4,12u+1)$ E on point set $V \cup \{\infty\}$ from D by placing on $G \cup \{\infty\}$ an $S(2,4,13)$ for each $G \in \mathcal{G}$. By Lemma 33 the lowest-valued set of labels that could possibly be assigned by rk^+ to $G \in \mathcal{G}$ is

$$L = \{1, v/12 + 1, 2v/12 + 1, \ldots, 11v/12 + 1\}.$$

Hence, if we can show that there exists a labelling $\mathsf{rk}_{13} : [0, 9] \cup \{\mathrm{a}, \mathrm{b}, \mathrm{c}\} \to \{0\} \cup L$ of the points of the unique $S(2,4,13)$ D_{13} of Table 5.2 such that $\mathsf{MinSum}(D_{13}, \mathsf{rk}_{13}) \geq 13v/12 + 3$, then we are done. The following labelling satisfies this condition:

$\mathsf{rk}_{13}(0) = 0, \mathsf{rk}_{13}(1) = 6v/12 + 1, \mathsf{rk}_{13}(2) = 7v/12 + 1, \mathsf{rk}_{13}(3) = 8v/12 + 1,$
$\mathsf{rk}_{13}(4) = 9v/12 + 1, \mathsf{rk}_{13}(5) = 11v/12 + 1, \mathsf{rk}_{13}(6) = 10v/12 + 1, \mathsf{rk}_{13}(7) = 2v/12 + 1,$
$\mathsf{rk}_{13}(8) = 3v/12 + 1, \mathsf{rk}_{13}(9) = 1, \mathsf{rk}_{13}(\mathrm{a}) = v/12 + 1, \mathsf{rk}_{13}(\mathrm{b}) = 4v/12 + 1,$ and
$\mathsf{rk}_{13}(\mathrm{c}) = 5v/12 + 1.$

Indeed, we have verified by computer that $\mathsf{MinSum}(D_{13}, \mathsf{rk}_{13}) = 7v/6 + 4$.

Next, let rk'^{+} be the labelling of $V \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}$ satisfying:

1. $\mathsf{rk}'^{+}(\{\infty_1\}) = v$, $\mathsf{rk}'^{+}(\{\infty_2\}) = v + 1$, $\mathsf{rk}'^{+}(\{\infty_3\}) = v + 2$, $\mathsf{rk}'^{+}(\{\infty_4\}) = v + 3$, and
2. $\mathsf{rk}'^{+}(x) = \mathsf{rk}(x)$ for all $x \in V$.

As in (C2) construct from D an $S(2, 4, 12u+4)$ E' on point set $V \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}$ by placing on $G \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}$ an $S(2, 4, 16)$ for each $G \in \mathcal{G}$. By Lemma 33, the lowest-valued set of labels that could possibly be assigned by rk'^{+} to $G \in \mathcal{G}$ is

$$L' = \{0, v/12, 2v/12, \ldots, 11v/12\}.$$

Thus, if we can show that there exists a labelling

$$\mathsf{rk}_{16} : [0, 9] \cup \{\mathrm{a, b, c, d, e, f}\} \rightarrow L \cup \{v, v + 1, v + 2, v + 3\}$$

of the points of the unique $S(2, 4, 16)$ D_{16} of Table 5.2 such that:

1. $\mathsf{rk}_{16}^{-1}(\{v, v + 1, v + 2, v + 3\})$ is a block of D_{16}, and
2. $\mathsf{MinSum}(D_{16}, \mathsf{rk}_{16}) \geq 13v/12 + 2$,

then we are done. The following labelling satisfies both conditions:

$$\mathsf{rk}_{16}(0) = v, \mathsf{rk}_{16}(1) = 6v/12, \mathsf{rk}_{16}(2) = 7v/12, \mathsf{rk}_{16}(3) = 2v/12, \mathsf{rk}_{16}(4) = 8v/12,$$

$$\mathsf{rk}_{16}(5) = 9v/12, \mathsf{rk}_{16}(6) = 3v/12, \mathsf{rk}_{16}(7) = v/12, \mathsf{rk}_{16}(8) = 4v/12, \mathsf{rk}_{16}(9) = 0,$$

$$\mathsf{rk}_{16}(\mathrm{a}) = v + 1, \mathsf{rk}_{16}(\mathrm{b}) = v + 2, \mathsf{rk}_{16}(\mathrm{c}) = v + 3, \mathsf{rk}_{16}(\mathrm{d}) = 11v/12,$$

$$\mathsf{rk}_{16}(\mathrm{e}) = 10v/12, \text{ and } \mathsf{rk}_{16}(\mathrm{f}) = 5v/12.$$

Indeed, by inspection, $\{0, \mathrm{a, b, c}\}$ is a block of D_{16} and we have verified by computer that $\mathsf{MinSum}(D_{16}, \mathsf{rk}_{16}) = 17v/12$. □

As an immediate consequence of Theorem 22, we have two MinSum bounds which together cover (practically) one quarter of the admissible orders of an $S(2,4,v)$:

Corollary 6. *For all* $v \equiv 13 \pmod{48}$ *with* $v \geq 61$ *there exists an* $S(2,4,v)$ D *such that* $\mathsf{MinSum}(D) \geq 13v/12 + 1$*. For all* $v \equiv 16 \pmod{48}$ *with* $v \geq 64$ *there exists an* $S(2,4,v)$ D *such that* $\mathsf{MinSum}(D) \geq 13v/12 - 2$*.*

Theoretically, per Lemma 30, given a Stinson master GDD S_μ, a hyperoval-intervaled point ordering HOrd_{S_μ} of S_μ, and rk a WAPW labelling of any design of $\mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, then if in particular $D = \mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$ is min-worst and max-worst optimal relative to rk and satisfies both (5.3) and (5.4), then for any $D' \in \mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, $\mathsf{DiffSum}(D, \mathsf{rk}) \leq \mathsf{DiffSum}(D', \mathsf{rk})$. However, it is unclear how to ensure that D satisfies (5.3) and (5.4). By Lemma 29, one can at least ensure that D satisfies (5.3) by making κ min-worst consistent with respect to rk. This same approach could only satisfy both (5.3) and (5.4) provided that for each min-worst block $B \in m_w(S_\mu, \mathsf{rk})$, then for all $D' \in \mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, we have the guarantee that

$$\min\{\mathsf{sum}(A, \mathsf{rk}) : A \in D_B\} \geq \min\{\mathsf{sum}(A, \mathsf{rk}) : A \in D'_B\},$$

and

$$\max\{\mathsf{sum}(A, \mathsf{rk}) : A \in D_B\} \leq \max\{\mathsf{sum}(A, \mathsf{rk}) : A \in D'_B\}.$$

Alas, we don't know how to honor this guarantee. Thus, at the potential cost of obtaining the minimum $\mathsf{DiffSum}$ over all designs of $\mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$, we take the approach in the form of Algorithm 2, which, for a given Stinson master GDD S_μ computes the minimum $\mathsf{DiffSum}$ over all $D \in \mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$ such that if $D = \mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$, then κ is min-worst consistent with respect to a WAPW

Algorithm 2 Compute $\mathsf{DiffSum}$ ($\texttt{DSBest}$) for $12u$ construction

1: Let S_μ be a Stinson master GDD and HOrd_{S_μ} a hyperoval-intervaled point ordering of S_μ
2: $\texttt{DSBest} \leftarrow \infty$
3: **for** each permutation σ of the set $[0, 11]$ **do**
4:     Let rk be a WAPW labelling of any design in $\mathrm{TUCD}(S_\mu, \mathsf{HOrd}_{S_\mu})$ with corresponding permutation σ
5:     **for** $D \in \mathfrak{D}'$ **do**
6:         **for** each block type T_i **do**
7:             Let $B_i \in m_w(S_\mu, \mathsf{rk})$ be the min-worst block of type T_i
8:             Let $C_i \in M_w(S_\mu, \mathsf{rk})$ be the max-worst block of type T_i
9:             $\texttt{MinSum}_i \leftarrow$ minimum block sum over all blocks of D_{B_i}
10:             $\texttt{MaxSum}_i \leftarrow$ maximum block sum over all blocks of D_{C_i}
11:         **end for**
12:         $\texttt{MinSum} \leftarrow$ minimum of all $\texttt{MinSum}_i$'s
13:         $\texttt{MaxSum} \leftarrow$ maximum of all $\texttt{MaxSum}_i$'s
14:         **if** $\texttt{MaxSum} - \texttt{MinSum} < \texttt{DSBest}$ **then**
15:             $\texttt{DSBest} \leftarrow \texttt{MaxSum} - \texttt{MinSum}$
16:         **end if**
17:     **end for**
18: **end for**
19: **return** $\texttt{DSBest}$

labelling rk of D. In Algorithm 2, the symbol $\mathfrak{D}'$ appears on line 5; we now define it. Let U_ι denote the underlying GDD of the Stinson ingredient GDD, and R_ι a complete set of representatives of the equivalence classes of $\mathfrak{A}(U_\iota)$ induced by $\sim_{\mathfrak{A}(U_\iota)}$. For $i \in [1, 3]$, let K_i denote a (maximum) set of eight choice maps for S_μ with codomain restricted to R_ι with the property that for distinct $\kappa, \kappa' \in K_i$, then for the min-worst block $B_i \in m_w(S_\mu, \mathsf{rk})$ and max-worst block $C_i \in M_w(S_\mu, \mathsf{rk})$ of type T_i, where rk is the labelling of line 4, (1) $\kappa(B_i) = \kappa(C_i)$ and $\kappa'(B_i) = \kappa'(C_i)$, and (2) $\kappa(B_i) \neq \kappa'(B_i)$. Then

$$\mathfrak{D}' = \{\mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu}) : \kappa \in \bigcup_{i \in [1,3]} K_i\}.$$

By running Algorithm 2, we get:

Lemma 34. *Let S_μ be the Stinson master GDD of type 3^u, with $u \equiv 1 \pmod 4$ and $u \geq 5$, and put $v = 12u$. Then there exists a WAPW labelling* rk *of some* $D \in TUCD(S_\mu, \mathsf{HOrd}_{S_\mu})$ *such that* $\mathsf{DiffSum}(D, \mathsf{rk}) = 2v - 8$.

By running a slightly modified version of Algorithm 2 that returns some $D \in \mathfrak{D}'$ that realizes the DiffSum of $2v - 8$, we obtain the 4-GDD described in Lemma 35:

Lemma 35. *Let $S_\iota = (X, \mathcal{G}, \mathcal{A}, \alpha)$ denote the Stinson ingredient GDD and let S_μ denote the Stinson master 3-GDD of type 3^u. Put $v = 12u$ and*

$$\sigma(0) = 9, \sigma(1) = 8, \sigma(2) = 7, \sigma(3) = 11, \sigma(4) = 10, \sigma(5) = 6,$$
$$\sigma(6) = 3, \sigma(7) = 2, \sigma(8) = 5, \sigma(9) = 1, \sigma(10) = 0, \sigma(11) = 4,$$

so that for any design in $TUCD(S_\mu, \mathsf{HOrd}_{S_\mu})$, rk *is a WAPW labelling with corresponding permutation σ. Further, for $i \in [1, 3]$, let $\mathcal{B}_i$ be the set of blocks of S_μ type T_i; then define the choice map κ for S_μ such that:*

1. *For each $B \in \mathcal{B}_1$, $\kappa(B) \circ \alpha$ gives the nesting determined by $\mathscr{A}_1$ of Figure 5.2;*
2. *for each $B \in \mathcal{B}_2$, $\kappa(B) \circ \alpha$ gives the nesting determined by $\mathscr{A}_1$ of Figure 5.2; and*
3. *for each $B \in \mathcal{B}_3$, $\kappa(B) \circ \alpha$ gives the nesting determined by $\mathscr{A}_6$ of Figure 5.2.*

Then if $D = TUC(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu})$, *the two properties are satisfied:*

1. $\mathsf{MaxSum}(D, \mathsf{rk}) = 3v - 6$ *such that every block B of D with* $\mathsf{sum}(B, \mathsf{rk}) = 3v - 6$ *satisfies* $|\mathsf{rk}(B) \cap [v/2, v-1]| = 3$, *and*
2. $\mathsf{MinSum}(D, \mathsf{rk}) = v + 2$ *such that every block B of D with* $\mathsf{sum}(B, \mathsf{rk}) = v + 2$ *satisfies* $|\mathsf{rk}(B) \cap [0, v/2 - 1]| = 3$;

hence, $\mathsf{DiffSum}(D, \mathsf{rk}) = 2v - 8$.

Proof. Again, D was obtained via a modified version of Algorithm 2, so our only aim in this proof is to demonstrate that (1) every block B of D with $\mathsf{sum}(B, \mathsf{rk}) = 3v - 6$ satisfies $|\mathsf{rk}(B) \cap [v/2, v-1]| = 3$ and (2) every block B of D with $\mathsf{sum}(B, \mathsf{rk}) = v + 2$ satisfies $|\mathsf{rk}(B) \cap [0, v/2 - 1]| = 3$. Let B_i and C_i be the min-worst and max-worst blocks, respectively, with respect to rk of type T_i. As κ is min-worst consistent with respect to rk, by Lemma 29 we need only verify that (1) holds with respect to D_{B_i} and that (2) holds with respect to D_{C_i}; both verifications have been done by computer. □

Analogous to the approach of Theorem 22, we "extend" the labelling of the 4-GDD D of type 12^u of Lemma 35 to label an $S(2, 4, 12u + 1)$ and an $S(2, 4, 12u + 4)$ that result from filling the groups of D. We must emphasize at the outset that the labellings of Theorem 23 below are fictional, since they are based on WAPW labellings, which, as we've already noted, cannot exist. However, they still can be used to derive an upper bound on the $\mathsf{DiffSum}$.

Theorem 23. *Let $v = 12u$ with $u \equiv 1 \pmod 4$. Then the following exist:*

1. *A labelling rk^+ of an $S(2, 4, v + 1)$ E such that $\mathsf{MaxSum}(E, \mathsf{rk}^+) = 3v - 3$ and $\mathsf{MinSum}(E, \mathsf{rk}^+) = v + 3$, so that $\mathsf{DiffSum}(E, \mathsf{rk}^+) = 2v - 6$, and*
2. *a labelling rk'^+ of an $S(2, 4, v + 4)$ E' such that $\mathsf{MaxSum}(E', \mathsf{rk}'^+) = 3v + 6$ and $\mathsf{MinSum}(E', \mathsf{rk}'^+) = v + 6$, so that $\mathsf{DiffSum}(E', \mathsf{rk}'^+) = 2v$.*

Proof. Let σ and $D = \mathrm{TUC}(S_\mu, \kappa, \mathsf{HOrd}_{S_\mu}) = (V, \mathcal{G}, \mathcal{A})$ be the permutation of $[0, 11]$ and the 4-GDD of type 12^u, respectively, of Lemma 35. Let rk be a WAPW labelling of D with corresponding permutation σ. Now let rk^+ be the labelling of $V \cup \{\infty\}$ satisfying:

1. $\mathsf{rk}^+(\infty) = 6v/12$,
2. $\mathsf{rk}^+(x) = \mathsf{rk}(x)$ for all $x \in \mathsf{rk}^{-1}([0, 6v/12 - 1])$, and

3. $\mathsf{rk}^+(y) = \mathsf{rk}(y) + 1$ for all $y \in \mathsf{rk}^{-1}([6v/12, v-1])$.

As in (C1), construct an $S(2,4,12u+1)$ E on point set $V \cup \{\infty\}$ from D by placing on $G \cup \{\infty\}$ an $S(2,4,13)$ for each $G \in \mathcal{G}$. By Lemma 33, the lowest-valued set of labels that could possibly be assigned by rk^+ to $G \in \mathcal{G}$ is

$$L = \left\{0, \frac{v}{12}, \frac{2v}{12}, \ldots, \frac{5v}{12}, \frac{6v}{12} + 1, \frac{7v}{12} + 1, \ldots, \frac{11v}{12} + 1\right\}.$$

Conversely, the highest-valued set of labels that could possibly be assigned by rk^+ to $G \in \mathcal{G}$ is

$$H = \left\{\frac{v}{12} - 1, \frac{2v}{12} - 1, \ldots, \frac{6v}{12} - 1, \frac{7v}{12}, \frac{8v}{12}, \ldots, v\right\};$$

thus, H can be obtained by adding $v/12 - 1$ to each element of L. Hence, if we can show that there exists a labelling $\mathsf{rk}_{13} : [0,9] \cup \{\mathrm{a}, \mathrm{b}, \mathrm{c}\} \to \{6v/12\} \cup L$ of the points of the unique $S(2,4,13)$ D_{13} of Table 5.2 such that:

1. $\mathsf{MinSum}(D_{13}, \mathsf{rk}_{13}) \geq v + 3$, and
2. $\mathsf{MaxSum}(D_{13}, \mathsf{rk}_{13}) \leq 3v - 3 - (v/3 - 4) = 8v/3 - 7$,

then we are done. The following labelling satisfies both of these conditions:

$\mathsf{rk}_{13}(0) = 6v/12, \mathsf{rk}_{13}(1) = 9v/12 + 1, \mathsf{rk}_{13}(2) = 10v/12 + 1, \mathsf{rk}_{13}(3) = 11v/12 + 1,$

$\mathsf{rk}_{13}(4) = 8v/12 + 1, \mathsf{rk}_{13}(5) = 7v/12 + 1, \mathsf{rk}_{13}(6) = 6v/12 + 1, \mathsf{rk}_{13}(7) = 5v/12,$

$\mathsf{rk}_{13}(8) = 4v/12, \mathsf{rk}_{13}(9) = 3v/12, \mathsf{rk}_{13}(\mathrm{a}) = 2v/12, \mathsf{rk}_{13}(\mathrm{b}) = 0,$ and $\mathsf{rk}_{13}(\mathrm{c}) = v/12.$

Indeed, we have verified by computer that $\mathsf{MinSum}(D_{13}, \mathsf{rk}) = 13v/12 + 1$ and $\mathsf{MaxSum}(D_{13}, \mathsf{rk}) = 29v/12 + 3$.

Next, let rk'^+ be the labelling of $V \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}$ satisfying:

1. $\mathsf{rk}'^+(\{\infty_1\}) = 6v/12$, $\mathsf{rk}'^+(\{\infty_2\}) = 6v/12 + 1$, $\mathsf{rk}'^+(\{\infty_3\}) = 6v/12 + 2$, $\mathsf{rk}'^+(\{\infty_4\}) = 6v/12 + 3$;

2. $\mathsf{rk}'^{+}(x) = \mathsf{rk}(x)$ for all $x \in \mathsf{rk}^{-1}([0, 6v/12-1])$; and
3. $\mathsf{rk}'^{+}(y) = \mathsf{rk}(y) + 4$ for all $y \in \mathsf{rk}^{-1}([6v/12, v-1])$.

As in (C2), construct an $S(2,4,12u+4)$ E' on point set $V \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}$ by placing on $G \cup \{\infty_1, \infty_2, \infty_3, \infty_4\}$ an $S(2,4,16)$ for each $G \in \mathcal{G}$, making sure that $\{\infty_1, \infty_2, \infty_3, \infty_4\}$ is a block in each placed $S(2,4,16)$. By Lemma 33, the lowest-valued set of labels that could possibly be assigned by rk'^{+} to $G \in \mathcal{G}$ is

$$L' = \left\{0, \frac{v}{12}, \frac{2v}{12}, \ldots, \frac{5v}{12}, \frac{6v}{12}+4, \frac{7v}{12}+4, \ldots, \frac{11v}{12}+4\right\}.$$

Conversely, the highest-valued set of labels that could possibly be assigned by rk'^{+} to $G \in \mathcal{G}$ is

$$H' = \left\{\frac{v}{12}-1, \frac{2v}{12}-1, \ldots, \frac{6v}{12}-1, \frac{7v}{12}+3, \frac{8v}{12}+3, \ldots, v+3\right\};$$

thus, H' can be obtained by adding $v/12 - 1$ to each element of L'. Hence, if we can show that there exists a labelling

$$\mathsf{rk}_{16} : [0,9] \cup \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}, \mathrm{e}, \mathrm{f}\} \to \{6v/12, 6v/12+1, 6v/12+2, 6v/12+3\} \cup L'$$

of the points of the unique $S(2,4,16)$ D_{16} of Table 5.2 such that:

1. $\mathsf{rk}_{16}^{-1}(\{6v/12, 6v/12+1, 6v/12+2, 6v/12+3\})$ is a block of D_{16},
2. $\mathsf{MinSum}(D_{16}, \mathsf{rk}_{16}) \geq v+6$, and
3. $\mathsf{MaxSum}(D_{16}, \mathsf{rk}_{16}) \leq 3v+6-(v/3-4) = 8v/3+2$,

then we are done. The following labelling satisfies all three of these conditions:

$\mathsf{rk}_{16}(0) = 6v/12, \mathsf{rk}_{16}(1) = 6v/12+1, \mathsf{rk}_{16}(2) = 6v/12+2, \mathsf{rk}_{16}(3) = 6v/12+3,$

$\mathsf{rk}_{16}(4) = 9v/12+4, \mathsf{rk}_{16}(5) = 8v/12+4, \mathsf{rk}_{16}(6) = 6v/12+4, \mathsf{rk}_{16}(7) = 11v/12+4,$

$\mathsf{rk}_{16}(8) = 7v/12+4, \mathsf{rk}_{16}(9) = 5v/12, \mathsf{rk}_{16}(\mathrm{a}) = 3v/12, \mathsf{rk}_{16}(\mathrm{b}) = 2v/12,$

$\mathsf{rk}_{16}(\mathrm{c}) = 4v/12, \mathsf{rk}_{16}(\mathrm{d}) = v/12, \mathsf{rk}_{16}(\mathrm{e}) = 10v/12+4,$ and $\mathsf{rk}_{16}(\mathrm{f}) = 0.$

Indeed, by inspection, $\{0, 1, 2, 3\}$ is a block of D_{16}, and we have verified by computer that $\mathsf{MinSum}(D_{16}, \mathsf{rk}_{16}) = 5v/4$ and $\mathsf{MaxSum}(D_{16}, \mathsf{rk}_{16}) = 29v/12 + 13$. □

As an immediate consequence of Theorem 23, we get a DiffSum bound which covers (practically) one quarter of the admissible orders of an $S(2, 4, v)$:

Corollary 7. *For all* $v \equiv 13, 16 \pmod{48}$ *with* $v \geq 61$ *there exists an* $S(2, 4, v)$ D *such that* $\mathsf{DiffSum}(D) \leq 2v - 8$.

5.4 A MinSum Bound via the $3v + 1$ Construction

It is in this section that the resolvable Bose-averaging triple systems of Chapter 4 are used to derive labellings of $S(2, 4, v)$s.

THE $3v + 1$ CONSTRUCTION ([47]). Let $(V, \mathcal{B})$ be an $S(2, 4, v)$, and X a set satisfying $|X| = 2v + 1$ and $X \cap V = \emptyset$. Let $(X, \mathcal{C})$ be a KTS$(2v + 1)$ with resolution $\mathcal{R} = \{R_1, \ldots, R_v\}$ (since $v \equiv 1, 4 \pmod{12}$, such a system exists). For $i \in [1, v]$, set $D_i = \{\{v_i, x, y, z\} : v_i \in V, \{x, y, z\} \in R_i\}$, and put $\mathcal{D} = \bigcup_i D_i$. Then $(V \cup X, \mathcal{B} \cup \mathcal{D})$ is an $S(2, 4, 3v + 1)$.

Lemma 36. *Let* $D = (X, \mathcal{C})$ *be a KTS*$(2v + 1)$ *with* $v \equiv 1, 4 \pmod{12}$ *and* $\mathsf{MinSum}(D, \mathsf{rk}) = 2v + 1$*, the greatest possible by Theorem 1. Then there exists an* $S(2, 4, u = 3v + 1)$ *having* $\mathsf{MinSum} \geq (4u + 2)/3$.

Proof. As v is admissible, there exists an $S(2, 4, v)$ $D' = (V, \mathcal{B})$. Apply the $3v + 1$ construction with D and D' as ingredients to obtain an $S(2, 4, 3v + 1)$ E. Then any labelling rk' of E whose restriction to X is rk has MinSum at least $(2v + 1) + 2v + 1 = 4v + 2 = (4u + 2)/3$. □

Thus, since the Bose-averaging triple systems of order $v \equiv 9 \pmod{18}$ are resolvable by Theorem 19, which, when labelled with the Bose labelling of [22], attain optimal MinSum v, we get:

Theorem 24. *For all* $v \equiv 13, 40 \pmod{108}$*, there exists an* $S(2,4,v)$ D *with* $\mathit{MinSum}(D) \geq (4v+2)/3$*.*

Chapter 6

BLOCK LABELLING RESOLVABLE 1-ROTATIONAL $S(2, k, v)$S

In this chapter, block labellings of certain resolvable 1-rotational Steiner 2-designs with block size $k \geq 3$ are given which, in all but one case (the *exceptional case*), make the point sums equal. A recursive construction is also shown to yield designs whose point sums are equal. Finally, we give a different block labelling of the class of Moore designs satisfying the exceptional case with improved worst-case $\mathsf{DiffSum}$.

6.1 Preliminaries

Let G be an additive group of order v, N a subgroup of G of order n, and k a positive integer. A $(G, N, k, 1)$ *difference family* is a set $\mathcal{F}$ of k-subsets of G (*base blocks*) such that $k(k-1)|\mathcal{F}| = |G \setminus N|$ and for each element $d \in G \setminus N$ there exists a unique ordered pair (g, h) of elements of some base block of $\mathcal{F}$ such that $d = g - h$. When G is cyclic of order v, we simply call $\mathcal{F}$ a $(v, n, k, 1)$ difference family. $\mathcal{F}$ is *resolvable* if the union of its base blocks is a system of representatives of the nontrivial (right) cosets of N in G, and in that case we call it a $(G, N, k, 1)$-*RDF*. A $(G, N, k, 1)$ difference family $\mathcal{F}$ with $|N| = k - 1$ is a *1-rotational* difference family. If $\mathcal{F}$ is also resolvable, then it generates a *resolvable 1-rotational Steiner 2-design*, as follows.

Construction 2 ([6])**.** Let $\mathcal{F}$ be a 1-rotational $(G, N, k, 1)$-RDF. Put

$$\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\}$$

and let S be a complete system of representatives for the cosets of N in G. Then $\mathcal{R} = \{\mathcal{P}_0 + s : s \in S\}$ gives a resolution of an $S(2, k, |G| + 1)$.

The blocks of $\mathcal{F}$ contained in the block set of the $S(2,k,|G|+1)$ D generated by the application of Construction 2 with $\mathcal{F}$ as the ingredient 1-rotational $(G,N,k,1)$-RDF are the *base blocks of* D. Perhaps the most famous application of Construction 2 uses as ingredients a class of $(\mathbb{F}_n \times \mathbb{Z}_3, \{0\} \times \mathbb{Z}_3, 4, 1)$-RDFs produced by Moore's construction.

MOORE'S CONSTRUCTION. Let $n = 4t+1$ be a prime power, and x be a primitive element of $\mathbb{F}_n$ (and thus $x^{2t} = -1 \in \mathbb{F}_n$). Then

$$\mathcal{F} = \{\{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\} : i \in [0, t-1]\}$$

is an $(\mathbb{F}_n \times \mathbb{Z}_3, \{0\} \times \mathbb{Z}_3, 4, 1)$-RDF.

A difference family produced by the Moore construction is a *Moore difference family*. Applying Construction 2 with a Moore difference family (i.e., a $(\mathbb{F}_n \times \mathbb{Z}_3, \{0\} \times \mathbb{Z}_3, 4, 1)$-RDF) yields a resolvable 1-rotational $S(2,4,3n+1)$. A difference $(\sigma, c) - (\sigma', c)$ (with subtraction performed coordinate-wise) of any two points of a Moore difference family with the same second coordinate is a *pure difference*; a difference $(\sigma, c) - (\sigma', c')$, $c \not\equiv c' \pmod 3$ of any two points of a Moore difference family with distinct second coordinates is a *mixed difference*.

We illustrate Moore's construction and Construction 2 together with a small example.

Example 4. Put $n = 5$; then 2 is a primitive element of $\mathbb{F}_5$ and hence Moore's construction yields $\mathcal{F} = \{\{(1,0), (4,0), (2,1), (3,1)\}\}$, an $(\mathbb{F}_5 \times \mathbb{Z}_3, \{0\} \times \mathbb{Z}_3, 4, 1)$-RDF. Applying in turn Construction 2 using $\mathbb{F}_5 \times \{0\}$ as the designated complete system of representatives for the cosets of $\{0\} \times \mathbb{Z}_3$ in $\mathbb{F}_5 \times \mathbb{Z}_3$, we obtain the resolvable

1-rotational $S(2,4,16)$ on point set $(\mathbb{F}_5 \times \mathbb{Z}_3) \cup \{\infty\}$ with blocks:

$$\{(1,0),(4,0),(2,1),(3,1)\},\{(1,1),(4,1),(2,2),(3,2)\},\{(1,2),(4,2),(2,0),(3,0)\},$$

$$\{(2,0),(0,0),(3,1),(4,1)\},\{(2,1),(0,1),(3,2),(4,2)\},\{(2,2),(0,2),(3,0),(4,0)\},$$

$$\{(3,0),(1,0),(4,1),(0,1)\},\{(3,1),(1,1),(4,2),(0,2)\},\{(3,2),(1,2),(4,0),(0,0)\},$$

$$\{(4,0),(2,0),(0,1),(1,1)\},\{(4,1),(2,1),(0,2),(1,2)\},\{(4,2),(2,2),(0,0),(1,0)\},$$

$$\{(0,0),(3,0),(1,1),(2,1)\},\{(0,1),(3,1),(1,2),(2,2)\},\{(0,2),(3,2),(1,0),(2,0)\},$$

and

$$\{\infty,(0,0),(0,1),(0,2)\},$$

$$\{\infty,(1,0),(1,1),(1,2)\},$$

$$\{\infty,(2,0),(2,1),(2,2)\},$$

$$\{\infty,(3,0),(3,1),(3,2)\},$$

$$\{\infty,(4,0),(4,1),(4,2)\}.$$

6.2 General Block Labellings of Resolvable 1-Rotational $S(2,k,v)$s, $k \geq 3$

Suppose that $\mathcal{F}$ is a resolvable 1-rotational $(G,N,k,1)$ difference family, so that $(G,+)$ is an additive group having N as a subgroup. For any two subsets $S, S' \subset G$ with $S' = \{s'_0, \ldots, s'_{|S'|-1}\}$, define

$$S + s'_0 + s'_1 + \cdots + s'_{|S'|-1} = \{s + s'_0 + \cdots + s'_{|S'|-1} : s \in S\},$$

and for any collection $\mathcal{C}$ of subsets of G and any subset $S' = \{s'_0, \ldots, s'_{|S'|-1}\}$ of G, define

$$\mathcal{C} + s'_0 + s'_1 + \cdots + s'_{|S'|-1} = \{S + s'_0 + \cdots + s'_{|S|-1} : S \in \mathcal{C}\}.$$

Now $S = \{0\} \cup \bigcup_{B \in \mathcal{F}} B$ is a complete system of representatives of the cosets of N in G, which we write as $S = \{s_0 = 0, s_1, \ldots, s_{|S|-1}\}$. Applying Construction 2, put

$$\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\},$$

so that $\mathcal{R} = \{\mathcal{P}_0 + s : s \in S\}$ is a resolution of an $S(2, k, |G| + 1)$, say $D = (V, \mathcal{B})$. An $\mathcal{R}$*-intervaled block labelling* of D is a block labelling $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$ whose inverse rk^{-1} maps each sub-interval of $[0, |\mathcal{B}| - 1]$ of the form

$$[i((k-1)|\mathcal{F}| + 1), (i+1)(k-1)|\mathcal{F}|],$$

where $i \in [0, |S|-1]$, to the blocks of a unique parallel class of $\mathcal{R}$ such that in particular rk assigns to $\mathcal{P}_0$ the first interval of labels $[0, (k-1)|\mathcal{F}|]$. For any such $\mathcal{R}$-intervaled block labelling, given a point $x \in V$, there exists a unique value $\ell_{x,i} \in [0, (k-1)|\mathcal{F}|]$ such that $x \in \mathsf{rk}^{-1}(i((k-1)|\mathcal{F}| + 1) + \ell_{x,i})$. Any such $\ell_{x,i}$ is a *parallel class-relative label* with respect to rk. We thus write the point sum of x with respect to rk as

$$\sum_{i=0}^{|S|-1} (i(k-1)|\mathcal{F}|) + \sum_{i=0}^{|S|-1} \ell_{x,i}. \tag{6.1}$$

The first summation of (6.1) is independent of x. The second summation is the *resolution-relative point sum of x (with respect to rk).* Labelling in this manner ensures that differences only arise in the second summation.

Let rk be an $\mathcal{R}$-intervaled block labelling of D, and suppose that $\iota = \mathsf{rk}(\{N \cup \{\infty\}\})$. Define the sequence

$$\begin{aligned} S &= (0, 1, \ldots, \iota - 1, \iota + 1, \iota + 2, \ldots, (k-1)|\mathcal{F}| - 1) \\ &= (s_0, s_1, \ldots, s_{(k-1)|\mathcal{F}|-1}), \end{aligned}$$

and for each $i \in [0, |\mathcal{F}| - 1]$, define the $(k-1)$-set $I_i = \{s_{i(k-1)}, \ldots, s_{i(k-1)+k-2}\}$. If $\mathcal{F} = \{B_0, \ldots, B_{|\mathcal{F}|-1}\}$, rk is an $(\mathcal{R}, N)$*-intervaled block labelling* of D provided that $\mathsf{rk}(\{B_i + n : n \in N\}) = I_i$ for each $i \in [0, |\mathcal{F}| - 1]$.

Table 6.1: Summary of labellings with corresponding $\mathsf{DiffSum}$ (bound)

$\lvert\mathcal{F}\rvert$	$\lvert N\rvert$	Labelling to apply	$\mathsf{DiffSum}$ of labelling
even	even	Theorem 25	0 (egalitarian)
even	odd	Theorem 25	0 (egalitarian)
odd	even	Theorem 26	0 (egalitarian)
odd	odd	Theorem 27	$\geq k-1$ and $\leq k+1$

Let rk be an $\mathcal{R}$-intervaled block labelling of D. Then rk is *development-consistent with respect to* S if for all $i \in [0,(k-1)|\mathcal{F}|]$ and $j \in [1, |S|-1]$,

$$\mathsf{rk}^{-1}(i + j((k-1)|\mathcal{F}|+1)) = \mathsf{rk}^{-1}(i) + s_j.$$

In words, for each $B \in \mathcal{P}_0$, the labels assigned by rk to $\{B+s : s \in S\}$ can be arranged into an arithmetic sequence with common difference $((k-1)|\mathcal{F}|+1)$.

Henceforth we focus on labellings that are both development-consistent and $(\mathcal{R}, N)$-intervaled. When rk is such a labelling and if S is a group, then for each $a \in [0, |\mathcal{F}|-1]$, the multiset union

$$\bigcup_{b\in[0,|S|-1], c\in I_a} \mathsf{rk}^{-1}\left(b((k-1)|\mathcal{F}|+1)+c\right)$$

is equal to k copies of G. This follows from the fact that for each $B \in \mathcal{F}$, the multiset $\{B+h+n : h \in S, n \in N\}$ consists of k copies of G.

We supply three distinct development-consistent $(\mathcal{R}, N)$-intervaled block labellings (given in Theorems 25, 26, and 27) for resolvable 1-rotational Steiner 2-designs generated by $(G, N, k, 1)$ difference families that satisfy the *labelling condition*: the union of the base blocks of the generating difference family together with $0 \in G$ is a group. Table 6.1 specifies for the four possible classes of such designs, determined by the parity of $|\mathcal{F}|$ and $|N|$, which labelling to apply and the resulting $\mathsf{DiffSum}$ (bound). We begin with a labelling of the first two classes.

Theorem 25. *Suppose that $\mathcal{F}$, with $|\mathcal{F}|$ even, is a 1-rotational $(G, N, k, 1)$-RDF such that*

$$H = \{0\} \cup \bigcup_{B \in \mathcal{F}} B$$

is a subgroup of G. Applying Construction 2, designate H as the complete system of representatives for the cosets of N in G and put $\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\}$, so that $\mathcal{R} = \{\mathcal{P}_0 + h : h \in H\}$ is a resolution of an $S(2, k, |G| + 1)$, say $D = (V, \mathcal{B})$. Then D admits an egalitarian labelling.

Proof. Let $\mathcal{F} = \{B_0, \ldots, B_{|\mathcal{F}|-1}\}$, $h_0 = 0$, $H \setminus \{0\} = \{h_1, \ldots, h_{k|\mathcal{F}|}\}$, and $N = \{n_0, \ldots, n_{k-2}\}$. Consider the $\mathcal{R}$-intervaled block labelling $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$ that is development-consistent with respect to H and satisfies the two conditions:

1. For all $i \in [0, |\mathcal{F}|/2 - 1]$ and $j \in [0, k - 2]$, $\mathsf{rk}^{-1}((k - 1)i + j) = B_i + n_j$ and $\mathsf{rk}^{-1}((k - 1)|\mathcal{F}| - (k - 1)i - j) = B_{|\mathcal{F}|-i} + n_j$.
2. $\mathsf{rk}^{-1}((k - 1)|\mathcal{F}|/2) = \{N \cup \{\infty\}\}$.

By the first condition, rk is $(\mathcal{R}, N)$-intervaled. Hence, for any $x \in G$,

$$\begin{aligned}
\sum_{i=0}^{|H|-1} \ell_{x,i} &= k \sum_{i=0}^{(|\mathcal{F}|-2)/2} (i(k - 1) + (k - 1)|\mathcal{F}| - i(k - 1)) + (k - 1)|\mathcal{F}|/2 \\
&= k(|\mathcal{F}|/2)(k - 1)|\mathcal{F}| + (k - 1)|\mathcal{F}|/2 \\
&= \frac{(k - 1)|\mathcal{F}|}{2}(k|\mathcal{F}| + 1).
\end{aligned}$$

Similarly, the resolution-relative point sum of ∞ is

$$\sum_{i=0}^{|H|-1} \ell_{\infty,i} = (k|\mathcal{F}| + 1)(k - 1)|\mathcal{F}|/2,$$

and thus rk is egalitarian. □

Next, our labelling for the third class of designs hinges on an auxiliary result.

Lemma 37. *For each even $n \geq 4$, there exist two permutations σ_n and σ'_n of $\mathbb{Z}_n$ such that*

$$\bigcup_{i \in \mathbb{Z}_n} (\sigma_n(i) + \sigma'_n(i)) = [n/2 - 1, n - 2] \cup [n, 3n/2 - 1].$$

Proof. Put $\sigma_n(i) = i$ for all $i \in \mathbb{Z}_n$. Suppose that $n \equiv 0 \pmod 4$. Then for all $i \in S = [0, n/4 - 1] \cup [3n/4, n - 1]$, put $\sigma'_n(i) = i + n/2 \pmod n$, so that

$$\bigcup_{i \in S} (\sigma_n(i) + \sigma'_n(i)) = \{n/2, n/2 + 2, \ldots, n - 2\} \cup \{n, n + 2, \ldots, 3n/2 - 2\}.$$

For all $j \in S' = [n/4, 3n/4 - 2]$, put $\sigma'_n(j) = j + n/2 + 1 \pmod n$, ensuring that

$$\bigcup_{j \in S'} (\sigma_n(j) + \sigma'_n(j)) = \{n + 1, n + 3, \ldots, 3n/2 - 3\} \cup \{n/2 - 1, n/2 + 1, \ldots, n - 3\}.$$

Finally, put $\sigma'_n(3n/4 - 1) = 3n/4$.

Now suppose that $n \equiv 2 \pmod 4$. Then for all $i \in T = [0, (n - 6)/4] \cup [(3n - 2)/4, n - 1]$, put $\sigma'_n(i) = i + n/2 + 1 \pmod n$; it follows that

$$\bigcup_{i \in T} (\sigma_n(i) + \sigma'_n(i)) = \{n/2 + 1, n/2 + 3, \ldots, n - 2\} \cup \{n, n + 2, \ldots, 3n/2 - 1\}.$$

For all $j \in T' = [(n + 2)/4, (3n - 6)/4]$, put $\sigma'_n(j) = j + n/2 \pmod n$; hence,

$$\bigcup_{j \in T'} (\sigma_n(j) + \sigma'_n(j)) = \{n + 1, n + 3, \ldots, 3n/2 - 2\} \cup \{n/2, n/2 + 2, \ldots, n - 3\}.$$

Finally, put $\sigma'_n((n - 2)/4) = (n - 2)/4$. □

Corollary 8. *For each even $n \geq 4$, there exist two permutations σ_n, σ'_n of $\mathbb{Z}_n$ and one permutation σ_{n+1} of $\mathbb{Z}_{n+1}$ with $\sigma_{n+1}(n) = n/2$ such that for all $i \in \mathbb{Z}_n$, $\sigma_n(i) + \sigma'_n(i) + \sigma_{n+1}(i) = 3n/2 - 1$.*

Proof. Apply Lemma 37 to obtain two permutations σ_n and σ'_n. Then for each $i \in \mathbb{Z}_n$, there exists a unique $j \in [0, n/2-1] \cup [n/2+1, n]$ such that $\sigma_n(i) + \sigma'_n(i) = 3n/2 - 1 - j$, so put $\sigma_{n+1}(i) = j$. □

We now label the third class of Steiner 2-designs.

Theorem 26. *Suppose that $\mathcal{F}$ is a resolvable 1-rotational $(G, N, k, 1)$-RDF such that $|\mathcal{F}| \geq 3$ is odd, $|N| \geq 4$ is even, and*

$$H = \{0\} \cup \bigcup_{B \in \mathcal{F}} B$$

is a subgroup of G. Applying Construction 2, designate H as the complete system of representatives for the cosets of N in G and put $\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\}$, so that $\mathcal{R} = \{\mathcal{P}_0 + h : h \in H\}$ is a resolution of an $S(2, k, |G| + 1)$, say $D = (V, \mathcal{B})$. Then D admits an egalitarian labelling rk.

Proof. Let $\mathcal{F} = \{B_0, \ldots, B_{|\mathcal{F}|-1}\}$, $h_0 = 0$, $H \setminus \{0\} = \{h_1, \ldots, h_{k|\mathcal{F}|}\}$, and $N = \{n_0, \ldots, n_{k-2}\}$. Applying Corollary 8, let $\sigma_{k-1}, \sigma'_{k-1}$ be two permutations of $\mathbb{Z}_{k-1}$ and σ_k a permutation of $\mathbb{Z}_k$ with $\sigma_k((k-1)/2) = k - 1$ such that for all $i \in \mathbb{Z}_{k-1}$, $\sigma_{k-1}(i) + \sigma'_{k-1}(i) + \sigma_k(i) = 3(k-1)/2 - 1$. Suppose that $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$ is $\mathcal{R}$-intervaled, development-consistent with respect to H, and has the three properties:

1. For all $i \in [1, (|\mathcal{F}| - 3)/2]$ and $j \in [0, k-2]$, $\mathsf{rk}^{-1}((k-1)i + j) = B_i + n_j$ and $\mathsf{rk}^{-1}((k-1)|\mathcal{F}| - (k-1)i - j) = B_{|\mathcal{F}|-i} + n_j$.
2. For $i \in [0, k-2]$,

   a) $\mathsf{rk}^{-1}(\sigma_{k-1}(i)) = B_0 + n_i$, and

   b) $\mathsf{rk}^{-1}((k-1)|\mathcal{F}| - k + 2 + \sigma'_{k-1}(i)) = B_{|\mathcal{F}|-1} + n_i$;

   and for $j \in [0, (k-3)/2] \cup [(k+1)/2, k-1]$, $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}| - 1)/2 + \sigma_k(j)) = B_{(|\mathcal{F}|-1)/2} + n_j$.
3. $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}| - 1)/2 + (k-1)/2) = \{N \cup \{\infty\}\}$.

The first two properties imply that rk is $(\mathcal{R}, N)$-intervaled. This, as well as Corollary 8, imply that the resolution-relative point sum of any $x \in G$ is

$$k\left(\frac{|\mathcal{F}|-3}{2}(k-1)|\mathcal{F}| + \frac{3(k-1)-2}{2} + (k-1)|\mathcal{F}| - k + 2 + \frac{(k-1)(|\mathcal{F}|-1)}{2}\right) +$$
$$(k-1)(|\mathcal{F}|-1)/2 + (k-1)/2$$
$$= \frac{|\mathcal{F}|(k-1)(|\mathcal{F}|k+1)}{2}.$$

Likewise, the resolution-relative point sum of ∞ is

$$(k|\mathcal{F}|+1)\left((k-1)(|\mathcal{F}|-1)/2 + (k-1)/2\right)$$
$$= \frac{|\mathcal{F}|(k-1)(|\mathcal{F}|k+1)}{2},$$

and thus rk is egalitarian. □

The constituents of the fourth class of Steiner 2-designs, those for which both $|\mathcal{F}|$ and $|N|$ are odd, seem the most difficult to label well. Because $|\mathcal{F}|$ is odd, we cannot partition $\mathcal{F}$ into pairs of base blocks, as we did in the labelling of Theorem 25. Because $|N|$ is also odd, we cannot assign to each ∞-block the same (middle) parallel class-relative label, for this places a significant gap between the point sum of ∞ and the average point sum. Instead, we assign to $(|H|-1)/2$ ∞-blocks the parallel class-relative label $((k-1)|F|-1)/2$, and to the remaining $(|H|+1)/2$ ∞-blocks the parallel class-relative label $((k-1)|F|+1)/2$, getting the point sum of ∞ close to the average point sum. For this reason, our labelling cannot be development-consistent. Our strategy for this case follows: We select three base blocks $B_0, B_{(|\mathcal{F}|-1)/2}$, and $B_{\mathcal{F}-1}$, and arrange the blocks of the three $(k-1)$-sets $\{B_0+n : n \in N\}$, $\{B_{(|\mathcal{F}|-1)/2}+n : n \in N\}$, and $\{B_{|\mathcal{F}|-1}+n : n \in N\}$ using three permutations. We then partition the remaining base blocks into pairs.

Lemma 38. *For all odd $n \geq 3$, there exist three permutations $\sigma_{n,0}, \sigma_{n,1}, \sigma_{n,2}$ of $[0, n-1]$ such that for $i, j \in [0, n-1]$, $\sigma_{n,0}(i) + \sigma_{n,1}(i) + \sigma_{n,2}(i) = \sigma_{n,0}(j) + \sigma_{n,1}(j) + \sigma_{n,2}(j)$.*

Proof. Define $\sigma_{n,0}(i) = n-1-i$ for all $i \in [0, n-1]$, and define $\sigma_{n,1}(j) = (n-1)/2 - j \pmod{n}$ for all $j \in [0, n-1]$. Then for $i \in [0, (n-1)/2]$, $\sigma_{n,0}(i) + \sigma_{n,1}(i) = (3n-3)/2 - 2i$ and for $j \in [(n+1)/2, n-1]$, $\sigma_{n,0}(j) + \sigma_{n,0}(j) = n-1-j+(3n-1)/2-j = (5n-3)/2-2j$. Thus, the range of $\sigma_{n,0} + \sigma_{n,1}$ over $[0, n-1]$ is $[(n-1)/2, (3n-3)/2]$. Accordingly, for all $i \in [0, n-1]$, put $\sigma_{n,2}(i) = n-1-j$ whenever $\sigma_{n,0}(i) + \sigma_{n,1}(i) = (n-1)/2 + j$, so that $\sigma_{n,0}(h) + \sigma_{n,1}(h) + \sigma_{n,2}(h) = (3n-3)/2$ for all $h \in [0, n-1]$, as desired. □

Theorem 27. *Suppose that $\mathcal{F}$ is a resolvable 1-rotational $(G, N, k, 1)$ difference family such that $|\mathcal{F}|$ and $|N|$ are odd, $|\mathcal{F}| \geq 3$, and*

$$H = \{0\} \cup \bigcup_{B \in \mathcal{F}} B$$

is a subgroup of G. Applying Construction 2, designate H as the complete system of representatives for the cosets of N in G and put $\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\}$, so that $\mathcal{R} = \{\mathcal{P}_0 + h : h \in H\}$ is a resolution of an $S(2, k, |G|+1)$, say $D = (V, \mathcal{B})$. Then D admits a block labelling rk with $\mathsf{DiffSum}$ at most $k+1$ and at least $k-1$.

Proof. Let $\mathcal{F} = \{B_0, \ldots, B_{|\mathcal{F}|-1}\}$, $h_0 = 0$, $H \setminus \{0\} = \{h_1, \ldots, h_{k|\mathcal{F}|}\}$, $N = \{n_0, \ldots, n_{k-2}\}$, and $B_\infty = \{N \cup \{\infty\}\}$. Moreover, let $\sigma_{k-1,0}, \sigma_{k-1,1}$, and $\sigma_{k-1,2}$ denote the three permutations of $[0, k-2]$ from Lemma 38. Let $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}|-1]$ be an $\mathcal{R}$-intervaled block labelling with the five properties:

- P1. For all $i \in [0, ((k-1)|\mathcal{F}|-3)/2] \cup [((k-1)|\mathcal{F}|+3)/2, (k-1)|\mathcal{F}|]$ and $j \in [1, |H|-1]$, $\mathsf{rk}^{-1}(i + j((k-1)|\mathcal{F}|+1)) = \mathsf{rk}^{-1}(i) + h_j$.
- P2. For all $i \in [1, (|\mathcal{F}|-3)/2]$ and $j \in [0, k-2]$, $\mathsf{rk}^{-1}((k-1)i + j) = B_i + n_j$ and $\mathsf{rk}^{-1}((k-1)|\mathcal{F}| - (k-1)i - j) = B_{|\mathcal{F}|-i} + n_j$.

P3. a) For all $j \in [0, k-2]$, $\mathsf{rk}^{-1}(\sigma_{k-1,0}(j)) = B_0 + n_j$.

b) For all $j \in [0, k-2]$, $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}|-1) + 1 + \sigma_{k-1,1}(j)) = B_{|\mathcal{F}|-1} + n_j$.

c) For $j \in [0, (k-4)/2]$, $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}|-1)/2 + j) = B_{(|\mathcal{F}|-1)/2} + n_{\sigma^{-1}_{k-1,2}(j)}$

d) For $j \in [k/2, k-1]$, $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}|-1)/2 + j) = B_{(|\mathcal{F}|-1)/2} + n_{\sigma^{-1}_{k-1,2}(j-1)}$.

P4. a) For all $i \in [0, (|H|-3)/2]$, $\mathsf{rk}^{-1}(i((k-1)|\mathcal{F}|+1) + ((k-1)|\mathcal{F}|-1)/2) = B_\infty + h_i$.

b) For all $i \in [(|H|-1)/2, |H|-1]$, $\mathsf{rk}^{-1}(i((k-1)|\mathcal{F}|+1) + ((k-1)|\mathcal{F}|+1)/2) = B_\infty + h_i$.

P5. a) For all $i \in [0, (|H|-3)/2]$, $\mathsf{rk}^{-1}(i((k-1)|\mathcal{F}|+1) + ((k-1)|\mathcal{F}|+1)/2) = B_{(|\mathcal{F}|-1)/2} + n_{\sigma^{-1}_{k-1,2}((k-2)/2)} + h_i$.

b) For all $i \in [(|H|-1)/2, |H|-1]$, $\mathsf{rk}^{-1}(i((k-1)|\mathcal{F}|+1) + ((k-1)|\mathcal{F}|-1)/2) = B_{(|\mathcal{F}|-1)/2} + n_{\sigma^{-1}_{k-1,2}((k-2)/2)} + h_i$.

By properties P4(a) and P4(b), rk is not development-consistent; yet by properties P2 and P3(a) - (d) it is $(\mathcal{R}, N)$-intervaled.

By properties P4(a) and P4(b), the resolution-relative point sum for ∞ is

$$\begin{aligned}\sum_{i=0}^{|H|-1} \ell_{\infty,i} &= \frac{(|H|-1)((k-1)|\mathcal{F}|-1) + (|H|+1)((k-1)|\mathcal{F}|+1)}{4} \\ &= \frac{k|\mathcal{F}|((k-1)|\mathcal{F}|-1) + (k|\mathcal{F}|+2)((k-1)|\mathcal{F}|+1)}{4} \\ &= \frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| + 1}{2}\end{aligned}$$

The resolution-relative point sum for $x \in G$ depends on which one of the following $2k+4$ mutually exclusive types it is.

T1. $x \in H + n_i$ for some $i \in \{\sigma^{-1}_{k-1,2}(0), \sigma^{-1}_{k-1,2}(1), \ldots, \sigma^{-1}_{k-1,2}((k-4)/2)\}$ and either

a) $x \in B_\infty + h_j$ for some $j \in [0, (|H|-3)/2]$, or

b) $x \in B_\infty + h_j$ for some $j \in [(|H|-1)/2, |H|-1]$.

T2. $x \in H + n_i$ for some $i \in \{\sigma_{k-1,2}^{-1}(k/2), \sigma_{k-1,2}^{-1}((k+2)/2), \ldots, \sigma_{k-1,2}^{-1}(k-2)\}$ and either

a) $x \in B_\infty + h_j$ for some $j \in [0, (|H|-3)/2]$, or

b) $x \in B_\infty + h_j$ for some $j \in [(|H|-1)/2, |H|-1]$.

T3(α, β). There exists an α-set $S \subseteq [0, (|H|-3)/2]$ and a β-set $T \subseteq [(|H|-1)/2, |H|-1]$ such that for each $i \in S$, $x \in B_{(|\mathcal{F}|-1)/2} + n_{\sigma_{k-1,2}^{-1}((k-2)/2)} + h_i$ and each $j \in T$, $x \in B_{(|\mathcal{F}|-1)/2} + n_{\sigma_{k-1,2}^{-1}((k-2)/2)} + h_j$; and either

a) $x \in B_\infty + h_j$ for some $j \in [0, (|H|-3)/2]$, or

b) $x \in B_\infty + h_j$ for some $j \in [(|H|-1)/2, |H|-1]$.

In sum, we have the set of $2k+4$ point types

$$\{\text{T1(a)}, \text{T1(b)}, \text{T2(a)}, \text{T2(b)}\} \bigcup \bigcup_{\{(\alpha,\beta):\alpha+\beta=k\}} \{\text{T3}(\alpha,\beta)\text{(a)}, \text{T3}(\alpha,\beta)\text{(b)}\}.$$

If x is of type T1(a) then its resolution-relative point sum is

$$k\left(\frac{3k-6}{2} + \frac{3(k-1)(|\mathcal{F}|-1)+2}{2} + \frac{|\mathcal{F}|-3}{2} \cdot (k-1)|\mathcal{F}|\right) + \frac{(k-1)|\mathcal{F}|-1}{2}$$
$$= \frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| - k - 1}{2}.$$

Thus, if x is of type T1(b), its resolution-relative point sum is

$$\frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| - k + 1}{2}.$$

If x is of type T2(a), its resolution-relative point sum is

$$k\left(\frac{3k-6}{2} + \frac{3(k-1)(|\mathcal{F}|-1)+4}{2} + \frac{|\mathcal{F}|-3}{2} \cdot (k-1)|\mathcal{F}|\right) + \frac{(k-1)|\mathcal{F}|-1}{2}$$
$$= \frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| + k - 1}{2}.$$

Hence, if x is of type T2(b), its resolution-relative point sum is

$$\frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| + k + 1}{2}.$$

The calculations for the T3 types derive from the calculations of the T1 and T2 types. Indeed, the T3 types may be ordered increasingly by their corresponding resolution-relative point sums as the sequence

$$(\mathrm{T3}(0,k)(\mathrm{a}), \mathrm{T3}(0,k)(\mathrm{b}), \mathrm{T3}(1,k-1)(\mathrm{a}), \mathrm{T3}(1,k-1)(\mathrm{b}), \ldots, \mathrm{T3}(k,0)(\mathrm{b})),$$

where a T3$(0,k)$(a) point has the least resolution-relative point sum, equal to the resolution-relative point sum of a T1(a) point, and a T3$(k,0)$(b) point has the greatest resolution-relative point sum, equal to the resolution-relative point sum of a T2(b) point. Thus, the $\mathsf{DiffSum}$ of rk is at most the difference between the resolution-relative point sums of a type T2(b) and a type T1(a) point, which is

$$\frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| + k + 1 - (|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| - k - 1)}{2}$$
$$= k + 1.$$

Moreover, there must exist a point of type T1(a) or T1(b), and there must exist a point of type T2(a) or T2(b). Hence, the $\mathsf{DiffSum}$ is at least $k-1$. □

We now verify that egalitarian labellings cannot exist for this fourth class of Steiner 2-designs. As noted in [15], the average point sum of an $S(t,k,v)$ D is $r(b-1)/2$, where r is the replication number and b is the number of blocks of D. Hence, if b is even and r is odd, then the average point sum is not integral, and thus D cannot admit an egalitarian labelling. Now let $\mathcal{B}$ be the block set of a resolvable 1-rotational Steiner 2-design D generated by a $(G,N,k,1)$-RDF $\mathcal{F}$. Then D has replication number $r = |G|/(k-1)$. Supposing that $|\mathcal{F}|$ and $|N|$ are odd, then since

$$|\mathcal{F}| = \frac{1}{k}\left(\frac{|G|}{|N|} - 1\right)$$
$$\iff |G| = (k|\mathcal{F}| + 1)|N|,$$

$|G|$ is odd, and hence r is odd. Moreover, a parallel class of $\mathcal{B}$ has $|\mathcal{F}|+1$ blocks; that is, an even number of blocks, so that $|\mathcal{B}|$ is even.

6.3 Meeting the labelling condition

In this section we show that many of the difference families in the literature, both directly and recursively constructed, satisfy the labelling condition imposed on all the designs labelled in Section 6.2.

6.3.1 Direct Constructions

It is common to construct 1-rotational $(G, N, k, 1)$-RDFs with the form: $G = \mathbb{F}_q \oplus H$ and $N = \{0\} \oplus H$, where H is an (additive) group. Following [4], this is the *standard form*. Given any such difference family, the union of its base blocks together with $0 \in G$ must be a subgroup of G, because any arbitrary system of representatives for the cosets of N in G is a group isomorphic to $\{0\} \oplus H$. To our knowledge, every direct construction in the literature of an infinite class of 1-rotational $(G, N, k, 1)$-RDFs has the standard form. Small examples exist that do not have the standard form. For instance, Example 1.3 of [3] is a cyclic $(51, 3, 4, 1)$-RDF, the union of whose base blocks together with 0 do not form a subgroup of $\mathbb{Z}_{51}$. As another instance, every 1-rotational KTS(33) is either a $(\mathbb{Z}_{32}, \{0, 16\}, 3, 1)$-RDF or a $(Q_{32}, \{1, x^8\}, 3, 1)$-RDF, where Q_{32} is the dicyclic group of order 32 [8]. It is routine to verify that not one of the former kind of RDFs can satisfy the labelling condition.

6.3.2 Recursions

In [35] Jimbo and Vanstone present a recursive construction for resolvable 1-rotational Steiner 2-designs. In [6] Buratti and Zuanni rephrase their construction in the language of the difference families. We first define a key ingredient of their construction. A $(w, k, 1)$ *difference matrix* is a $k \times w$ matrix $D = (d_{ij})$ with entries from $\mathbb{Z}_w$ such that for each $1 \le i < j \le k$,

$$\mathbb{Z}_w = \{d_{i\ell} - d_{j\ell} : 1 \le \ell \le k\}.$$

A $(w, k, 1)$ difference matrix D is *good* if no row of D contains any element of $\mathbb{Z}_w$ more than once.

Construction 3 (Buratti and Zuanni's restatement of the Jimbo-Vanstone construction [6]). Let $\mathcal{D} = \{D_i : i \in I\}$ and $\mathcal{E} = \{E_j : j \in J\}$ be resolvable $((k-1)v, k-1, k, 1)$ and $((k-1)w, k-1, k, 1)$ difference families, respectively. Suppose that $\gcd(w, k-1) = 1$ and let $D = (d_{ih})$ be a good $(w, k, 1)$ difference matrix. For each $D_i = \{d_{i1}, d_{i2}, \ldots, d_{ik}\} \in \mathcal{D}$ and each $h \in [1, w]$, put $D_{(i,h)} = \{d_{i1} + (k-1)va_{1h}, d_{i2} + (k-1)va_{2h}, \ldots, d_{ik} + (k-1)va_{kh}\}$. For each $E_j = \{e_{j1}, e_{j2}, \ldots, e_{jk}\} \in \mathcal{E}$, put $E_j^* = \{ve_{j1}, ve_{j2}, \ldots, ve_{jk}\}$. Then the set

$$\mathcal{F} = \{D_{(i,h)} \pmod{(k-1)vw} : i \in I, h \in [1, w]\} \cup \{E_j^* \pmod{(k-1)vw} : j \in J\}$$

is a $((k-1)vw, k-1, k, 1)$-RDF.

Any difference family yielded by an application of Construction 3 satisfies the labelling condition, provided that the ingredient families of the application also satisfy it.

Theorem 28. *Let $\mathcal{D} = \{D_i : i \in I\}$ and $\mathcal{E} = \{E_j : j \in J\}$ be resolvable $((k-1)v, k-1, k, 1)$ and $((k-1)w, k-1, k, 1)$ difference families, respectively, that each satisfy the labelling condition. Suppose that* $\gcd(w, k-1) = 1$ *and let $D = (d_{ih})$ be a good $(w, k, 1)$ difference matrix. Then with $\mathcal{D}$ and $\mathcal{E}$ as ingredients of Construction 3, the resulting $((k-1)vw, k-1, k, 1)$ difference family $\mathcal{F}$ also meets the labelling condition.*

Proof. By assumption, the set $\bigcup_{D \in \mathcal{D}} D \cup \{0\}$ is a subgroup of $\mathbb{Z}_{(k-1)v}$ of order v, and is thus precisely the set of all distinct multiples of $k-1$ modulo $(k-1)v$. Likewise, the union of the base blocks of $\mathcal{E}$ together with 0 is precisely the set of all distinct multiples of $k-1$ modulo $(k-1)w$. Hence, as $\mathcal{F}$ is resolvable, the union of its base blocks consists of all distinct nonzero multiples of $k-1$ modulo $(k-1)vw$. Thus, adjoining to this union the zero element must give us a subgroup (isomorphic to $\mathbb{Z}_{vw}$) of $\mathbb{Z}_{(k-1)vw}$. □

6.3.3 General asymptotic constructions

Here are some asymptotic constructions that instantiate the standard form.

Theorem 29 (Corollary 4.2 of [5])**.** *For any integer k and any prime $p \equiv k(k+1)+1 \pmod{2k(k+1)}$ sufficiently large there exists a $((k-1)p, k-1, k, 1)$-RDF.*

Hence applying Construction 2, we have:

Corollary 9. *For any integer k and any prime $p \equiv k(k+1)+1 \pmod{2k(k+1)}$ sufficiently large there exists a resolvable 1-rotational $S(2, k, (k-1)p+1)$.*

The next four results are from [20].

Theorem 30. *Let p be a prime power satisfying $p \equiv 3 \pmod 4$. Then for any prime power $q \equiv 1 \pmod{p+1}$ sufficiently large, there exists a resolvable 1-rotational $S(2, p+1, pq+1)$.*

Theorem 31. *Let p and $p+2$ be twin prime powers satisfying $p > 2$. Then for any prime power $q \equiv 1 \pmod{p(p+2)+1}$ sufficiently large, there exists a resolvable 1-rotational $S(2, p(p+2)+1, p(p+2)q+1)$.*

Theorem 32. *Let $m \geq 3$ be an integer. Then for any sufficiently large prime power $q \equiv 1 \pmod{2^m}$, there exists a resolvable 1-rotational $S(2, 2^m, (2^m-1)q+1)$.*

Theorem 33. *Let p be a prime power satisfying $p \equiv 1 \pmod 4$. Then for any prime power $q \equiv 1 \pmod{2p+2}$ sufficiently large, there exists a resolvable 1-rotational $S(2, p+1, pq+1)$.*

6.3.4 Existence tables for small k

Attention has focused on producing resolvable 1-rotational $S(2,k,v)$s of the standard form with $k \in [3,9]$. In general the known orders v for such Steiner 2-designs do not originate solely from asymptotic constructions. Table 6.2 gives (some) orders v for which a resolvable 1-rotational $S(2,k,v)$ exists whose generating RDF satisfies the conditions of either Theorem 25 or Theorem 26, so that the design admits an egalitarian labelling. For $k = 3, 4$ we also provide the orders obtained by feeding the appropriate subset of the base set of orders obtained via the constructions of [46] and [43], respectively, into the Jimbo-Vanstone construction (JVC). For $k = 5$ we provide a collection of orders produced via an asymptotic construction [39] that is tailored to that specific blocksize. Table 6.3 gives (some) orders v for which a resolvable 1-rotational $S(2,k,v)$ exists whose generating RDF satisfies the conditions of Theorem 27, so that the design admits a (non-egalitarian) labelling having DiffSum at most $k+1$ and at least $k-1$.

Table 6.2: Orders of resolvable 1-rotational $S(2,k,v)$s with egalitarian labelling

k	v
3	$v \in \{8s+1:$ each prime factor of s is congruent to 1 mod 6$\}$ [7], $v \in \{2s+1:$ each prime factor of s is congruent to 1 mod 6$\}$([46] + JVC)
4	$v \in \{3s+1 : s$ is a product of primes, each congruent to 1 mod 4, such that the number of primes congruent to 5 mod 8 is even$\}$ ([43] + JVC)
5	$v \in \{125, 725, 845, 965, 1085, 1685, 2285, 2405, 2525, 2765, 3005, 3965\}$[4] and $v = 4p+1$ for p sufficiently large such that $p \equiv 1 \pmod{30}$ and $(11+5\sqrt{5})/2$ mod p is not a cube [39]
6	$v \in \{5p+1 : p = 12t+1$ is prime, $p \notin \{13, 37\}$, and $(p-1)/6 \equiv 0 \pmod 2\}$ [3]
7	$v \in \{1687, 5719, 13783, 17815, 27895, 35287, 37303, 37975, 39319, 45367, 49399,$ 52087,55447,58135$\}$[4]
8	$v = 1576$ [20] $v \in \{7p+1 : p = 8t+1$ is prime, $p \neq 17,$ and $(p-1)/8 \equiv 0 \pmod 2\}$ [3]
9	$v \in \{7929, 12249, 52569, 77049\}$ [4]

Table 6.3: Orders of resolvable 1-rotational $S(2,k,v)$ admitting $k-1 \leq \mathsf{DiffSum} \leq k+1$ labelling

k	v
4	$v \in \{3s+1 : s$ is a product of primes, each congruent to 1 mod 4, such that the number of primes congruent to 5 mod 8 is odd$\}$ ([43] + JVC)
6	$v \in \{5p+1 : p = 12t+1$ is prime and $(p-1)/6 \equiv 1 \pmod 2\}$ [3]
8	$v \in \{624, 2976\}$ [20] $v \in \{7p+1 : p = 8t+1$ is prime, $p \neq 89,$ and $(p-1)/8 \equiv 1 \pmod 2\}$ [3]

6.4 Improving the DiffSum bound for Moore Designs

The aim of this section is to demonstrate that those Moore difference families having an odd number of base blocks generate via Construction 2 Steiner 2-designs admitting labellings with DiffSum at most 3. Were one to apply Theorem 27 to label such designs, the DiffSum would, at worst, be $k+1=5$ (and at best be $k-1=3$). However, that is not the approach we take.

Let $n = 4t+1$ be a prime power. For simplicity, for any $\sigma_i, \sigma_j \in \mathbb{F}_n$ and $c \in \mathbb{Z}_3$, denote $(\sigma_i, c) \oplus (\sigma_j, 0) = (\sigma_i + \sigma_j, c)$ by $(\sigma_i, c) \oplus \sigma_j$; also define $\infty \oplus \sigma_i = \infty$. For any subset $S \subseteq \mathbb{F}_n \times \mathbb{Z}_3$ define $S \oplus \sigma_j = \{(\sigma_i, c) \oplus \sigma_j : (\sigma_i, c) \in S\}$ and for any set $\mathcal{S}$ of subsets of $\mathbb{F}_n \times \mathbb{Z}_3$, define $\mathcal{S} \oplus \sigma_j = \{S \oplus \sigma_j : S \in \mathcal{S}\}$. For $\sigma_i, \sigma_j \in \mathbb{F}_n^\times$ and $c \in \mathbb{Z}_3$, let $(\sigma_i, c) \cdot \sigma_j = (\sigma_j \cdot \sigma_i, c)$, with multiplication performed over $\mathbb{F}_n^\times$. For any subset $S \subseteq \mathbb{F}_n \times \mathbb{Z}_3$, define $S \cdot \sigma_j = \{(\sigma_i, c) \cdot \sigma_j : (\sigma_i, c) \in S\}$.

A Moore difference family $\mathcal{F}$ has the standard form and thus meets the labelling condition, so any Moore difference family with an even number of base blocks (equivalently, t is even) admits an egalitarian labelling. When $|\mathcal{F}|$ is odd (equivalently, t is odd) we do not develop the base parallel class, henceforth denoted $\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in \{0\} \oplus \mathbb{Z}_3\}$, over the union of the base blocks of $\mathcal{F}$, but instead develop it, as Moore did in [43], over $\mathbb{F}_n \times \{0\}$, to obtain the *classical* resolution $\mathcal{R} = \{\mathcal{P}_0 \oplus \sigma : \sigma \in \mathbb{F}_n\}$. The resolvable 1-rotational $S(2, 4, 3n + 1)$ with classical resolution $\mathcal{R}$ is the *Moore design of order* $3n+1$ (MD$(3n+1)$) and $\mathcal{F}$ is its *generating* Moore difference family. A block of MD$(3n + 1)$ in the generating Moore difference family is a *base* block. Blocks of MD$(3n+1)$ having two points with second coordinate $i \pmod 3$ and two points with second coordinate $i + 1 \pmod 3$ are *secants*; blocks containing ∞ are ∞-*blocks*. A secant of MD$(3n + 1)$ is of *type* i if the set of second coordinates of its constituent points is $\{i, (i + 1) \bmod 3\}$.

Let $p = 4t + 1$ be a prime, set

1. $\{c_0, c_1\} = \{0, 1\}$,
2. $D = \bigcup_{i=0}^{(p-1)/2} \{B \oplus i\}$,
3. $Y_{c_0} = \{y \in \mathbb{F}_p : \exists B_1, B_2 \in D, B_1 \neq B_2, \text{ s.t. } (y, c_0) \in B_1 \cap B_2\}$, and
4. $N_{c_1} = \{n \in \mathbb{F}_p : \forall B \in D, (n, c_1) \notin B\}$,

and define the *ordered* classical resolution to be the classical resolution $\mathcal{R} = \{\mathcal{P}_0, \ldots, \mathcal{P}_{p-1}\}$ of the MD$(3p + 1)$ such that $\mathcal{P}_i = \mathcal{P}_0 \oplus i$ for all $i \in [0, p - 1]$. A secant base block B (necessarily of type 0) of MD$(3p + 1)$ is (c_0, c_1)-*special* if the two conditions are satisfied:

1. For $y \in Y_{c_0}$ the unique ∞-block that contains (y, c_0) occurs in $\mathcal{P}_j$ for some $j \in [0, (p - 1)/2]$, and
2. for $z \in N_{c_1}$ the unique ∞-block that contains (z, c_1) occurs in $\mathcal{P}_j$ for some $j \in [(p + 1)/2, p - 1]$.

Equivalently, B is (c_0, c_1)-special if:

1. For $y \in Y_{c_0}$, $y \in [0, (p - 1)/2]$, and
2. for $z \in N_{c_1}$, $z \in [(p + 1)/2, p - 1]$.

Lemma 39. *Let $p = 4t+1$ be a prime, x a primitive element of $\mathbb{F}_p$, $\{0,1\} = \{c_0, c_1\}$, and $B = \{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\}$ a secant base block of $MD(3p+1)$. Then B is (c_0, c_1)-special if and only if*

$$x^i, x^{i+t} \pmod{p} \in [1, (p-1)/4] \cup [(3p+1)/4, p-1].$$

Proof. Set

1. $D = \bigcup_{i=0}^{(p-1)/2} \{B \oplus i\}$,
2. $Y_{c_0} = \{y \in \mathbb{F}_p : \exists B_1, B_2 \in D, B_1 \neq B_2, \text{ s.t. } (y, c_0) \in B_1 \cap B_2\}$, and
3. $N_{c_1} = \{n \in \mathbb{F}_p : \forall B \in D, (n, c_1) \notin B\}$.

For both directions of the proof of the biconditional, we suppose without loss of generality that $c_0 = 0$ and $c_1 = 1$.

The proof of the forward direction has two cases. First, suppose to the contrary that B is (c_0, c_1)-special and without loss of generality that $x^i \in [(p+3)/4, (p-1)/2]$; then $-x^i \in [(p+1)/2, (3p-3)/4]$. But

$$(p+3)/4 + (p-1)/2 = (3p+1)/4 > (3p-3)/4,$$

and thus there exists some $y > (p-1)/2$ with $y \in Y_{c_0}$, a contradiction. Second, suppose to the contrary and without loss of generality that $x^{i+t} \in [(p+3)/4, (p-1)/2]$; then $-x^{i+t} \in [(p+1)/2, (3p-3)/4]$. But

$$(3p-3)/4 + (p-1)/2 = (5p-5)/4 \equiv (p-5)/4 \pmod{p}$$

and $(p-5)/4 < (p-1)/4 < (p+3)/4$; thus $(p-1)/4 \in N_{c_1}$, a contradiction

For the reverse direction, suppose without loss of generality that $x^i, x^{i+t} \in [1, (p-1)/4]$ so that $-x^i, -x^{i+t} \pmod{p} \in [(3p+1)/4, p-1]$. But

$$(p-1)/4 + (p-1)/2 = (3p-3)/4 < (3p+1)/4$$

and therefore for all $y \in Y_{c_0}$, $y \leq (p-1)/2$. Moreover,

$$(3p+1)/4 + (p-1)/2 = (5p-1)/4 \equiv (p-1)/4 \pmod p$$

and hence for all $n \in N_{c_1}$, $n > (p-1)/2$. □

Lemma 40. *Let*

$$B_1 = \{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\}, \text{ and}$$
$$B_2 = \{(x^j, 0), (-x^j, 0), (x^{j+t}, 1), (-x^{j+t}, 1)\}$$

be two distinct base blocks of MD$(3p+1)$, with $p = 4t+1$ a prime, so that $i, j \in [0, t-1]$. Choose $\alpha_1 \in \{x^i, -x^i\}$, $\alpha_2 = \{x^j, -x^j\}$, $\beta_1 = \{x^{i+t}, -x^{i+t}\}$, and $\beta_2 = \{x^{j+t}, -x^{j+t}\}$ such that $S = \{\alpha_1, \alpha_2, \beta_1, \beta_2\} \subset [1, (p-1)/2]$. Then if $\max(S) - \min(S) \leq (p-1)/4$, *there exists a (c_0, c_1)-special base block of MD$(3p+1)$.*

Proof. There are four cases to treat:

1. $x^t\alpha_1 \equiv \beta_1 \pmod p$ and $x^t\alpha_2 \equiv \beta_2 \pmod p$,
2. $x^t\alpha_1 \equiv \beta_1 \pmod p$ and $x^t\alpha_2 \equiv -\beta_2 \pmod p$,
3. $x^t\alpha_1 \equiv -\beta_1 \pmod p$ and $x^t\alpha_2 \equiv \beta_2 \pmod p$, or
4. $x^t\alpha_1 \equiv -\beta_1 \pmod p$ and $x^t\alpha_2 \equiv -\beta_2 \pmod p$.

Supposing that $\max\{S\} - \min\{S\} \leq (p-1)/4$, then by Lemma 39, each of the following four sets, subject to the constraints of the corresponding case, gives the $\mathbb{F}_p$-coordinates of the points of a (c_0, c_1)-special base block of MD$(3p+1)$ (with all arithmetic performed modulo p):

1. $\{\alpha_1-\alpha_2, -\alpha_1+\alpha_2, x^t(\alpha_1-\alpha_2), x^t(\alpha_2-\alpha_1)\} = \{\alpha_1-\alpha_2, -\alpha_1+\alpha_2, \beta_1-\beta_2, \beta_2-\beta_1\}$,
2. $\{\alpha_2 - \beta_1, -\alpha_2 + \beta_1, x^t(\alpha_2 - \beta_1), x^t(-\alpha_2 + \beta_1)\} = \{\alpha_2 - \beta_1, -\alpha_2 + \beta_1, -\beta_2 + \alpha_1, \beta_2 - \alpha_1\}$,

3. $\{\alpha_1-\beta_2, \beta_2-\alpha_1, x^t(\alpha_1-\beta_2), x^t(\beta_2-\alpha_1)\} = \{\alpha_1-\beta_2, \beta_2-\alpha_1, -\beta_1+\alpha_2, -\alpha_2+\beta_1\}$, and

4. $\{-\alpha_1+\alpha_2, \alpha_1-\alpha_2, x^t(-\alpha_1+\alpha_2), x^t(\alpha_1-\alpha_2)\} = \{-\alpha_1+\alpha_2, \alpha_1-\alpha_2, \beta_1-\beta_2, -\beta_1+\beta_2\}$.

□

Let $p = 4t+1$ be prime, $\mathcal{F}$ the generating Moore difference family for MD$(3p+1)$, and $B \in \mathcal{F}$. Then $(\sigma, c) \in \mathbb{F}_p \times \{1, 2\}$ is a *mixed difference of* B (or the mixed difference *occurs in* B) if there exist $b_i, b_j \in B$ for which $(\sigma, c) = b_i - b_j$; specifically, (σ, c) is a *mixed difference (of* B*) between* b_i *and* b_j. There are two mixed differences that occur between b_i and b_j: one whose $\mathbb{F}_p$-coordinate, say σ, is in $[1, (p-1)/2]$ and the other whose $\mathbb{F}_p$-coordinate is $-\sigma \pmod p \in [(p+1)/2, p-1]$; the former is the *pairwise-minimum* mixed difference between b_i and b_j. As $B = \{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\}$, with $i \in [0, t-1]$, a routine verification gives the following result:

Lemma 41. *Let* $p = 4t+1$ *be prime, and* $\mathcal{F}$ *the generating Moore difference family for MD*$(3p+1)$*. Given* $B \in \mathcal{F}$*, if* (σ, c_1) *is a mixed difference that occurs between two elements of* B*, then* (σ, c_2) *is a mixed difference that occurs between the remaining two elements of* B*, where* $\{c_1, c_2\} = \{1, 2\}$*.*

A mixed difference of B is *split* if it occurs between one element whose $\mathbb{F}_p$-coordinate is in $[1, (p-1)/2]$ and a second element whose $\mathbb{F}_p$-coordinate is in $[(p+1)/2, p-1]$. Conversely, a mixed difference of B is *joined* if it occurs between two elements, both of whose $\mathbb{F}_p$-coordinates are in $[1, (p-1)/2]$, or between two elements, both of whose $\mathbb{F}_p$-coordinates are in $[(p+1)/2, p-1]$.

Lemma 42. *Let* $p = 4t+1$ *be prime, and* $\mathcal{F}$ *the generating Moore difference family for MD*$(3p+1)$*. If* (σ, c) *is a pairwise-minimum split mixed difference of some* $B \in \mathcal{F}$*,* *then there exists a (pairwise-minimum) joined mixed difference (σ', c) of B, with $\sigma' < \sigma$.*

Proof. Let $B = \{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\}$, with $i \in [0, t-1]$, and suppose without loss of generality that the two mixed differences between $(x^{i+t}, 1)$ and $(x^i, 0)$ are split, so that $x^i \in [1, (p-1)/2]$ and $x^{i+t} \in [(p+1)/2, p-1]$. There are two major cases to cover, and henceforth, we assume that all arithmetic is performed modulo p.

Case 1. Suppose that $x^i < -x^{i+t}$. Then there are two subcases to cover:

1. $x^i - x^{i+t}$ is the $\mathbb{F}_p$-coordinate of the pairwise-minimum split mixed difference between $(x^{i+t}, 1)$ and $(x^i, 0)$, or
2. $x^{i+t} - x^i$ is the $\mathbb{F}_p$-coordinate of the pairwise-minimum split mixed difference between $(x^{i+t}, 1)$ and $(x^i, 0)$.

Suppose that the first subcase holds. Then $-x^{i+t} - x^i < x^i + -x^{i+t}$; that is, the $\mathbb{F}_p$-coordinate of the pairwise-minimum joined mixed difference between $(-x^{i+t}, 1)$ and $(x^i, 0)$ is less than $x^i - x^{i+t}$. Suppose that the second subcase holds. Then $-x^{i+t} - x^i < x^{i+t} - x^i$; that is, the $\mathbb{F}_p$-coordinate of the pairwise-minimum joined mixed difference between $(-x^{i+t}, 1)$ and $(x^i, 0)$ is less than $x^{i+t} - x^i$.

Case 2. Suppose that $-x^{i+t} < x^i$. Then there are two subcases to cover:

1. $x^i - x^{i+t}$ is the $\mathbb{F}_p$-coordinate of the pairwise-minimum mixed difference between $(x^{i+t}, 1)$ and $(x^i, 0)$, or
2. $x^{i+t} - x^i$ is the $\mathbb{F}_p$-coordinate of the pairwise-minimum mixed difference between $(x^{i+t}, 1)$ and $(x^i, 0)$.

Suppose that the first subcase holds. Then $x^i - (-x^{i+t}) < x^i - x^{i+t}$; that is, the $\mathbb{F}_p$-coordinate of the pairwise-minimum joined mixed difference between $(-x^{i+t}, 1)$ and $(x^i, 0)$ is less than $x^i - x^{i+t}$. Suppose that the second subcase holds. Then $x^{i+t} - (-x^i) < x^{i+t} - x^i$; that is, the $\mathbb{F}_p$-coordinate of the pairwise-minimum joined mixed difference between $(x^{i+t}, 1)$ and $(-x^i, 0)$ is less than $x^{i+t} - x^i$. □

Henceforth, we identify every point of a Moore difference family with its $\mathbb{F}_p$-coordinate.

Lemma 43. *Let $p = 4t + 1$ be prime with $p \geq 13$, $\mathcal{F}$ the generating Moore difference family for MD$(3p + 1)$, and $M = \{1, 2, 3, 4\}$ the four (pairwise-minimum) mixed differences of $\mathcal{F}$. Then every possible way in which distinct $m, m' \in M$ can occur as mixed differences in some $B \in \mathcal{F}$ is given, thus:*

1. *If mixed differences 1 and 2 occur in some $B \in \mathcal{F}$, then either $\{(p-3)/2, (p-1)/2, (p+1)/2\} \subset B$ or $\{(p-3)/2, (p-1)/2, (p+3)/2\} \subset B$.*
2. *If mixed differences 1 and 3 occur in some $B \in \mathcal{F}$, then either $\{1, 2, p-1\} \subset B$ or $\{1, 2, p-2\} \subset B$.*
3. *If mixed differences 1 and 4 occur in some $B \in \mathcal{F}$, then either $\{(p-5)/2, (p-3)/2, (p+3)/2\} \subset B$ or $\{(p-5)/2, (p-3)/2, (p+5)/2\} \subset B$.*
4. *If mixed differences 2 and 3 occur in some $B \in \mathcal{F}$, then either $\{(p-5)/2, (p-1)/2, (p+1)/2\} \subset B$ or $\{(p-5)/2, (p-1)/2, (p+5)/2\} \subset B$.*
5. *If mixed differences 2 and 4 occur in some $B \in \mathcal{F}$, then either $\{1, 3, p-3\} \subset B$ or $\{1, 3, p-1\} \subset B$.*
6. *If mixed differences 3 and 4 occur in some $B \in \mathcal{F}$, then either $\{(p-7)/2, (p-1)/2, (p+1)/2\} \subset B$ or $\{(p-7)/2, (p-1)/2, (p+7)/2\} \subset B$.*

Proof. By Lemma 41, p is sufficiently large that it cannot be the case that for distinct $m, m' \in M$, mixed difference m occurs between two elements of B, while m' occurs between the remaining two elements of B. Hence, at most two distinct mixed differences of M can occur in $B \in \mathcal{F}$, and these mixed differences occur between b and b_1 and b and b_2, where $b, b_1, b_2 \in B$ are distinct. It is routine to verify that this leaves only two possible valuations of the triple $\{b, b_1, b_2\}$ for each pair of mixed differences, as given in the statement of this lemma. □

We are now equipped to describe a procedure for obtaining a (c_0, c_1)-special base block.

Lemma 44. *Let $p = 4t + 1$ be prime with $p \geq 29$. Then MD$(3p + 1)$ has a (c_0, c_1)-special base block.*

Proof. Let $\mathcal{F}$ be the generating Moore difference family for MD$(3p + 1)$. There are sixteen potential cases to cover, depending on whether $1, 2, 3,$ and 4 are the $\mathbb{F}_p$-coordinates of a (pairwise-minimum) joined or split mixed difference of $\mathcal{F}$. In fact, eight of these cases are without substance; by Lemma 42, 1 cannot be a split mixed difference. Here are the remaining eight:

1. 1 is joined, 2 is joined, 3 is joined, and 4 is joined.
2. 1 is joined, 2 is joined, 3 is joined, and 4 is split.
3. 1 is joined, 2 is joined, 3 is split, and 4 is joined.
4. 1 is joined, 2 is joined, 3 is split, and 4 is split.
5. 1 is joined, 2 is split, 3 is joined, and 4 is joined.
6. 1 is joined, 2 is split, 3 is joined, and 4 is split.
7. 1 is joined, 2 is split, 3 is split, and 4 is joined.
8. 1 is joined, 2 is split, 3 is split, and 4 is split.

Suppose that the first case holds. Then by Lemma 43, the blocks of $\mathcal{F}$ containing mixed differences $1, 2, 3,$ and 4 are distinct. For $i \in [1, 4]$, let B_i denote the block in $\mathcal{F}$ having mixed difference i, and suppose that $B_i \cap [1, (p-1)/2] = \{\alpha_i, \beta_i\}$. Now check if either $\{\alpha_1, \beta_1\}$ or $\{\alpha_2, \beta_2\}$ is contained in $[1, (p-1)/4]$; if so, then by Lemma 39, we are done. If not, then there are two subcases to consider:

1.1. $\{\alpha_1, \beta_1, \alpha_2, \beta_2\} \subset [(p-1)/4, (p-1)/2]$, or

1.2. there exists an $i \in \{1, 2\}$ such that $\alpha_i < (p-1)/4$ and $\beta_i > (p-1)/4$, or vice-versa.

If subcase 1.1 holds, then by Lemma 40, we are done. If subcase 1.2 holds, then $\{\alpha_2, \beta_2\} = \{(p-5)/4, (p+3)/4\}$. If $\{\alpha_1, \beta_1\} \neq \{(p-3)/2, (p-1)/2\}$, then apply Lemma 40. Otherwise, if either $\{\alpha_3, \beta_3\}$ or $\{\alpha_4, \beta_4\}$ is contained in $[1, (p-1)/4]$, then by Lemma 39, we are done. If not, then there are two sub-subcases to consider:

1.2.1. $\{\alpha_3, \beta_3, \alpha_4, \beta_4\} \subset [(p-1)/4, (p-1)/2]$, or

1.2.2. there exists an $i \in \{3, 4\}$ such that $\alpha_i < (p-1)/4$ and $\beta_i > (p-1)/4$, or vice-versa.

If subcase 1.2.1 holds, then apply Lemma 40. If subcase 1.2.2 holds, then $\{\alpha_4, \beta_4\} = \{(p-9)/4, (p+7)/4\}$ and $\{\alpha_3, \beta_3\} \subset [(p-1)/4, (p-5)/2]$. But setting $S = \{\alpha_3, \beta_3, \alpha_4, \beta_4\}$, then

$$\begin{aligned} \max\{S\} - \min\{S\} &\leq (p-5)/2 - (p-9)/4 \\ &= (p-1)/4, \end{aligned}$$

and thus an application of Lemma 40 finishes the job.

Suppose that the second case holds. Then by Lemma 42, there are three subcases to treat:

2.1. Mixed differences 1 and 4 occur in some $B \in \mathcal{F}$,

2.2. Mixed differences 2 and 4 occur in some $B \in \mathcal{F}$, or

2.3. Mixed differences 3 and 4 occur in some $B \in \mathcal{F}$.

If subcase 2.1 holds, then by Lemma 43, $\{(p-5)/2, (p-3)/2\} \subset B$. Let $\{\alpha_2, \beta_2\}$ be the subset of the block of $\mathcal{F}$ containing (joined) mixed difference 2 that is contained in $[1, (p-1)/2]$. If $\{\alpha_2, \beta_2\} \subset [1, (p-1)/4]$, then apply Lemma 39. If not, then there are two sub-subcases to consider:

2.1.1. $\{\alpha_2, \beta_2\} \subset [(p-1)/4, (p-1)/2]$

2.1.2. $\alpha_2 < (p-1)/4$ and $\beta_2 > (p-1)/4$, or vice-versa.

If sub-subcase 2.1.1 holds, then apply Lemma 40. If sub-subcase 2.1.2 holds, then $\{\alpha_2, \beta_2\} = \{(p-5)/4, (p+3)/4\}$, and $(p-3)/2 - (p-5)/4 = (p-1)/4$, so again apply Lemma 40. If subcase 2.2 holds, then by Lemma 43, $\{1, 3\} \subset B$; hence, B is (c_0, c_1)-special by Lemma 39. If subcase 2.3 holds, then by Lemma 43, $\{(p-7)/2, (p-1)/2\} \subset B$. Let $\{\alpha_1, \beta_1\}$ be the subset of the block of $\mathcal{F}$ containing (joined) mixed difference 1. If $\{\alpha_1, \beta_1\} \subset [1, (p-1)/4]$, then apply Lemma 39; otherwise, $\{\alpha_1, \beta_1\} \subset [(p-1)/4, (p-3)/2]$, so apply Lemma 40.

Suppose that the third case holds. Then by Lemma 42, there are two subcases to treat:

3.1. Mixed differences 1 and 3 occur in some $B \in \mathcal{F}$, or

3.2. Mixed differences 2 and 3 occur in some $B \in \mathcal{F}$.

If subcase 3.1 holds, then by Lemma 43, $\{1, 2\} \subset B$; hence B is (c_0, c_1)-special by Lemma 39. If subcase 3.2 holds, then by Lemma 43, $\{(p-5)/2, (p-1)/2\} \subset B$. Let $\{\alpha_1, \beta_1\}$ be the subset of the block of $\mathcal{F}$ containing (joined) mixed difference 1. If $\{\alpha_1, \beta_1\} \subset [1, (p-1)/4]$, then apply Lemma 39; otherwise, $\{\alpha_1, \beta_1\} \subset [(p-1)/4, (p-$

3)/2], so apply Lemma 40. Treat the fourth case in the same way that the third case was just treated.

Suppose that the fifth case holds. Then by Lemma 42 and 43, mixed differences 1 and 2 occur in some $B \in \mathcal{F}$ such that $\{(p-3)/2, (p-1)/2\} \subset B$. Let $\{\alpha_3, \beta_3\}$ and $\{\alpha_4, \beta_4\}$ be the subsets of the blocks of $\mathcal{F}$ containing (joined) mixed differences 3 and 4, respectively, contained in $[1, (p-1)/2]$. If for $i \in \{3, 4\}$, $\{\alpha_i, \beta_i\} \subset [1, (p-1)/4]$, then apply Lemma 39; if $\{\alpha_i, \beta_i\} \subset [(p-1)/4, (p-1)/2]$, then apply Lemma 40. Otherwise, we have without loss of generality that $\alpha_i < (p-1)/4$ and $\beta_i > (p-1)/4$; in this case, setting $S = \{\alpha_3, \beta_3, \alpha_4, \beta_4\}$, then $\max\{S\} - \min\{S\} \leq 5$ (hence our requirement that $p \geq 29$), so apply Lemma 40.

Suppose that the sixth case holds. Then by Lemmas 42 and 43 there exist two blocks $B, B' \in \mathcal{F}$ such that $\{(p-3)/2, (p-1)/2\} \subset B$ and $\{(p-7)/2, (p-1)/2\} \subset B'$. Hence, $B = B'$, so that $\{(p-7)/2, (p-3)/2, (p-1)/2\} \subset B$, but this is impossible, since every block of $\mathcal{F}$ has precisely two of its points contained in $[1, (p-1)/2]$.

Suppose that the seventh or eighth case holds. Then by Lemma 42, the mixed differences 1, 2, and 3 occur in the same block of $\mathcal{F}$, which is impossible by Lemma 41, since p is sufficiently large.

□

Let $\mathbb{F}_q = p^n$ be a finite field, with p prime. A fundamental result [40] in finite field theory is that if x is a primitive element of $\mathbb{F}_q$, then

$$\mathbb{F}_q = \bigcup_{\{a_0,\ldots,a_{n-1}\} \in \binom{\mathbb{F}_p}{n}} \left\{ \sum_{i=0}^{n-1} a_i x^i \right\},$$

with arithmetic performed over $\mathbb{F}_q$. A *polynomial-based indexing in* x of $\mathbb{F}_q = \{\sigma_0 = 0, \ldots, \sigma_{q-1}\}$ is an indexing of the elements of $\mathbb{F}_q$ such that for each $i \in [0, p^{n-1} - 1]$ and any $f, g \in \{\sigma_{ip}, \ldots, \sigma_{ip+p-1}\}$, there exists a set $\{a_{i,1}, a_{i,2}, \ldots, a_{i,n-1}\} \subseteq \mathbb{F}_p$ such that

$$f = \alpha + \sum_{j=1}^{n-1} a_{i,j} x^i, \text{ and}$$

$$g = \beta + \sum_{j=1}^{n-1} a_{i,j} x^i,$$

with $\alpha, \beta \in \mathbb{F}_p$. In words, a polynomial-based indexing in x of $\mathbb{F}_q$ partitions the elements of $\mathbb{F}_q$ into p-sets, each consisting of those polynomials (treating x as an indeterminate) that have identical coefficients for each corresponding term of degree greater than zero. Now suppose in particular that $q = 4t + 1$, with t odd, and let $\mathbb{F}_q = \{\sigma_0 = 0, \ldots, \sigma_{q-1}\}$ be a polynomial-based indexing in x of $\mathbb{F}_q$. For $i \in [0, p^{n-1} - 1]$, the *corresponding sub-Moore isomorphism of index i for MD$(3q + 1)$* is the map

$$\varphi_i : \{\sigma_{ip}, \ldots, \sigma_{ip+p-1}\} \times \mathbb{Z}_3 \cup \{\infty\} \to \mathbb{F}_p \times \mathbb{Z}_3 \cup \{\infty\}$$

such that $\varphi_i(\infty) = \infty$ and $\varphi_i(f, c) = (\alpha, c)$ given $f = \alpha + \sum_{j=1}^{n-1} a_{i,j} x^i \in \mathbb{F}_q$. That is, φ_i "deletes" from f all terms of degree greater than zero.

Theorem 34 below allows us to get DiffSum 3 labellings of Moore designs having nontrivial prime power order.

Theorem 34. *Suppose that $q = p^n = 4t + 1$ with t odd and p prime, x a primitive element of $\mathbb{F}_q$, and let MD$(3q + 1) = (V = \mathbb{F}_q \times \mathbb{Z}_3, \mathcal{B})$ with ordered classical resolution $\mathcal{R} = \{\mathcal{P}_0, \ldots, \mathcal{P}_{q-1}\}$. If $\mathbb{F}_q = \{\sigma_0 = 0, \ldots, \sigma_{q-1}\}$ is a polynomial-based indexing in x of $\mathbb{F}_q$, then $\mathcal{B}$ contains p^{n-1} disjoint isomorphic copies of MD$(3p + 1)$, determined by the corresponding sub-Moore isomorphisms φ_i, $i \in [0, p^{n-1} - 1]$, for MD$(3q + 1)$, .*

Proof. Since $q = 4t + 1$ with t odd, $q \equiv 5 \pmod 8$. Thus, $p \equiv 5 \pmod 8$, say $p = 4s + 1$ with s odd, since $1, 3, 7 \in (\mathbb{Z}/8\mathbb{Z})^\times$ have orders 1, 2, and 2, respectively. Thus, if y is a primitive element of $\mathbb{F}_p$, then $y^s \in \mathbb{F}_p$ is a primitive fourth root of unity over $\mathbb{F}_q$, so that the group of fourth roots of unity over $\mathbb{F}_q$ is a subgroup of $\mathbb{F}_p^\times$.

Now for any integer α,

$$\begin{aligned} &\alpha \equiv 1 \pmod{\alpha - 1} \\ \iff &\alpha^n - 1 \equiv 1^n - 1 \pmod{\alpha - 1} \\ \iff &\alpha^n - 1 \equiv 0 \pmod{\alpha - 1}. \end{aligned}$$

Thus $p - 1 \mid p^n - 1$ and hence $s \mid t$. Now $z = x^{t/s}$ is a primitive element of $\mathbb{F}_p$, for suppose to the contrary that there exists some $i \in [1, 4s - 1]$ such that $z^i = 1$. Then $x^{it/s} = 1$ and $1 \leq it/s < 4t$, contradicting that x is a primitive element of $\mathbb{F}_q$. Hence, z has order $4s$ in $\mathbb{F}_q^\times$, implying that $\langle z \rangle = \mathbb{F}_p^\times$.

That

$$\bigcup_{i \in [0,t-1]} \{x^i, -x^i, x^{i+t}, -x^{i+t}\} = \mathbb{F}_q^\times,$$

and the fact that x^t, a fourth root of unity over $\mathbb{F}_q$, must belong to $\mathbb{F}_p$, imply

$$\bigcup_{i \in [0,s-1]} \{x^{it/s}, -x^{it/s}, x^{it/s+t}, -x^{it/s+t}\} = \mathbb{F}_p^\times.$$

Hence, setting

$$\mathcal{P}'_0 = \bigcup_{i \in [0,s-1], c \in \mathbb{Z}_3} \{\{(z^i, c), (-z^i, c), (z^{i+t}, c+1), (-z^{i+t}, c+1)\}\},$$

then $\mathcal{P}'_0 \subset \mathcal{P}_0$.

For each $i \in [0, p^{n-1} - 1]$, the set

$$\mathcal{B}'_i = \bigcup_{j \in [0,p-1]} (\mathcal{P}'_0 \oplus \sigma_{ip+j} \cup \{\infty, (\sigma_{ip+j}, 0), (\sigma_{ip+j}, 1), (\sigma_{ip+j}, 2)\}) \subset \mathcal{B}$$

is isomorphic to the blockset of MD$(3p + 1)$, the isomorphism being the sub-Moore isomorphism

$$\varphi_i : \{\sigma_{ip}, \ldots, \sigma_{ip+p-1}\} \times \mathbb{Z}_3 \cup \{\infty\} \to \mathbb{F}_p \times \mathbb{Z}_3 \cup \{\infty\}$$

of index i for MD$(3q + 1)$. $\square$

We now have the tools to construct our $\mathsf{DiffSum}$ 3 labellings.

Lemma 45. *Suppose that $q = p^n = 4t + 1$ with t odd, p prime, and $n > 0$. If $MD(3p+1)$ has a (c_0, c_1)-special base block, $MD(3q+1) = (V = \mathbb{F}_q \times \mathbb{Z}_3 \cup \{\infty\}, \mathcal{B})$ admits a block labelling rk with $\mathsf{DiffSum}$ at most 3.*

Proof. Let x be a primitive element of $\mathbb{F}_q$, with $\mathbb{F}_q = \{\sigma_0 = 0, \ldots, \sigma_{q-1}\}$ a polynomial-based indexing in x of $\mathbb{F}_q$ such that φ_i is the corresponding sub-Moore isomorphism of index i, $i \in [0, p^{n-1} - 1]$, for MD$(3q + 1)$, and S a putative (c_0, c_1)-special base block of MD$(3p + 1)$. We refine our indexing of $\mathbb{F}_q$ by further requiring that:

1. For all $i \in \{0, 2, 4, \ldots, p^{n-1} - 1\}$ and $j \in [0, p - 1]$, $\varphi_i(\sigma_{ip+j}, \cdot) = (j, \cdot)$, and
2. for all $i \in \{1, 3, 5, \ldots, p^{n-1} - 2\}$ and $j \in [0, p - 1]$, $\varphi_i(\sigma_{ip+j}, \cdot) = (p - 1 - j, \cdot)$.

Finally, let $\mathcal{R} = \{\mathcal{P}_0, \ldots, \mathcal{P}_{3q}\}$ be the classical resolution of MD$(3q + 1)$ such that $\mathcal{P}_i = \mathcal{P}_0 \oplus \sigma_i$ for all $i \in [0, q - 1]$.

Now suppose rk satisfies the ten conditions:

C1. $\mathcal{R}$-intervaled: For all $i \in [0, q - 1]$, $\mathsf{rk}^{-1}([i(3t + 1), 3t + i(3t + 1)]) = \mathcal{P}_i$.

C2. For all $i \in [0, (3t - 3)/2] \cup [(3t + 3)/2, 3t]$ and $j \in [0, q - 1]$,

$$\mathsf{rk}^{-1}(i + j(3t + 1)) = \mathsf{rk}^{-1}(i) \oplus \sigma_j.$$

C3. $\mathsf{rk}^{-1}(0)$ is a type 0 secant, $\mathsf{rk}^{-1}(1)$ is a type 2 secant, and $\mathsf{rk}^{-1}(2)$ is a type 1 secant.

C4. $\mathsf{rk}^{-1}(3t - 2)$ is a type 2 secant, $\mathsf{rk}^{-1}(3t - 1)$ is a type 1 secant, and $\mathsf{rk}^{-1}(3t)$ is a type 0 secant.

C5. For $j \in [1, (t - 3)/2]$ and $k \in \{0, 1, 2\}$, both $\mathsf{rk}^{-1}(3j + k)$ and $\mathsf{rk}^{-1}(3t - 3j - k)$ are type k secants.

C6. If $c_0 = 0$ and $c_1 = 1$, then $\mathsf{rk}^{-1}((3t-3)/2)$ is a type 1 secant and $\mathsf{rk}^{-1}((3t+3)/2)$ is a type 2 secant. Conversely, if $c_0 = 1$ and $c_1 = 0$, then $\mathsf{rk}^{-1}((3t-3)/2)$ is a type 2 secant and $\mathsf{rk}^{-1}((3t+3)/2)$ is a type 1 secant.

C7. For all $i \in \{0, 2, 4, \ldots, p^{n-1} - 1\}$ and $j \in [0, (p-1)/2]$,

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t-1)/2)$$

is the ∞-block of $\mathcal{P}_{ip+j}$ and

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t+1)/2) = \varphi_i^{-1}(S) \oplus \sigma_{ip+j}.$$

C8. For all $i \in \{0, 2, 4, \ldots, p^{n-1} - 1\}$ and $j \in [(p+1)/2, p-1]$,

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t+1)/2)$$

is the ∞-block of $\mathcal{P}_{ip+j}$ and

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t-1)/2) = \varphi_i^{-1}(S) \oplus \sigma_{ip+j}.$$

C9. For all $i \in \{1, 3, 5, \ldots, p^{n-1} - 2\}$ and $j \in [0, (p-1)/2]$,

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t+1)/2)$$

is the ∞-block of $\mathcal{P}_{ip+j}$ and

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t-1)/2) = \varphi_i^{-1}(S) \oplus \sigma_{ip+j}.$$

C10. For all $i \in \{1, 3, 5, \ldots, p^{n-1} - 2\}$ and $j \in [(p+1)/2, p-1]$,

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t-1)/2)$$

is the ∞-block of $\mathcal{P}_{ip+j}$ and

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t+1)/2) = \varphi_i^{-1}(S) \oplus \sigma_{ip+j}.$$

Let $\rho \in V$. As $\mathcal{P}_i$ is a parallel class for each $i \in [0, q-1]$, there is a unique value $\ell_i \in [0, 3t]$ such that $\rho \in \mathsf{rk}^{-1}(i(3t+1)+\ell_i)$. The point sum of ρ with respect to rk may thus be written

$$\sum_{i=0}^{q-1}(i(3t+1)+\ell_i) = (3t+1)(4t+1)(2t) + \sum_{i=0}^{q-1}\ell_i,$$

so that the second summation is the resolution-relative point sum of ρ. Now consider any $(y, c) \in V - \{\infty\}$. By C5, the multiset of summands of the resolution-relative point sum of (y, c) $L = \{\ell_i : i \in [0, q-1]\}$ for (y, c) contains the multiset $M = \{3i+c, 3i+c, 3(t-i)-c, 3(t-i)-c, 3i+((c+2) \bmod 3), 3i+((c+2) \bmod 3), 3(t-i)-((c+2) \bmod 3), 3(t-i)-((c+2) \bmod 3) : i \in [1, (t-3)/2]\}$. We compute $L - M$ (multiset difference) on a case-by-case basis, depending on the value of c, as follows. For all cases, we suppose without loss of generality that $c_0 = 0$ and $c_1 = 1$.

Suppose that $c = 0$. Then L is given by the (multiset) union of M together with $M_{0,0}, M_{0,1}$, and $M_{0,2}$ defined thus:

1. $M_{0,0} = \{0, 0, 1, 1, 3t-2, 3t-2, 3t, 3t\}$ (C3 and C4)
2. $M_{0,1} = \{(3t+3)/2, (3t+3)/2\}$ (by C6, $\mathsf{rk}^{-1}((3t+3)/2)$ is a type 2 secant.)
3. $M_{0,2} = \{(3t-1)/2, (3t-1)/2, (3t-1)/2\}$ or $M_{0,2} = \{(3t-1)/2, (3t-1)/2, (3t+1)/2\}$ or $M_{0,2} = \{(3t-1)/2, (3t+1)/2, (3t+1)/2\}$.

Accounting for the variants of $M_{0,2}$ requires an explanation. Put

$$U = \bigcup_{i \in [0, p^{n-1}-1], j \in [0, p-1]} \left(\varphi_i^{-1}(S) \oplus \sigma_{ip+j}\right). \tag{6.2}$$

Then any point $(z, c') \in \mathbb{F}_q \times \{0, 2\}$ occurs in exactly two distinct blocks of U; say that $(y, 0)$ in particular occurs in blocks B_1 and B_2 of U. In fact, there exists some unique $i \in [0, p^{n-1}-1]$ such that $B_1, B_2 \in \bigcup_{j=0}^{p-1} \mathcal{P}_{ip+j}$. Moreover, the unique ∞-block, say B_∞, that contains $(y, 0)$ occurs in $\mathcal{P}_{ip+k}$ for some unique $k \in [0, p-1]$ satisfying

$\varphi_i(y,0) = (k,0)$. By C7 up to C10, together with the fact that S is a (c_0, c_1)-special base block of MD$(3p+1)$, there are exactly four ways that rk could assign labels to B_1, B_2, and B_∞, where $k_1, k_2, k_3 \in [ip, ip+p-1]$:

1. $\mathsf{rk}(B_1) = k_1(3t+1) + (3t+1)/2$, $\mathsf{rk}(B_2) = k_2(3t+1) + (3t+1)/2$, and $\mathsf{rk}(B_\infty) = k_3(3t+1) + (3t-1)/2$;
2. $\mathsf{rk}(B_1) = k_1(3t+1) + (3t-1)/2$, $\mathsf{rk}(B_2) = k_2(3t+1) + (3t+1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t+1) + (3t+1)/2, k_3'(3t+1) + (3t-1)/2\}$;
3. $\mathsf{rk}(B_1) = k_1(3t+1) + (3t+1)/2$, $\mathsf{rk}(B_2) = k_2(3t+1) + (3t-1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t+1) + (3t+1)/2, k_3'(3t+1) + (3t-1)/2\}$; or
4. $\mathsf{rk}(B_1) = k_1(3t+1) + (3t-1)/2$ and $\mathsf{rk}(B_2) = k_2(3t+1) + (3t-1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t+1) + (3t+1)/2, k_3'(3t+1) + (3t-1)/2\}$;

hence the three variations of $M_{0,2}$.

Suppose that $c = 1$. Then L is given by the (multiset) union of M together with $M_{1,0}, M_{1,1}$, and $M_{1,2}$, defined thus:

1. $M_{1,0} = \{0, 0, 2, 2, 3t-1, 3t-1, 3t, 3t\}$ (C3 and C4).
2. $M_{1,1} = \{(3t-3)/2, (3t-3)/2\}$ (by C6, $\mathsf{rk}^{-1}((3t-3)/2)$ is a type 1 secant).
3. $M_{1,2} = \{(3t-1)/2, (3t-1)/2, (3t+1)/2\}$ or $M_{1,2} = \{(3t-1)/2, (3t+1)/2, (3t+1)/2\}$, or $M_{1,2} = \{(3t+1)/2, (3t+1)/2, (3t+1)/2\}$.

Similar to $M_{0,2}$, $M_{1,2}$ is formed as follows. We know that that $(y,1)$ occurs in two distinct blocks, say, B_1 and B_2 of U (see (6.2)). Indeed, there exists a unique $i \in [0, p^{n-1}-1]$ for which $B_1, B_2 \in \bigcup_{j=0}^{p-1} \mathcal{P}_{ip+j}$. Moreover, the unique ∞-block, say B_∞, that contains $(y,1)$ occurs in $\mathcal{P}_{ip+k}$ for some unique $k \in [0, p-1]$ satisfying $\varphi_i(y,1) = (k,1)$. By C7 up to C10, together with the fact that S is a (c_0, c_1)-special base block of MD$(3p+1)$, there are exactly four ways that rk could assign labels to B_1, B_2, and B_∞, where $k_1, k_2, k_3 \in [ip, ip+p-1]$:

1. $\mathsf{rk}(B_1) = k_1(3t+1)+(3t-1)/2$, $\mathsf{rk}(B_2) = k_2(3t+1)+(3t-1)/2$, and $\mathsf{rk}(B_\infty) = (3t+1)/2$;
2. $\mathsf{rk}(B_1) = k_1(3t+1)+(3t-1)/2$, $\mathsf{rk}(B_2) = k_2(3t+1)+(3t+1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t+1)+(3t+1)/2, k_3'(3t+1)+(3t-1)/2\}$;
3. $\mathsf{rk}(B_1) = k_1(3t+1)+(3t+1)/2$, $\mathsf{rk}(B_2) = k_2(3t+1)+(3t-1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t+1)+(3t+1)/2, k_3'(3t+1)+(3t-1)/2\}$; or
4. $\mathsf{rk}(B_1) = k_1(3t+1)+(3t+1)/2$, $\mathsf{rk}(B_2) = k_2(3t+1)+(3t+1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t+1)+(3t+1)/2, k_3'(3t+1)+(3t-1)/2\}$;

hence the three variations of $M_{1,2}$.

Finally, suppose that $c=2$. Then L is given by the (multiset) union of M together with $M_{2,0}, M_{2,1}$, $M_{2,2}$, and $M_{2,3}$, defined thus:

1. $M_{2,0} = \{1,1,2,2,3t-2,3t-2,3t-1,3t-1\}$ (C3 and C4).
2. $M_{2,1} = \{(3t-3)/2, (3t-3)/2\}$ (by C6, $\mathsf{rk}^{-1}((3t-3)/2)$ is a type 1 secant).
3. $M_{2,2} = \{(3t+3)/2, (3t+3)/2\}$ (by C6, $\mathsf{rk}^{-1}((3t+3)/2)$ is a type 2 secant).
4. $M_{2,3} = \{(3t-1)/2\}$ or $M_{2,3} = \{(3t+1)/2\}$ (this accounts for the ∞-block that contains $(y,2)$ – see C7 up to C10).

We now compute the sum of the elements of each variant of L. If $c=0$, then the sum of the elements of the multiset union $M_{0,0} \cup M_{0,1} \cup M_{0,2}$ falls in the interval $[18t+(3t-1)/2, 18t+(3t-1)/2+2]$, and thus the sum of the elements of L for any $(y,0) \in V$ falls in the interval $[6t^2+(3t-1)/2, 6t^2+(3t-1)/2+2]$. If $c=1$, then the sum of the elements of $M_{1,0} \cup M_{1,1} \cup M_{1,2}$ falls in the interval $[18t+(3t-1)/2-1, 18t+(3t-1)/2+1]$, and thus the sum of the elements of L

for any $(y,1) \in V$ falls in the interval $[6t^2 + (3t-1)/2 - 1, 6t^2 + (3t-1)/2 + 1]$. If $c = 2$, then the sum of the elements of $M_{2,0} \cup M_{2,1} \cup M_{2,2} \cup M_{2,3}$ falls in the interval $[18t + (3t-1)/2, 18t + (3t-1)/2 + 1]$, and thus the sum of the elements of L for any $(y,2) \in V$ falls in the interval $[6t^2 + (3t-1)/2, 6t^2 + (3t-1)/2 + 1]$. At last, by C7 up to C10, the sum of the elements of L for $\infty \in V$ is

$$\begin{aligned}\frac{q-1}{2} \cdot \frac{3t+1}{2} + \frac{q+1}{2} \cdot \frac{3t-1}{2} &= \frac{3qt + q - 3t - 1 + 3qt - q + 3t - 1}{4} \\ &= \frac{3qt-1}{2} \\ &= \frac{12t^2 + 3t - 1}{2} \\ &= 6t^2 + \frac{3t-1}{2}.\end{aligned}$$

Hence rk has $\mathsf{DiffSum}$ at most 3. □

Theorem 35. *Suppose that $q = p^n = 4t + 1$ with t odd and $p \geq 13$ prime. Then MD$(3q+1)$ admits a labelling with $\mathsf{DiffSum}$ at most 3.*

Proof. Applying Lemmas 44 and 45, we obtain the desired labellings for each MD$(3q+1)$ with t odd and $p \geq 29$. Here are the three base blocks of the generating Moore difference family for MD(40), using 6 as the primitive element of $\mathbb{F}_{13}$:

$$\{(1,0),(12,0),(8,1),(5,1)\}, \{(6,0),(7,0),(9,1),(4,1)\}, \text{ and}$$
$$\{(10,0),(3,0),(2,1),(11,1)\}.$$

By Lemma 39, the third base block is (c_0, c_1)-special, and thus by Lemma 45, MD(40) admits the desired labelling. □

6.5 Concluding Remarks

The single base block of MD(16) is not (c_0, c_1)-special, and we have verified by computer that if $\mathcal{R}$ is the classical resolution of MD(16), then the least $\mathsf{DiffSum}$ of any $\mathcal{R}$-intervaled labelling of MD(16) is 6. In general, for $|\mathcal{F}|$ and $|N|$ odd, we do not believe that $k-1$ is the best possible $\mathsf{DiffSum}$. Indeed, we have devised $\mathsf{DiffSum}$ 1 labellings, which we do not present here, for an infinite class of $S(2,4,v)$s.

Chapter 7

CONCLUSION

7.1 Summary

We began the main body of this thesis by determining the maximum double independence number for all admissible orders of an STS, a natural outgrowth of the observation of Theorem 2 that for an STS to meet the theoretical optimum $\mathsf{DiffSum}$ bound of Theorem 1, it must have a sufficiently large pair of disjoint independent sets.

We then executed a three-pronged strategy to address the central aim of this thesis: labelling $S(2, k, v)$s with $k > 3$. First, we supplied what one might call *partially determined* point labellings arising from special classes of large independent sets; partially determined in the sense that only a proper subset of points need to be assigned a particular set of labels. To give the major examples from the thesis:

1. In Lemma 1 and its derivatives, two disjoint independent sets are assigned the least and greatest collection of labels, respectively, but it doesn't matter how the remaining points are labelled, and in fact it doesn't even matter exactly how the two independent sets are assigned the lowest and highest-valued labels.
2. The application of the $3v + 1$ construction of Lemma 36, wherein no regard is given for how exactly labels are assigned to the sub-$S(2, 4, v)$

Contrast this with what one might call the *completely determined* point labellings of Dau and Milenkovic (the Bose and Skolem labellings of [22]), in which every point is carefully assigned an exact label. We must admit that our labellings produced by the first prong are not as good as the state-of-the-art point labellings of Steiner triple systems, which come within a constant summand of the corresponding MinSum and DiffSum bounds of Theorem 1, and we suspect that if point labellings meeting the Theorem 1 bounds do exist for an infinite class of $S(2,4,v)$s, then they are completely determined.

Second, improving on the DiffSum bounds obtained from the first prong, we supplied *worst case* (and in a certain sense fictional) point labellings of those $S(2,4,v)$s that result from filling in the groups of the 4-GDDs produced by the $12u$ construction, obtaining an upper bound of $2v-8$ on the DiffSum, which is considerably far from the corresponding Theorem 1 DiffSum bound of $v-4$. This is to be expected, since our ignorance of the structure of GRL $S(2,4,v)$s forces us to assume the worst-possible state of affairs: the existence of a weighted block of the Stinson master GDD receiving the least-valued set of labels. We remind the reader that the first two prongs are the only work done in this difficult subject, so perfection was not expected.

Third, and most successfully from the standpoint of access balancing, we supplied completely determined block labellings of 1-rotational resolvable $S(2,k,v)$s that either attain the best-possible DiffSum of 0 or come within (a summand of) $k+1$ of it.

7.2 Open Problems and Future Work

The major loose end that has emerged over the course of this thesis that has not been tied up is our failure to find an $S(2,4,37)$ with a pair of disjoint maximum ovals. The main problem with this order is that it is too small to contain a non-trivial sub-$S(2,4,v)$: By the Rees-Stinson theorem of [59], an $S(2,4,w)$ contains a sub-$S(2,4,v)$ if and only if $w \geq 3v+1$. As we've seen, it is common to apply WFC with a sub-design, but this is a non-starter for order 37. Further, there is little hope of finding a desired $S(2,4,37)$ that has been enumerated; in [38] Krčadinac enumerated the largest-known collection of non-isomorphic $S(2,4,37)$s: 51402 in total, and in the same paper speculated that this is but a sliver of the total number. The design may thus need to be directly constructed.

Improvements can also be made in our work. For example, one could more intelligently apply the $3v+1$ construction to derive a better MinSum bound. Indeed, there is no pressing need, as in Lemma 36, for the sub-KTS$(2v+1)$ D to attain the optimal MinSum of $2v+1$; a better requirement is that the MinSum of each parallel class $\mathcal{P}$ of D be sufficiently high relative to the label of the point of the sub-$S(2,4,v)$ adjoined to the triples of $\mathcal{P}$ by the $3v+1$ construction. Under this requirement, it is fine for certain parallel classes to have relatively low MinSum. A cursory inspection of the Bose labelling suggests that the majority of the labelled blocks have block sum $2v+1$, so either a new labelling of the Bose-averaging triple system needs to be devised, or some other class of Kirkman triple systems needs to be used for this approach.

There's also plenty of unexplored research directions to pursue, both theoretical and practical. For one, our work in Chapter 4 has established that for one-third of the admissible KTS orders (namely, $v \equiv 9 \pmod{18}$), a *weakly 3-chromatic* KTS(v) exists, which is to say a KTS whose point set partitions into three independent sets. A problem of interest to (pure) design theorists is to determine the spectrum of weakly 3-chromatic Kirkman triple systems. Second, we have seen in Chapter 6 that 1-rotational resolvable Steiner 2-designs satisfying the labelling condition are perfectly suited to admit egalitarian block labellings. Does such a wide-ranging class of Steiner systems exist that are, as it were, "designed" to meet (or at least come within a constant summand of) the bounds of Theorem 1? While we know, per Theorem 2, that Steiner systems must satisfy necessary conditions on the sizes of their independent sets to be capable of meeting the MinSum and DiffSum bounds of Theorem 1, we still have no general sufficient condition. Instead, the approach has been to find (or even stumble into) the right (direct) construction for the job; e.g., the Bose and Skolem constructions for optimal MinSum and the Schreiber-Wilson construction for close to optimal DiffSum. This approach is fine for Steiner triple systems, for which direct constructions abound, but it seems especially limited for block size four, given that all direct constructions of $S(2,4,v)$s come from difference families, which appear ill-suited for point labelling. A more viable approach then, is to understand how to better label recursively constructed $S(2,4,v)$s.

The simplicity of the Dau and Milenkovic labelling model comes at a practical cost. It is common that for a given storage system, the rank of the popularity of a file is inversely related to the number of access requests for that file; this is a specific instance of an empirical law observed in many data sets of the physical and social sciences known as *Zipf's law* [9, 45, 48]. By contrast, the labelling model of Dau and Milenkovic assumes a linear relation between a file's popularity rank and the frequency with which it is accessed. For example, as far as their model is concerned, since the blocks $\{0,7,11\}$ and $\{5,6,7\}$ have identical block sum, the associated storage units have identical cumulative popularity. Yet, if the associated storage system fits the Zipf distribution, we should except the first storage unit to be accessed much more frequently than the second, since it contains the most popular file. A remedy to this shortcoming is to instead label files by absolute popularity.

REFERENCES

[1] Ahmed Assaf. “Modified group divisible designs”. *Ars Combin.* 29 (1990), pp. 13–20.

[2] William M. Brummond. “Kirkman systems that attain the upper bound on the minimum block sum, for access balancing in distributed storage”. *arXiv preprint arXiv:1906.02157* (2019).

[3] M. Buratti and N.J. Finizio. “Existence results for 1-rotational resolvable Steiner 2-designs with block size 6 or 8”. *Bull Inst. Combin. Appl* 50 (2007), pp. 29–44.

[4] Marco Buratti. “Some constructions for 1-rotational BIBD’s with block size 5”. *Australasian Journal of Combinatorics* 17 (1998), pp. 199–228.

[5] Marco Buratti, Jie Yan, and Chengmin Wang. “From a 1-rotational RBIBD to a partitioned difference family”. *The Electronic Journal of Combinatorics* (2010), R139–R139.

[6] Marco Buratti and Fulvio Zuanni. “G-invariantly resolvable Steiner 2-designs which are 1-rotational over G”. *Bulletin of the Belgian Mathematical Society-Simon Stevin* 5.2/3 (1998), pp. 221–235.

[7] Marco Buratti and Fulvio Zuanni. “Explicit constructions for 1-rotational Kirkman triple systems”. *Utilitas Mathematica* 59 (2001), pp. 27–30.

[8] Marco Buratti and Fulvio Zuanni. “The 1-rotational Kirkman triple systems of order 33”. *Journal of Statistical Planning and Inference* 86.2 (2000), pp. 369–377.

[9] Niklas Carlsson, György Dán, Anirban Mahanti, and Martin Arlitt. “A longitudinal characterization of local and global bittorrent workload dynamics”. *International Conference on Passive and Active Network Measurement*. Springer. 2012, pp. 252–262.

[10] Yeow Meng Chee, Charles J. Colbourn, Hoang Dau, Ryan Gabrys, Alan C.H. Ling, Dylan Lusi, and Olgica Milenkovic. “Access balancing in storage systems by labeling partial Steiner systems”. *Designs, Codes and Cryptography* 88.11 (2020), pp. 2361–2376.

[11] K.J. Chen and L. Zhu. “On the existence of skew Room frames of type t^u”. *Ars Combin.* 43 (1996), pp. 65–79.

[12] Peter M. Chen, Edward K. Lee, Garth A. Gibson, Randy H. Katz, and David A. Patterson. "RAID: High-performance, reliable secondary storage". *ACM Computing Surveys (CSUR)* 26.2 (1994), pp. 145–185.

[13] Ludmila Cherkasova and Minaxi Gupta. "Analysis of enterprise media server workloads: access patterns, locality, content evolution, and rates of change". *IEEE/ACM Transactions on Networking* 12.5 (2004), pp. 781–794.

[14] Asaf Cidon, Stephen Rumble, Ryan Stutsman, Sachin Katti, John Ousterhout, and Mendel Rosenblum. "Copysets: Reducing the frequency of data loss in cloud storage". *Proceedings of 2013 USENIX Annual Technical Conference (ATC 2013)*. 2013, pp. 37–48.

[15] Charles J. Colbourn. "Egalitarian Steiner triple systems for data popularity". *Designs, Codes and Cryptography* (2021), pp. 1–23.

[16] Charles J. Colbourn and Jeffrey H. Dinitz. *Handbook of combinatorial designs*. CRC press, 2006.

[17] Charles J. Colbourn, Dean G. Hoffman, and Rolf Rees. "A new class of group divisible designs with block size three". *Journal of Combinatorial Theory, Series A* 59.1 (1992), pp. 73–89.

[18] Charles J. Colbourn, Daniel Horsley, and Chengmin Wang. "Trails of triples in partial triple systems". *Designs, Codes and Cryptography* 65.3 (2012), pp. 199–212.

[19] Charles J. Colbourn and Alexander Rosa. *Triple systems*. Oxford University Press, 1999.

[20] Simone Costa, Tao Feng, and Xiaomiao Wang. "Frame difference families and resolvable balanced incomplete block designs". *Designs, Codes and Cryptography* 86.12 (2018), pp. 2725–2745.

[21] Pramod K Das and Alexander Rosa. "Halving Steiner triple systems". *Discrete mathematics* 109.1-3 (1992), pp. 59–67.

[22] Hoang Dau and Olgica Milenkovic. "MaxMinSum Steiner systems for access balancing in distributed storage". *SIAM Journal on Discrete Mathematics* 32.3 (2018), pp. 1644–1671.

[23] Megan Dewar and Brett Stevens. *Ordering block designs: Gray codes, universal cycles and configuration orderings*. Springer Science & Business Media, 2012.

[24] Jean Doyen and Richard M Wilson. "Embeddings of Steiner triple systems". *Discrete Mathematics* 5.3 (1973), pp. 229–239.

[25] Salim El Rouayheb and Kannan Ramchandran. "Fractional repetition codes for repair in distributed storage systems". *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE. 2010, pp. 1510–1517.

[26] Arman Fazeli, Alexander Vardy, and Eitan Yaakobi. "Codes for distributed PIR with low storage overhead". *2015 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2015, pp. 2852–2856.

[27] A. D. Forbes, M. J. Grannell, and T. S. Griggs. "On colourings of Steiner triple systems". *Discrete Math.* 261.1-3 (2003), pp. 255–276.

[28] Steven Furino, Ying Miao, and Jianxing Yin. *Frames and resolvable designs: Uses, constructions and existence*. Vol. 3. CRC Press, 1996.

[29] Malcolm Greig and Alexander Rosa. "Maximal arcs in Steiner systems $S(2, 4, v)$". *Discrete mathematics* 267.1-3 (2003), pp. 143–151.

[30] Lucien Haddad and Vojtech Rödl. "Unbalanced Steiner triple systems". *Journal of Combinatorial Theory, Series A* 66.1 (1994), pp. 1–16.

[31] Philip Hall. "On representatives of subsets". *J. London Math. Soc* 10.1 (1935), pp. 26–30.

[32] Haim Hanani. "The existence and construction of balanced incomplete block designs". *The Annals of Mathematical Statistics* 32.2 (1961), pp. 361–386.

[33] Dean G. Hoffman, Charles C. Lindner, and Kevin T. Phelps. "Blocking sets in designs with block size 4". *European Journal of Combinatorics* 11.5 (1990), pp. 451–457.

[34] Mark Holland and Garth A. Gibson. "Parity declustering for continuous operation in redundant disk arrays". *ACM SIGPLAN Notices* 27.9 (1992), pp. 23–35.

[35] Masakazu Jimbo and Scott A. Vanstone. "Recursive constructions for resolvable and doubly resolvable 1-rotational Steiner 2-designs". *Utilitas Mathematica* 26 (1984), pp. 45–61.

[36] T.P. Kirkman. "Query VI". *Lady's and Gentleman's Diary* (1850).

[37] Thomas P. Kirkman. "On a problem in combinations". *Cambridge and Dublin Mathematical Journal* 2 (1847), pp. 191–204.

[38] Vedran Krčadinac. “Some new Steiner 2-designs $S(2, 4, 37)$”. *Ars Combin.* 78 (2006), pp. 127–135.

[39] Philip A. Leonard. “Realizations for direct constructions of resolvable Steiner 2-designs with block size 5”. *Journal of Combinatorial Designs* 8.3 (2000), pp. 207–217.

[40] Rudolf Lidl and Harald Niederreiter. *Finite fields*. 20. Cambridge university press, 1997.

[41] Alan CH Ling. “Hyperovals in Steiner systems”. *Journal of Geometry* 77.1-2 (2003), pp. 129–135.

[42] Jiaxi Lu. *Collected works of Lu Jiaxi on combinatorial designs*. Inner Mongolia People’s Press, 1990.

[43] Eliakim Hastings Moore. “Tactical memoranda I-III”. *American Journal of Mathematics* 18.3 (1896), pp. 264–290.

[44] Kevin T. Phelps and Vojtech Rödl. “Steiner triple systems with minimum independence number”. *Ars Combin.* 21 (1986), pp. 167–172.

[45] Tongqing Qiu, Zihui Ge, Seungjoon Lee, Jia Wang, Qi Zhao, and Jun Xu. “Modeling channel popularity dynamics in a large IPTV system”. *Proceedings of the eleventh international joint conference on Measurement and modeling of computer systems*. 2009, pp. 275–286.

[46] Dwijendra K. Ray-Chaudhuri and Richard M. Wilson. “Solution of Kirkman’s schoolgirl problem”. *Proc. symp. pure Math.* Vol. 19. 1971, pp. 187–203.

[47] Colin Reid and Alex Rosa. “Steiner systems $S(2, 4, v)$-a survey”. *The Electronic Journal of Combinatorics* (2012), DS18–Feb.

[48] Chris Roadknight, Ian Marshall, and Debbie Vearer. “File popularity characterisation”. *ACM Sigmetrics Performance Evaluation Review* 27.4 (2000), pp. 45–50.

[49] C.A. Rodger. “Linear spaces with many small lines”. *Discrete Mathematics* 129.1-3 (1994), pp. 167–180.

[50] C.A. Rodger, E.B. Wantland, K. Chen, and L. Zhu. “Existence of certain skew Room frames with application to weakly 3-chromatic linear spaces”. *Journal of Combinatorial Designs* 2.5 (1994), pp. 311–324.

[51] Vojtěch Rödl and Edita Šinajová. "Note on independent sets in Steiner systems". *Random Structures & Algorithms* 5.1 (1994), pp. 183–190.

[52] Alexander Rosa. "On certain valuations of the vertices of a graph". *Theory of graphs (Internat. symposium, Rome*. 1966, pp. 349–355.

[53] N Sauer and J Schönheim. "Maximal subsets of a given set having no triple in common with a Steiner triple system on the set". *Canadian Mathematical Bulletin* 12.6 (1969), pp. 777–778.

[54] Shmuel Schreiber. "Covering all triples on n marks by disjoint Steiner systems". *Journal of Combinatorial Theory, Series A* 15.3 (1973), pp. 347–350.

[55] J Sedláček. "Problem 27. Theory of graphs and its applications". *Proc. Symp. Smolenice. Praha*. 1963, pp. 163–164.

[56] Natalia Silberstein and Tuvi Etzion. "Optimal fractional repetition codes based on graphs and designs". *IEEE Transactions on Information Theory* 61.8 (2015), pp. 4164–4180.

[57] Natalia Silberstein and Anna Gál. "Optimal combinatorial batch codes based on block designs". *Designs, Codes and Cryptography* 78.2 (2016), pp. 409–424.

[58] Thoralf Skolem. "Some remarks on the triple systems of Steiner". *Mathematica Scandinavica* (1958), pp. 273–280.

[59] D.R. Stinson and R. Rees. "On the existence of incomplete designs of block size four having one hole". *Util. Math* 35 (1981), pp. 223–330.

[60] Douglas R. Stinson. *Combinatorial designs: constructions and analysis*. Springer Science & Business Media, 2007.

[61] Douglas R. Stinson. "The spectrum of nested Steiner triple systems". *Graphs and Combinatorics* 1.1 (1985), pp. 189–191.

[62] Richard M. Wilson. "An existence theory for pairwise balanced designs I. Composition theorems and morphisms". *Journal of Combinatorial Theory, Series A* 13.2 (1972), pp. 220–245.

[63] Richard M. Wilson. "Some partitions of all triples into Steiner triple systems". *Hypergraph seminar*. Springer. 1974, pp. 267–277.

[64] Wenjun Yu, Xiande Zhang, and Gennian Ge. “Optimal fraction repetition codes for access-balancing in distributed storage”. *IEEE Transactions on Information Theory* 67.3 (2020), pp. 1630–1640.

[65] Xiande Zhang and Gennian Ge. “On the existence of partitionable skew Room frames”. *Discrete mathematics* 307.22 (2007), pp. 2786–2807.

[66] Lie Zhu. “Some recent developments on BIBDs and related designs”. *Discrete Mathematics* 123.1-3 (1993), pp. 189–214.