Large sets of t-designs

Thesis by

Shahin Ajoodani-Namini

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1998

(Submitted July 14, 1997)

Acknowledgements

I sincerely thank my advisor Richard M. Wilson for his guidence and encouragement, without which this research would not have been completed.

It is a great pleasure to thank my advisor at University of Tehran G.B. Khosrovshahi, who introduced me to combinatorics, and taught me many things; and E. Lamken who helped me out in many occasions.

I am indebt to the California Institute of Technology and everyone in Mathematics Department, especially M. D'Elia, for the wonderful time spent here.

Abstract

We investigate the existence of large sets of t-designs. We introduce t-wise equivalence and (n, t)-partitionable sets. We propose a general approach to construct large sets of t-designs. Then, we consider large sets of a prescribed size n. We partition the set of all k-subsets of a v-set into several parts, each can be written as product of two trivial designs. Utilizing these partitions we develop some recursive methods to construct large sets of t-designs. Then, we direct our attention to the large sets of prime size. We prove two extension theorems for these large sets. These theorems are the only known recursive constructions for large sets which do not put any additional restriction on the parameters, and work for all t and k. One of them, has even a further advantage; it increase the strength of the large set by one, and it can be used recursively which makes it one of a kind. Then applying this theorem recursively, we construct large sets of t-designs for all t and some blocksizes k.

Hartman conjectured that the necessary conditions for the existence of a large set of size two are also sufficient. We suggest a recursive approach to the Hartman conjecture, which reduces this conjecture to the case that the blocksize is a power of two, and the order is very small. Utilizing this approach, we prove the Hartman conjecture for $t = 2$. For $t = 3$, we prove that this conjecture is true for infinitely many k, and for the rest of them there are at most $k/2$ exceptions.

In Chapter 4 we consider the case $k = t + 1$. We modify the recursive methods developed by Teirlinck, and then we construct some new infinite families of large sets of t-designs (for all t), some of them are the smallest known large sets. We also prove that if $k = t + 1$, then the Hartman conjecture is asymptotically correct.

Contents

Chapter 0 Introduction and Summary

In the first chapter, we define the main concepts like t-design, large set, etc. Then, we introduce some of our notations which are widely used throughout this thesis. The rest of definitions and notations will be introduced in subsequent chapters in the place they are actually needed. We introduce the t-set inclusion matrix and we explain how the existence problem in design theory can be reformulated as nonnegative integer solutions of a system of nonhomogeneous linear equations. Then we direct our attention to the null space of the t-set inclusion matrix. We give a short description of this null space in term of polynomials. We will show that the t-set inclusion matrix is of full rank, and we will find a triangular basis for its null space. Therefore, we obtain three equivalent ways to define t-designs, as collections of k-subsets, vectors with nonnegative integer entries, and regular polynomials. Throughout, this thesis we use the same notation for these three equivalent versions, and we switch from one notation to another whenever it makes it simpler to explain the ideas involved in the constructions. Finally, we give a short review of the known results on the existence of large sets.

In Chapter 2, we introduce the notion of t-wise equivalence which is basically a generalization of large sets, as large sets are partitions of $P_k(X)$ into t-wise equivalent subsets. We also define (n, t)-partitionable sets. We give a product construction for

(n,t)-partitionable sets which can increase the strength of these sets by one. We also explain a general approach to construct large sets of t-designs. To show the strength of this approach we give a short proof for a well known theorem on combining large sets only using two simple remarks we give right after the definition of t-wise equivalent sets. In the next section, we consider large sets of a prescribed size n. We obtain a partition of $v\Sigma k$ (the set of all k-subsets of a v-set) in which each part can be written as product of two trivial designs. These partitions will play a very important role in our discussion, and in particular they provide some interesting nontrivial identities involving binomial coefficients. Utilizing these partitions we prove the following theorem.

Theorem 1 *Let a, b, c, d, t, s, k, v_1 and v_2 be nonnegative integers such that $t \leq s < k \leq \min\{v_1, v_2\}$ and $s = k - 1 - a - b = t + c + d$. Suppose all of the following hold:*

(i) a $LS(1/n; t, i, v_1)$ exists for all $i \in \{k-a, \ldots, k\}$,

(ii) a $LS(1/n; t, i, v_2)$ exists for all $i \in \{k-b, \ldots, k\}$,

(iii) a $LS(1/n; t, k-a-l, v_1-l)$ exists for $1 \leq l \leq c$, and

(iv) a $LS(1/n; t, k-b-l, v_2-l)$ exists for $1 \leq l \leq d$,

Then a $LS(1/n; t, k, v_1+v_2-s)$ also exists.

If $b = c = d = 0$, then this theorem can be applied recursively to obtain an infinite family of large sets. In particular, if $k = t + 1$, then we will have the following theorem.

Theorem 2 *If a* $LS(\lambda; t, t+1, u+t)$ *exists, then a* $LS(m\lambda; t, t+1, mu+t)$ *also exists for all* $m \geq 1$.

In [17], Hartman conjectured that the necessary conditions for the existence of a $LS(1/2; t, k, v)$ are also sufficient. Theorem 2 together with $LS(4; 6, 7, 14)$ constructed in [28] will establish the Hartman conjecture for $k < 8$. Finally, to emphasize even more on the importance of t-wise equivalent sets, we direct our attention to the large sets of prime size. It must be noticed that this is not a restriction. As for a given large set of size n and a prime divisor p of n, one can obtain a large set of size p by simply grouping the designs in the given large set into p groups of size n/p. Once again, we find a partition of $v\Sigma k$ into several parts each can be written as a product of copies of trivial designs or some deformation of it. Then, utilizing the product construction for (n, t)-partitionable sets, we will prove the following theorems:

Theorem 3 *If a* $LS(1/p; t, n, u)$ *exists, then a* $LS(1/p; t, pn, pu)$ *also exists.*

Theorem 4 *If a* $LS(1/p; t, n, u-1)$ *exists and* $np < k < (n+1)p$, *then a* $LS(1/p; t-1, k, pu)$ *also exists.*

To the author's knowledge Theorems 2, 3 and 4, are the only known recursive constructions for large sets which do not put any additional restriction on the parameters. Theorems 2 and 3 are also have the advantage that they work for all t and k. The only other known construction of this type is due to Alltop [5], which

requires $v = 2k+1$ and t odd. Theorem 4 has even a further advantage; it increases t by one, and it can be used recursively which makes it one of a kind. Starting with nothing but a prime number, and applying this theorem recursively one can prove the following theorem.

Theorem 5 *Let p be any odd prime, and $l,\ t, m,\ a_0, \ldots, a_{t-1}$ be positive integers such that $t, l, m \geq 1$ and $1 \leq a_i < p$. Then a $LS(1/p; t, \sum_{i=0}^{t-1} a_i p^i + mp^t, (l-1)p^{t+1} + \sum_{i=1}^{t} p^i)$ exists.*

Theorem 5 is actually true even for $p = 2$. But in this case we probably prefer to start with a $LS(4; 6, 7, 14)$, so we can obtain designs of even smaller order, namely a $LS(1/2; t, 2^{t-3}-1, 2^{t-2}-2)$ for all $t \geq 6$. For $t \geq 9$, these designs are the smallest known t-designs. Prior to these result, the smallest known t-design (for $t > 8$) were of order $[(t+1)!]^{2t+1}$.

Moreover, if we also use Theorem 4, then we can prove even an stronger result. Let p be a prime number, and let k be a nonnegative integer such that at least $t+1$ of the coefficients in the p-adic expansion of k are nonzero. Then a $LS(1/p; t, k, v)$ exists in which $v < 2pk$. Therefore, for given t, for almost any blocksize k a large set of t-designs with block size k exists.

In Chapter 3, we restrict ourselves to the large sets of size two. First, we show that the necessary conditions can be written in the form $v > k + t$ and $v \equiv i \pmod{2^{f(k)}}$ for some $i \in A_{t,k}$ in which $2^{f(k)-1} \leq k < 2^{f(k)}$ and $A_{t,k}$ is defined

recursively by

$$\begin{cases} A(t, t+1) = \{t\}, \\ A(t,k) = \{t, \ldots, k-1\} \cup \{u | k+t < u < 2^n \ \& \ u \equiv i \text{ for some } i \in A(t, u-k)\}. \end{cases}$$

Then we apply the recursive constructions which were developed in Chapter 2 (mainly Theorem 2) to show that to prove the Hartman conjecture for given t and k, we only need to establish the existence of finitely many designs. More precisely, we prove the following theorem.

Theorem 6 *Let t, m, and l be three positive integers such that $m \leq l$ and $t < 2^m - 1$. If a $LS(1/2; t, i, 2^{f(i)} + t)$ exists for $t < i < 2^m$, and a $LS(1/2; t, 2^i + j, 2^{i+1} + t)$ exists for $m \leq i < l$ and $0 \leq j \leq \lfloor t/2 \rfloor$, then the necessary conditions for the existence of a $LS(1/2; t, k, v)$ are also sufficient.*

In particular, to prove this conjecture for $t = 2$, we only need to establish the existence of $LS(1/2; 2, k, 2k+2)$ for k a power of 2. We will give a direct construction for these designs. The idea is first to construct a $LS(1/2; 1, k, v)$ which is very close to be a large set of 2-designs. This can be established by applying methods similar to the ones which were used to construct large sets of prime size together with a few simple counting arguments. Then we apply a systematic trade-off on this large set of 1-designs to obtain a large set of 2-designs. Some of these ideas originally appeared in [16].

Next, we consider the case $t = 3$. Theorem 6 together with the table of well

known designs will establish the Hartman conjecture for $k < 16$. For $k \geq 16$, we are not aware of any construction which can establish the existence of the auxiliary designs in Theorem 6. Therefore, we choose a slightly different approach to prove that if $v \geq 2^{f(k)} + 3.2^{f(k)-4}$, then the necessary conditions are also sufficient. We prove this by induction on $f(k)$. Applying Theorem 1 with some suitable arguments reduce the problem to the existence of some designs of small order. The existence of most of theses designs follows by Theorems 3 and 4. A few of them have $v < 2k$, so the existence of their complement has already been established by induction hypothesis. To establish the existence of the rest of them, again we apply Theorem 1 together with the induction hypothesis and the fact that the Hartman conjecture is correct for $t = 2$. Now, it must be noticed that if $k \geq 2^{f(k)-1} + 3.2^{f(k)-4}$ and $2^{f(k)} + 3 \leq v < 2^{f(k)} + 3.2^{f(k)-4}$, then $v - k < 2^{f(k)-1}4$. Therefore, by induction hypothesis a $LS(1/2; 3, k, v)$ exists, and taking complements of these large sets we can settle all undecided cases for these values of k. The main result of this chapter is as follows:

Theorem 7 *The necessary conditions for the existence of a* $LS(1/2; t, k, v)$ *are also sufficient whenever one of the following holds (i)* $t = 2$, *(ii)* $t = 3$ *and* $k < 16$, *(iii)* $t = 3$ *and* $2^n + 3.2^{n-3} < k < 2^{n+1}$ *for some* $n \geq 4$, *(iv)* $t = 3$ *and* $v > 3k$.

Finally in Chapter 4 we direct our attention to the case $k = t + 1$. In [41], Teirlinck introduced r-trivial λ-factorizations and developed some recursive methods to construct r-trivial λ-factorizations. In particular, he proved that for given t there

exists $\lambda(t)$ such that the necessary conditions for the existence of a $LS(\lambda; t, t+1, v)$ are also sufficient whenever $\lambda(t)|\lambda$, and $\lambda(t)$ can be defined recursively by $\lambda(0) = 1$, and $\lambda(t+1) = \lambda(t)l(t+1)$ in which

$$l(t) = \text{l.c.m.}\{1, \ldots, t+1\} \cdot \text{l.c.m.}\{\binom{t}{i} | i = 1, \ldots, t\}. \quad (1)$$

We follow Teirlinck's approach to find some new large sets of t-designs (for all t), some of which have order smaller than those which were found in [41]. We first give a simple description of Teirlinck's construction which will enables us to put our main ideas in a much simpler way. As this discussion shows, the main reason that $\lambda(t)$ (in Teirlinck's construction) is so large is that he always start with a t-trivial λ-factorization which is only $(t-1)$-regular. Therefore, we try to construct 1-regular t-trivial λ-factorizations. It appears that if we start with a t-regular large set of $(t-1)$-designs, then we can construct such a factorization. More precisely, we prove the following Theorem.

Theorem 8 *Let a, b and t be three nonnegative integers such that $t < a \leq b$. If a t-trivial $LS(\lambda; t-1, t, u+t-1)$ and a $FS(\lambda w, t, w, u+t)$ exist, then a 1-regular a-trivial $FS(\lambda wab, t, wa, ub+t)$ exists.*

In order to be able to apply our construction recursively, we restrict ourselves to $(t+1)$-trivial large sets of t-designs. Our description of Teirlinck's method shows that most of his results can be easily carried to this case. In particular, the following

theorem can be proved:

Theorem 9 *Let $a = w/\delta$ in which $\delta = 2$ if w is even and $\delta = 1$ otherwise. If a 1-regular $(t+1)$-trivial $FS(\lambda, t, a, u+t)$ exists, then a $(t+1)$-trivial $LS(\delta\lambda; t, t+1, \delta uw + t)$ also exists.*

Applying these two theorems recursively, we show that in Teirlinck's theorem the equation 1 can be replaced with

$$l(t+1) = 2(t+1)(t+2)\text{l.c.m.}\{\binom{t+1}{i} | i \leq t+1\}.$$

Then we look at the large sets of a fixed size n. Again applying Theorems 8 and 9 recursively we will obtain the following theorem.:

Theorem 10 *Let n be a positive integers, then for $t \geq 0$, a $LS((2n)^t\{(t+1)!\}^2; t, t+1, 2^t n^{t+1}\{(t+1)!\}^2 + t)$ exists.*

For $t > 8$, some of designs which are constructed in Theorem 10 are the smallest known designs (of block size $t+1$). In fact, any other known nontrivial t-design with blocksize $(t+1)$ comes from Theorem 9 which is a modification of Teirlinck's main Theorem.

Finally, at the end we come back to the problem of halving complete designs. Utilizing the constructions which were developed in Chapter 2 and Theorems 8 and 9, we will prove that for $k = t+1$, the Hartman conjecture is asymptotically correct.

More precisely, we prove the following:

Theorem 11 *Let $t \geq 4$. If $v \equiv t \pmod{2^{f(t+1)}}$ and v is sufficiently large, then a $LS(1/2; t, t-1, v)$ exists.*

Chapter 1 Background

1.1 Preliminaries

Let X be a finite set, and $Y \subset \{0, \ldots, |X|\}$. The set of all subsets of X whose cardinality lies in Y will be denoted by $P_Y(X)$. For the sake of convenience we denote $P_{\{i\}}(X)$ and $P_{\{i,\ldots,j\}}(X)$ by $P_i(X)$ and $P_{i,j}(X)$, respectively.

Let X_1 and X_2 be two disjoint finite sets and let k_1 and k_2 be two nonnegative integers. Then for $\mathcal{B}_1 \subseteq P_{k_1}(X_1)$ and $\mathcal{B}_2 \subseteq P_{k_2}(X_2)$, we define

$$\mathcal{B}_1 * \mathcal{B}_2 = \{A_1 \cup A_2 | A_1 \in \mathcal{B}_1 \ \& \ A_2 \in \mathcal{B}_2\}.$$

Clearly $\mathcal{B}_1 * \mathcal{B}_2 \subseteq P_{k_1+k_2}(X_1 \cup X_2)$.

Let v, k, t, and λ be four positive integers such that $v \geq k \geq t \geq 0$. A *t-design* of *order* v, *blocksize* k, and *index* λ, or briefly a $S(\lambda; t, k, v)$ design, is a pair $D = (X, \mathcal{B})$ in which X is a finite set with cardinality v and $\mathcal{B}$ is a collection of elements of $P_k(X)$ such that every element of $P_t(X)$ appears exactly λ times in $\mathcal{B}$. D is called *uniform* of degree l or l-uniform if all of its blocks have the same multiplicity l, and it is called *simple* (1-uniform) if it has no repeated blocks. Let X be a v-set. Then it is easy to check that $(X, P_k(X))$ is a simple $S(\binom{v-t}{k-t}; t, k, v)$ design. This design is usually called the *trivial* or *complete* design and will be denoted by $TS(t, k, v)$. Before we

proceed any further, we would like to introduce the following notation which will be widely used in the rest of this thesis.

Notation 1.1.1 *Let $\mathcal{B} \subseteq P_k(X)$, for each $T \in P_t(X)$ the number of occurrences of T in the blocks of $\mathcal{B}$ will be denoted by $n(T;\mathcal{B})$. By convention, $n(T;\mathcal{B}) = 0$ whenever $t > k$.*

A simple counting argument shows that a $S(\lambda; t, k, v)$ design is also a $S(\lambda_i; i, k, v)$ design for $0 \leq i \leq t$ in which $\lambda_i\binom{k-i}{t-i} = \lambda\binom{v-i}{t-i}$. Therefore, a necessary condition for the existence of a $S(\lambda; t, k, v)$ design is that

$$\lambda_i = \lambda\binom{v-i}{t-i}/\binom{k-i}{t-i} = \lambda\binom{v-i}{k-i}/\binom{v-t}{k-t}$$

is an integer for $0 \leq i \leq t$.

Let $D = (X, \mathcal{B})$ be a $S(\lambda; t, k, v)$ design, and let $x \in X$. We define two collections $\mathcal{B}_x$ and $\mathcal{B}^x$ of subsets of $X \setminus \{x\}$ as follows:

$$\mathcal{B}_x = \{B \setminus \{x\} | x \in B \in \mathcal{B}\},$$
$$\mathcal{B}^x = \{B \in \mathcal{B} | x \notin B\}.$$

Let $S \in P_{t-1}(X \setminus \{x\})$. Then

$$n(S;\mathcal{B}_x) = n(S \cup \{x\};\mathcal{B}) = \lambda,$$
$$n(S;\mathcal{B}^x) = n(S;\mathcal{B}) - n(S \cup \{x\};\mathcal{B}) = \lambda_{t-1} - \lambda.$$

Therefore, $D_x = (X \setminus \{x\}, \mathcal{B}_x)$ and $D^x = (X \setminus \{x\}, \mathcal{B}^x)$ are $S(\lambda; t-1, k-1, v-1)$

and $S(\lambda_{t-1}-\lambda; t-1, k, v-1)$ designs, respectively. D_x and D^x are called the *derived* and *residual* designs of D with respect to x. Also we can define a collection $\mathcal{B}'$ of elements of $P_{v-k}(X)$ as follows:

$$\mathcal{B}' = \{X \setminus B \mid B \in \mathcal{B}\}.$$

Then for $T \in P_t(X)$ we have

$$n(T; \mathcal{B}') = \lambda' = \sum_{i=0}^{t} (-1)^i \binom{t}{i} \lambda_i.$$

Therefore, $D' = (X, \mathcal{B}')$ is $S(\lambda'; t, v-k, v)$ design. D' is usually called the *complement* of D.

A *large set* of disjoint $S(\lambda; t, k, v)$ designs, denoted by $LS(\lambda; t, k, v)$, is a partition of the k-subsets of a v-set into $S(\lambda; t, k, v)$ designs. Obviously, if a $LS(\lambda; t, k, v)$ exists, then $\lambda = \binom{v-t}{k-t}/n$ for some n. For the sake of simplicity, we usually write $LS(1/n; t, k, v)$ instead of $LS(\binom{v-t}{k-t}/n; t, k, v)$. Now, the necessary conditions for the existence of a $LS(1/n; t, k, v)$ can be written as $n \mid \binom{v-i}{k-i}$ for $i = 0, \ldots, t$.

Notation 1.1.2 *Let n be an integer greater than or equal to 2. The cyclic group of order n is denoted by $I_n = \{1, \ldots, n\}$. Whenever, we deal with a collection $\{A_1, \ldots, A_n\}$, we implicitly assume that subscripts are in I_n, so all subscript arithematics are performed in I_n.*

We end this section, by a simple lemma which will be implicitly used in several

places.

Lemma 1.1.1 *If a $LS(1/n; t, k, v)$ exists, then for $0 \leq i \leq t_1$ and $j \in \{k-i, \ldots, k\}$, a $LS(1/n; t-i, j, v-i)$ exist.*

Proof. Let $\{(X, \mathcal{B}_l) | 1 \leq l \leq n\}$ be a $LS(1/n; t, k, v)$, and let Y_1 and Y_2 be two subsets of X such that $Y_1 \cap Y_2 = \emptyset$, $|Y_1| = k-j$ and $|Y_2| = i+j-k$. For $1 \leq l \leq n$, let

$$\mathcal{B}'_l = \{B \setminus Y_1 | Y_2 \cap B = \emptyset \ \& \ Y_1 \subset B \in \mathcal{B}_l\}.$$

Then $\{(X \setminus (Y_1 \cup Y_2), \mathcal{B}'_l) | 1 \leq l \leq n\}$ is a $LS(1/n; t-i, j, v-i)$. □

1.2 The Incidence Matrix

Let X be a v-set, and $\mathcal{B}$ be a collection of elements of $P_k(X)$. For $B \in P_k(X)$, let $f(B)$ denote the multiplicity of B in $\mathcal{B}$. Then f is a function from $P_k(X)$ into nonnegative integers. Clearly, f uniquely determines $\mathcal{B}$. We usually use the same notation for f and $\mathcal{B}$.

For $i \leq |X|$, we choose an arbitrary ordering for $P_i(X)$. So we may write

$$P_i(X) = \{T_1, \ldots, T_{\binom{v}{i}}\},$$

$$P_k(X) = \{B_1, \ldots, B_{\binom{v}{k}}\}.$$

Given a collection g of elements of $P_k(X)$ we may identify g with the vector $(g(B_1), \ldots, g(B_{\binom{v}{k}}))$.

We define a $\binom{v}{t} \times \binom{v}{k}$ matrix $\phi_{t,k}(v) = (a_{ij})$ as follows:

$$a_{ij} = \begin{cases} 1, & \text{if } T_i \subset B_j, \\ 0, & \text{otherwise.} \end{cases}$$

Then g is a $S(\lambda; t, k, v)$ design if and only if

$$\phi_{t,k}(v).g = \lambda \mathbf{1}, \tag{1.1}$$

in which $\mathbf{1}$ is the all one vector. It is well known that if g_p is a particular solution of 1.1, then any solution of 1.1 can be written as $g = g_p + g_0$, in which g_0 is a solution of the following homogeneous system of linear equations:

$$\phi_{t,k}(v).g = 0. \tag{1.2}$$

Also it is easy to see that $\mathbf{1}$ is a solution of 1.1. Therefore, solutions of 1.2, which are called (t, k, v)-trades, are of particular interest. In the next section, we discuss some of their properties.

1.3 The Structure of (t, k, v)-Trades

Let $X = \{x_n | n \geq 1\}$ be a set of distinct indeterminates. Then a subset B of X can be identified with the monomial $\Pi_{x_i \in B} x_i$ (and the empty set will be identified with constant polynomial 1), and then every collection of the subsets of X will be

a polynomial $f \in Z[X]$ with nonnegative coefficients. Let $f \in Z[X]$. We say f is *regular* of degree (or blocksize) k if $f = \sum_{i=1}^{m} n_i X_i$ in which n_i's are nonzero integers, and X_i's are distinct k-subsets of $P_k(X)$. Therefore, 0-regular polynomials are just integers. f is called simple if $|n_i| = 1$ for $i \leq m$. Let f be a regular polynomial of degree k. We define found(f) to be the set of all x_i's such that $\deg_{x_i}(f) = 1$, and the order of f to be the cardinality of found(f). We also define

$$f^+ = \sum_{i=1}^{m} \max(n_i, 0) X_i,$$

$$f^- = \sum_{i=1}^{m} \min(n_i, 0) X_i,$$

$$\text{supp}(f) = f^+ + f^-.$$

Then $f = f^+ - f^-$. For $t \leq k$, we have

$$\phi_{t,k}(f) = \sum_{i=1}^{m} n_i P_t(X_i).$$

Since the parameter k is uniquely determined by f, we usually skip the subscript k in $\phi_{t,k}$ and we simply write ϕ_t.

A regular polynomial f of order v and blocksize k is called a ***signed design*** with parameters t, k, v, λ (denoted by $SS(\lambda; t, k, v)$) if $\phi_t(f) = \lambda P_t(\text{found}(f))$, and it is a t-design if $f^- = 0$. A (t, k, v)-***trade*** is a $SS(0; t, k, v)$ design. Clearly, a (t, k, v) trade is also a (t, k, u)-trade for $u \geq v$. Therefore, we usually skip the parameter v are refer to a (t, k, v)-trade as a (t, k)-trade. $\frac{1}{2}\phi_0(Supp(T))$ is called ***volume*** of T and is denoted by $\text{Vol}(T)$. Let T be a (t, k, v)-trade and $x \in Found(T)$. As in the

case of ordinary t-designs, we may define T_x and T^x. If $t > 0$, then T_x and T^x are $(t-1, k-1, v-1)$ and $(t-1, k, v-1)$-trades, respectively.

Lemma 1.3.1 *Let T be a nonzero (t,k)-trade, then $|found(T)| \geq k + t + 1$, and $Vol(T) \geq 2^t$.*

Proof. Since T is nonzero, it contains at least two distinct blocks. Therefore, the assertion is true for $t = 0$, and if $t > 0$, then there exists $x \in \text{found}(T)$ such that both T_x and T^x are nonzero. Thus, $\text{Vol}(T) = \text{vol}(T_x) + \text{vol}(T^x)$, and $|\text{found}(T)| \geq |\text{found}(T^x)| + 1$. Now, the assertion follows by induction on t. □

In Lemma 1.3.1, if both equalities hold, then T is called a ***minimal*** (t,k)-***trade.*** Now it is easy to check that if f is of blocksize k and $t \leq s < k$, then

$$\phi_t\phi_s(f) = \left[\binom{k}{s}\binom{s}{t}/\binom{k}{t}\right]\phi_t(f).$$

Therefore, a (t,k)-trade is also an (i,k)-trade for $0 \leq i \leq t$. Now if f and g are regular polynomials such that $\text{found}(f) \cap \text{found}(g) = \emptyset$, then fg is also regular, and

$$\phi_s(fg) = \sum_{i=0}^{s} \phi_i(f)\phi_{s-i}(g). \tag{1.3}$$

Therefore, if T_1 is a (t_1, k_1)-trade, T_2 is a regular polynomial of blocksize k_2, and $\text{found}(T_1) \cap \text{found}(T_2) = \emptyset$, then T_1T_2 is a $(t_1, k_1 + k_2)$-trade, and if T_2 is also a (t_2, k_2)-trade, then T_1T_2 is a $(t_1 + t_2 + 1, k_1 + k_2)$-trade, and in both cases, we have

$\text{supp}(T_1T_2) = \text{supp}(T_1)\text{supp}(T_2)$. Now, it is obvious that if $y_1, \ldots, y_{k+t+1}$ are distinct elements of X, then

$$T = (y_1 - y_2)\ldots(y_{2t+1} - y_{2t+2})y_{2t+3}\cdots y_{k+t+1}$$

is a minimal (t,k)-trade. It is well known that any minimal trade is of this form.

Let $V = \{x_1, \ldots, x_v\}$. The set of all (t,k)-trades whose foundation is a subset of V form a $\mathbf{Z}$-module which is usually denoted by $N(t,k,v)$. In fact, $N(t,k,v)$ is the null space of the incidence matrix $\phi_{t,k}(v)$. We have already shown that if $v < k+t+1$, then $N(t,k,v) = \{0\}$. We will prove that if $v > k+t$, then $\dim N(t,k,v) = \binom{v}{k} - \binom{v}{t}$, and we will find a triangular basis consisting of minimal trades.

Let T be a (t,k,v)-trade whose foundation is a subset of V, and let B be the smallest block in $\text{Supp}(T)$ in the lexicographic order. Write $B = \{x_i | i \in I\}$ in which $I = \{b_1, \ldots, b_k\} \in P_k(\{1, \ldots, v\}$ and $b_1 < b_2 < \cdots < b_k$. Let $i \in \{1, \ldots, t+1\}$, $A = \{x_{b_1}, \ldots, x_{b_{i-1}}\}$ and let $S = T_A$ be the derived trade of T with respect to the set A. Then S is a nonzero $(t+1-i, k+1-i)$-trade and since B is the smallest block in T, we must have

$$\text{found}(S) \subset \{x_j | b_i \leq j \leq v\}.$$

Therefore,

$$(t+1-i) + (k+1-i) < \text{found}(S) \leq v + 1 - b_i,$$

or equivalently

$$b_i \leq v-k-t-2+2i, \quad 1 \leq i \leq t+1.$$

Also it is trivial that $b_i \leq v-k+i$ for $t+1 < i \leq k$.

Definition 1.3.1 *Let $B = \{a_1, \ldots, a_k\} \in P_k(\{1, \ldots, v\})$ and $a_1 < \cdots < a_k$. Then B is called a (t, k, v)-starting block (or simply a starting block whenever the parameters t, k and v are clear from the context) if the following inequalities hold:*

$$\begin{cases} a_i \leq v-k-t-2+2i, & \text{for } 1 \leq i \leq t+1, \\ a_i \leq v-k+i & \text{otherwise.} \end{cases} \tag{1.4}$$

The set of all (v, k, t)-starting blocks and its cardinality will be denoted by $M(t, k, v)$ and $n(t, k, v)$, respectively.

Lemma 1.3.2 *If $v > k+t$, then $n(t, k, v) = \binom{v}{k} - \binom{v}{t}$.*

Proof. We prove the assertion by induction on v. Let $B = \{a_1, \ldots, a_k\} \in P_k(\{1, \ldots, v\})$ and $a_1 < \cdots < a_k$. We consider two cases:

Case (i): $a_1 = 1$. Now $B \in M(t, k, v)$ if and only if $B_1 = \{a_i - 1 | 2 \leq i \leq k\} \in M(t-1, k-1, v-1)$. Therefore, there are exactly $m(t-1, k-1, v-1)$ blocks of this form in $M(t, k, v)$.

Case (ii): $a_1 > 1$. If $v = k+t+1$, then $B \notin M(t, k, v)$ as 1.4 doesn't hold. Let $v > k+t+1$. Then $B \in M(t, k, v)$ if and only if $B_1 = \{a_i - 1 | 1 \leq i \leq k\} \in M(t, k, v-1)$. Therefore, there are exactly $m(t, k, v-1)$ blocks of this form in $M(t, k, v)$.

Therefore, we have the following recursive equations for $m(t,k,v)$'s

$$m(t,k,v) = \begin{cases} m(t-1,k-1,v-1), & \text{if } v = k+t+1, \\ m(t-1,k-1,v-1) + m(t,k,v-1), & \text{if } v > k+t+1, \end{cases}$$

and the assertion follows by induction on $k+t$. □

Lemma 1.3.3 *Let $B \in M(t,k,v)$. Then there exists a minimal (t,k,v)-trade T_B whose smallest block (in lexicographic order) is B and found$(T) \subset V$.*

Proof. Let $B = \{a_1, \ldots, a_k\}$ and $a_1 < \cdots < a_k$. Let

$$A_{t+1} = \{j | a_{t+1} < j \leq v \ \& \ j \notin B\},$$

and let $c_{t+1} = \min\{i | i \in A_{t+1}\}$. Now, for $2 \leq i \leq t+1$, we define A_{t+2-i} and c_{t+2-i} recursively by

$$A_{t+2-i} = \{j | a_{t+2-i} < j \leq v \ \& \ j \notin B\} \setminus \{c_j | t+2-i < j \leq t+1\},$$
$$c_{t+2-i} = \min\{l | l \in A_{t+2-i}\}.$$

(notice that by 1.4 each A_i is nonempty. Let

$$T_B = (x_{a_1} - x_{c_1}) \ldots (x_{a_{t+1}} - x_{c_{t-1}}) x_{a_{t+2}} \ldots x_{a_k}.$$

Then it is easy to check that B is the smallest block of T_B. □

Theorem 1.3.1 *$\mathcal{B} = \{T_B | B \in M(t,k,v)\}$ form a basis for $N(t,k,v)$. In particular, $dim N(t,k,v) = n(t,k,v) = \binom{v}{k} - \binom{v}{t}$ if $v > k+t$.*

Proof. Clearly $\mathcal{B}$ is an independent set as it is triangular (the starting blocks of its elements are distinct). We prove that $\mathcal{B}$ spans $N(t,k,v)$. Let T be a (t,k,v)-trade and let B be the smallest block in T. Let a_B be the multiplicity of B in T. Then $T - a_B T_B$ is also in $N(t,k,v)$ and its smallest block is greater than B. Repeating this process, we can find a positive integer l, starting blocks $B_1, \ldots, B_l$ and nonzero integers $a_1, \ldots, a_l$ such that $S = T - \sum_{i=1}^{l} a_i T_{B_i}$ does not contain any starting block. But we have already seen that the smallest block of any nonzero (t,k,v)-trade is a starting block, so $S = 0$, i.e. $T = \sum_{i=1}^{l} a_i T_{B_i}$ is in the span of $\mathcal{B}$. □

Theorem 1.3.2 *The t-set inclusion matrix $\phi_{t,k}(v)$ is of full rank.*

Proof. By definition $N(t,k,v)$ is the null space of $\phi_{t,k}(v)$. Therefore, $\text{rank}(\phi_{t,k}(v) = \binom{v}{k} - \dim(N(t,k,v) = \max\{\binom{v}{k}, \binom{v}{t}\}$. □

Lemma 1.3.4 *Let T be a $(t, t+1)$-trade, and B be a m-subset which is disjoint from found(T). Then $\phi_{t+1}(TB) = T$.*

Proof. The assertion is an immediate consequence of the identity 1.3 and the fact that a t-trade is also an i-trade for $i \leq t$. □

Theorem 1.3.3 *The necessary conditions for the existence of a $SS(\lambda; t, k, v)$ design are also sufficient.*

Proof. We remind that the necessary conditions are as follows: $\lambda_i = \lambda\binom{v-i}{t-i}/\binom{k-i}{t-i}\lambda$ is an integer for $0 \leq i \leq t$. We prove by induction on i $(0 \leq i \leq t)$ that a $SS(\lambda_i; i, k, v)$ exists. For $i = 0$ the assertion is trivial. Let $i > 0$, and let f be a $SS(\lambda_{i-1}; i-1, k, v)$ and $V = \text{found}(f)$. Let $g = \phi_i f - \lambda_i P_i(V)$. Then

$$\begin{aligned}\phi_{i-1}(g) &= \phi_{i-1}\phi_i f - \lambda_i \phi_{i-1}(P_i(V)) = (k+1-i)\phi_{i-1} f - (v+1-i)\lambda_i P_{i-1}(V) \\ &= ((k+1-i)\lambda_{i-1} - (v+1-i)\lambda_i)P_{i-1}(V) = 0.\end{aligned}$$

Therefore, g is a $(i-1, i)$-trade. By Theorem 1.3.1, we can write $g = \sum_{i=1}^{l} T_i$ in which T_i's are (not necessarily distinct) minimal $(i-1, i)$-trades. For $1 \leq i \leq l$, we choose $B_i \in P_{k-i}(V \setminus \text{found}(T_i))$. Then $h = g = \sum_{i=1}^{l} B_i T_i$ is a $(i-1, k)$-trade and by Lemma 1.3.4, $\phi_i(h) = g$. Now, we have

$$\phi_i(f - h) = \phi_i(f) - g = \lambda_i P_i(V).$$

Therefore $f - h$ is a $SS(\lambda_i; i, k, v)$ design. □

Theorem 1.3.4 *The necessary conditions for the existence of a $S(\lambda; t, k, v)$ are also sufficient whenever λ is sufficiently large.*

Proof. Let $\lambda(t, k, v) = \binom{v-t}{k-t} / \gcd\{\binom{v-i}{k-i} | 0 \leq i \leq t\}$. Then the necessary conditions for the existence of a $S(\lambda; t, k, v)$ can be written is the compact form $\lambda(t, k, v) | \lambda$. Let $n = \binom{v-t}{k-t}/\lambda(t, k, v)$. Let V be a v-set. For $i = 1, \ldots, n-1$, let f_i be a $SS(i\lambda(t, k, v); t, k, v)$ design on V and let N be the maximum of the multiplicities of

the blocks in the f_i^-'s. Then for $m \geq N$, $f_i + mP_k(V)$ is a $SS((mn+i)\lambda(t,k,v);t,k,v)$ design. In other words, the necessary conditions are also sufficient if $\lambda > N\binom{v-t}{k-t}$. □

Remark 1.3.1 *All of the results of this section except the existence of a triangular basis were originally proved by Graver and Jourkat [16]. The existence of this basis was established in [22]. Theorems 1.3.2, 1.3.3 and 1.3.4 were also independently proved by Wilson [44]. Proofs of Theorems 1.3.3 and 1.3.4 are rewritten from [16]. The rest of proofs are either new or a modification of a existing proof.*

1.4 Review of Known Results

In this section, we survey the known results for the existence of large sets of t-designs.

Let us start with $t = 1$. For $k = 2$, a $LS(\lambda;1,2,n)$ is simply a λ-factorization of K_n. It is well known that the necessary conditions for the existence of a λ-factorization of K_n are also sufficient. For $k > 2$, the same result is proved by Baranyai [6].

Next case is $t = 2$. For $k = 3$ a $S(\lambda;t,k,v)$ is called a triple system of order v and index λ. It is easy to see that a $LS(1;2,3,7)$ does not exist [7]. On the other hand, for any other value of v, the necessary conditions are also sufficient. This was proved through a series of recursive constructions developed by different authors which reduced the problem to a few small cases which were known to exist. The existence of $LS(3;2,3,6m+5)$ and $LS(6;2,3,6m+2)$ is established by Teirlinck [38], as these large sets can be derived from $LS(3\gcd\{4,n-1\};3,4,3n)$. For $v \equiv 0$ or 4

(mod 12), the result is proved by Schreiber [34]. Utilizing this result, Teirlink proved that a $LS(2\gcd\{3, u-1\}; 2, 3, 2u+2)$ exists for all $u \geq 1$ [40]. These results together reduce the problem to the case of Steiner triple systems, i.e. $\lambda = 1$ and $v \equiv 1$ or 3 (mod 6). This case was settled by Lu [29, 30] with at most six possible exceptions after several other authors had obtained partial results [7, 13, 24, 32, 33, 39, 43]. These six cases were settled in [35].

For $t = 2$ and $k > 3$ not much is known on the existence of large sets. For $v < 13$, it is shown in [26] that the necessary conditions for the existence of a large set are also sufficient except for $(t, k, v) = (2, 3, 7)$. Chouinard [10] has established the existence of a $LS(1; 2, 4, 13)$. This is the only known $LS(1; t, k, v)$ with $t \geq 2$ and $k \neq 3$. In [8], it is proved that a $LS(\binom{k}{2}; 2, k, v)$ exists whenever v is a prime power and $\gcd\{v(v-1), k(k-1)\} = 2$. One can also find some other families of large sets in [8], e.g. a $LS(15; 4, 6, 14)$.

In [17], Hartman has considered the partitioning of the complete design $(X, P_k(X))$ into two parts (designs) of equal number of blocks. He proved that the necessary conditions are also sufficient whenever $t = 2$ and $k = 3, 4$. He also obtained several other infinite families of this form. Consequently he makes the following conjecture:

Conjecture (A. Hartman, 1987). *There exists a partition of the complete design* $S\left(\binom{v-t}{k-t}; t, k, v\right)$ *into two* $S\left(\binom{v-t}{k-t}/2; t, k, v\right)$ *designs if and only if* $\binom{v-i}{k-i}$ *is even for* $i = 0, \ldots, t$.

This conjecture is proved to be correct for $t = 2$ and $k < 16$ [4]. In [28], Kreher and Radsznowski constructed a $LS(4; 6, 7, 14)$. Existence of this large set together with some well known recursive constructions establishes the Hartman conjecture for $t = 6$, $k = 7$. Then, taking the derived and the residuals of the large sets in this family one can settle the Hartman conjecture for $k \leq 7$.

In [37], Teirlinck introduced r-trivial λ-factorizations and developed some recursive methods to construct r-trivial λ-factorizations. In particular, he proved that for given t there exists $\lambda(t)$ such that the necessary conditions for the existence of a $LS(\lambda, t, t+1, v)$ are also sufficient whenever $\lambda(t)|\lambda$, and $\lambda(t)$ can be defined recursively by $\lambda(0) = 1$, and $\lambda(t+1) = \lambda(t)l(t+1)$ in which $l(t) = \text{lcm}\{1, \ldots, t+1\} \cdot \text{lcm}\{\binom{t}{i} | i = 1, \ldots, t\}$. He also obtained a few infinite families of large sets for $t \leq 6$.

Chapter 2 t-Wise Equivalence

In this chapter, we introduce the notion of *t-wise equivalent* sets which is basically a generalization of (t, k, v) trades. In the first section, we will discuss their importance in constructing large sets, and we find some recursive procedures to construct them. in the second section, we use t-wise equivalent sets to find several recursive constructions which will be useful in consequent chapters. Finally in the third section, to emphasize their importance and strength even more, we show how this simple idea can lead to constructing large sets of prime size and small order for all t.

2.1 t-Wise Equivalent Sets

Definition 2.1.1 *Let X be a finite set, and let t and k be two positive integers such that $t < k$. Two subsets A and B of $P_k(X)$ are said to be t-wise equivalent if the number of occurrences of each $T \in P_t(X)$ in A and B are the same, i.e. $n(T; A) = n(T; B)$. In particular, A and B are 0-wise equivalent if and only if $|A| = |B|$.*

Before we proceed in this line, we would like to make some remarks on the above definition to clarify its significance on constructing large sets.

Remark 2.1.1 *Simple enumerative arguments shows that any two t-wise equivalent sets are also $(t-1)$-wise equivalent. Hence, if $0 \leq i \leq t$, then any two t-wise equivalent sets are also i-wise equivalent.*

Remark 2.1.2 *Let X be a v-set, and let $\{\mathcal{B}_1, \ldots, \mathcal{B}_n\}$ be a partition of $P_k(X)$ into n mutually t-wise equivalent sets. Now, the numbers of occurrences of each $T \in P_t(X)$ in all $\mathcal{B}_i$'s are the same, and on the other hand, each t-subset of X in total appears in exactly $\binom{v-t}{k-t}$ blocks of the $\mathcal{B}_i$'s. Hence, each $(X, \mathcal{B}_i)$ $(1 \leq i \leq n)$ is a simple $S(\binom{v-t}{k-t}/n; t, k, v)$, and $\{(X, \mathcal{B}_i) | 1 \leq i \leq n\}$ is a $LS(\binom{v-t}{k-t}/n; t, k, v)$.*

Remark 2.1.3 *If $\mathcal{B}_1, \ldots, \mathcal{B}_m$ are mutually disjoint subsets of $P_k(X)$ such that each of them has a partition into n mutually t-wise equivalent sets, then their union, $\cup_{i=1}^{m} \mathcal{B}_i = \mathcal{B}$ has also a partition into n t-wise equivalent sets.*

In the light of the above remarks, our approach to construct large sets is as follows. First, we present some procedures to construct the (n, t)-***partitionable*** sets (the sets which have a partition into n disjoint t-wise equivalent subsets) from the (n, t_1)-partitionable sets $(t_1 \leq t)$, and then we give a partition of $P_k(X)$ into such sets. The following Lemma shows how one can construct (n, t)-partitionable sets from the older ones.

Lemma 2.1.1 *Let X_1 and X_2 be two disjoint sets, and let t_1, t_2, k_1, and k_2 be four integers such that $0 \leq t_1 \leq k_1$ and $0 \leq t_2 \leq k_2$. For $i = 1, 2$, let $\mathcal{B}_i \subseteq P_{k_i}(X_i)$, and suppose that $\mathcal{B}_1$ has a partition, say $\{\mathcal{F}_i | 1 \leq i \leq m\}$, into m mutually t_1-wise equivalent subsets. Then (i) $\mathcal{B}_1 * \mathcal{B}_2$ has a partition into m mutually t_1-wise*

equivalent subsets.

(ii) if $\mathcal{B}_2$ has a partition into m mutually t_2-wise equivalent subsets, then $\mathcal{B}_1 * \mathcal{B}_2$ has a partition into m mutually $(t_1 + t_2 + 1)$-wise equivalent subsets.

Proof. (i) It is easy to show that $\{\mathcal{F}_i * \mathcal{B}_2 | 1 \leq i \leq m\}$ is a partition of $\mathcal{B}_1 * \mathcal{B}_2$ into t_1-wise equivalent subsets. To prove (ii) let $\{\mathcal{G}_i | \leq i \leq m\}$ into m mutually t_2-wise equivalent subsets, and define

$$\mathcal{H}_i = \sum_{j=1}^{m} \mathcal{F}_j * \mathcal{G}_{a_{ij}}, \ 1 \leq i \leq m$$

in which $A = (a_{ij})$ is Latin square of order m. Let $T \in P_{t_1+t_2+1}(X_1 \cup X_2)$. Then either $|T \cap X_1| \leq t_1$ or $|T \cap X_2| \leq t_2$. If $|T \cap X_1| \leq t_1$, then we have

$$\begin{aligned} n(T;\mathcal{H}_i) &= \textstyle\sum_{j=1}^{m} n(T \cap X_1; \mathcal{F}_j) n(T \cap X_2; \mathcal{G}_{a_{ij}}) \\ &= \textstyle\sum_{j=1}^{m} [n(T \cap X_1; \mathcal{B}_1)/m]\, n(T \cap X_2; \mathcal{G}_{a_{ij}}) \\ &= \left[\textstyle\sum_{j=1}^{m} n(T \cap X_2; \mathcal{G}_{a_{ij}})\right] n(T \cap X_1; \mathcal{B}_1)/m \\ &= n(T \cap X_1; \mathcal{B}_1) n(T \cap X_2; \mathcal{B}_2)/m = n(T; \mathcal{B}_1 * \mathcal{B}_2)/m. \end{aligned}$$

A similar argument will work for $|T \cap X_2| \leq t_2$. Therefore $\mathcal{H}_i$'s are $(t_1 + t_2 + 1)$-wise equivalent. □

We end this section, with the following lemma which is a very simple but still useful application of t-wise equivalent sets in construction of large sets. This lemma is a special case of a more general construction by Van Trung [42].

Lemma 2.1.2 *If* $v \in \cap_{i=0}^{l} A(t, k+i)$, *then* $v + l \in A(t, k+l)$.

Proof. Let $|X| = v$, $Y_i = \{1, \ldots, i\} (1 \leq i \leq l)$ and $X \cap Y_l = \emptyset$. Then $\{Y_i * P_{k+l-i}(X) | 1 \leq i \leq l\}$ is a partition of $P_{k+l}(X \cup Y_l)$. Now, the assertion follows by remarks 2.1.1, 2.1.2, 2.1.3 and Lemma 2.1.1. □

2.2 Large Sets

In the following lemma, we obtain a partition of $P_k(X)$ which would be useful in establishing some of our main results. But first, we must give a couple more definitions.

Definition 2.2.1 *A finite set* Y *is said to be of the form* $\binom{v_1}{k_1} * \binom{v_2}{k_2}$ *whenever there exist two disjoint finite sets* Y_1 *and* Y_2 *such that* $|Y_1| = v_1$, $|Y_2| = v_2$, *and* $Y = P_{k_1}(Y_1) * P_{k_2}(Y_2)$.

Notation 2.2.1 *The set of all* v*'s such that an* $LS(1/n; t, k, v)$ *exists will be denoted by* $A(t, k, n)$.

Lemma 2.2.1 *Let* u, v *and* k *be three positive integers such that* $k \leq \min(u, v)$, *and let* X *be a* $(u + v - k + 1)$*-set. Then* $P_k(X)$ *has a partition* $\{\mathcal{B}_1, \ldots, \mathcal{B}_{k+1}\}$ *in which* $\mathcal{B}_i$ *is of the form* $\binom{v-i+1}{k+1-i} * \binom{u-k+i-1}{i-1}$.

Proof. Let $X = \{1, \ldots, u+v-k+1\}$. For $1 \leq i \leq k+1$, we define

$$X_i = \{1, \ldots, v+1-i\},$$
$$Y_i = \{v+3-i, \ldots, u+v-k+1\},$$
$$\mathcal{B}_i = P_{k+1-i}(X_i) * P_{i-1}(Y_i).$$

Clearly, each $\mathcal{B}_i$ is of the desired form. We will show that they form a partition of $P_k(X)$.

First, we show that $\mathcal{B}_i$'s are pairwise disjoint. Let $1 \leq i < j \leq k+1$, and $B \in \mathcal{B}_j$. Then $v+2-j \notin B$, so

$$|B \cap X_i| = |B \cap X_j| + |B \cap (X_i \setminus X_{j+1})| \leq |B \cap X_j| + |X_i \setminus X_{j+1}|$$
$$\leq (k+1-j) + (j-i-1) = k-i,$$

while for $C \in \mathcal{B}_i$, $|C \cap X_i| = k+1-i$. Therefore, $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$.

Let $B \in P_k(X)$, and let $r_i = |B \cap X_i|$, $1 \leq i \leq k+1$. Clearly, we have

$$0 \leq r_{i+1} \leq r_i \leq r_{i-1} + 1 \leq k+1.$$

If $r_1 = 0$, then $B \in \mathcal{B}_{k+1}$. If $r_{k+1} = k$, then we have $B \in \mathcal{B}_1$. Otherwise, we can find l such that $r_l = r_{l-1} = k+1-l$, and consequently $|B \cap X_l| = k+1-l$ and $v+2-l \notin B$, so $B \in \mathcal{B}_l = P_{k+1-l}(X_l) * P_{l-1}(Y_l)$. Therefore, $\cup_{i=1}^{k+1} \mathcal{B}_i = P_k(X)$. □

Lemma 2.2.2 *Let v_1, v_2, s and k be three positive integers such that $s \leq k-1 < \min(v_1, v_2)$. Let a and b be two nonnegative integers such that $a+b = k-1-s$. Let*

Z be a set of the form $\binom{v_1+v_2-s}{k}$. Then Z has a partition $\{C_1, \ldots, C_{k+1}\}$ such that

(i) for $1 \le i \le a+1$, C_i is of the form $\binom{v_1}{k+1-i} * \binom{v_2-s}{i-1}$,

(ii) for $1 \le i \le s$, C_{a+1+i} is of the form $\binom{v_1-i}{k-a-i} * \binom{v_2-s+i-1}{a+i}$

(iii) for $1 \le i \le b+1$, C_{k+2-i} is of the form $\binom{v_1-s}{i-1} * \binom{v_2}{k+1-i}$.

Proof. Let $u = v_2 + k - s - 1$, $v = v_1 + k - s - 1$, and define X, X_i, Y_i and $\mathcal{B}_i$'s $(1 \le i \le k+1)$ as in Lemma 2.2.1. Let

$$Y_1 = \{v-k+1, \ldots, v-k+b\} \cup \{v-a+1, \ldots, v\},$$

then $|X \backslash Y_1| = v_1+v_2-s$, so without loss of generality we may assume $Z = P_k(X \backslash Y_1)$. Let

$$C_i = \{B | B \in \mathcal{B}_i \ \& \ B \cap Y_1 = \emptyset\}, \ 1 \le i \le k+1.$$

It is straightforward to check that the C_i's have the desired properties. □

Theorem 2.2.1 *Let a, b, c, d, t, s, k, v_1 and v_2 be nonnegative integers such that $t \le s < k \le \min\{v_1, v_2\}$ and $s = k-1-a-b = t+c+d$. Let $v_1 \in \cap_{i=k-a}^{k} A(t,i,n)$, $v_2 \in \cap_{i=k-b}^{k} A(t,i,n)$, $v_1 - l \in A(t, k-a-l)$ for $1 \le l \le c$, and $v_2 - l \in A(t, k-b-l, n)$ for $1 \le l \le d$. Then $v_1 + v_2 - s \in A(t,k,n)$.*

Proof. Let Z be a set of the form $\binom{v_1+v_2-s}{k}$. Define C_i's $(1 \le i \le k+1)$ as in Lemma 2.2.2. In view of Remarks 2.1.2 and 2.1.3, in order to prove the statement, we must show that each C_i is (n,t)-partitionable.

If $i \leq a+c+1$ or $k-b-d \leq i$, then C_i is product of a (n,t)-partitionable set and another set, so by Lemma 2.1.1 C_i is (n,t)-partitionable.

Let $a+c+1 < i \leq k-b-d$ and write $i = a+c+1+j$. Then $1 \leq j \leq t$ and C_i is of form $\binom{v_1-c-j}{k-a-c-j} \times \binom{v_2-s+j+c-1}{a+c+j}$. Now, by assumption $v_1 \in A(t, k-a, n)$ and $v_2 \in A(t, k-b, n)$, so by Lemma 1.1.1, $v_1 - j - c \in A(t-j, k-a-c-j, n)$ and $v_2 - s + j + c - 1 = v_2 - d - (t+1-j) \in A(j-1, a+c+j, n)$. Therefore, by Lemma 2.1.1, C_i is (n,t)-partitionable. □

Theorem 2.2.2 *If* $v \in \cap_{i=t+1}^{k} A(t,i,n)$ *and* $u \in A(t,k,n)$, *then* $\{u + l(v-t) | l \geq 1\} \subset A(t,k,n)$.

Proof. The assertion follows by induction on l (and applying Theorem 2.2.1 with $b = c = d = 0$). □

In particular, if $k = t+1$, we will have the following theorem.

Theorem 2.2.3 *If a* $LS(\lambda; t, t+1, u+t)$ *exists, then a* $LS(m\lambda; t, t+1, mu+t)$ *also exists for all* $m \geq 1$.□

2.3 Large Sets of Prime Size

Throughout this section, we assume p is a prime, u, k and n are positive integers such that $np \leq k < (n+1)p$ and $u > n$. Let $X = \{1, \ldots, up\}$ and $A_i = \{(i-1)p + 1, \ldots, ip\}$ for $1 \leq i \leq u$. Let $Y = \{A_1, \ldots, A_u\}$ and order Y by

$$A_i < A_j \text{ if and only if } i < j$$

We define a function ϕ from the power set of Y into the power set of X by

$$\phi(B) = \bigcup_{A_i \in B} A_i, \text{ for } B \subset Y.$$

The following lemma is immediate.

Lemma 2.3.1 *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are j-wise equivalent subsets of $P_m(Y)$, then $\phi(\mathcal{B}_1)$ and $\phi(\mathcal{B}_2)$ are j-wise equivalent subsets of $P_{mp}(X)$.* □

Let $l, m, a_1, \ldots, a_l$ be positive integers such that $l \geq 1$, $1 \leq a_i < p$ $(1 \leq i \leq l)$ and $k = mp + \sum_{i=1}^{l} a_i$. Let $B \in P_k(X)$ and $T = \{C_1, \ldots, C_l\} \in P_l(Y)$, $C_1 < \ldots < C_l$. Define

$$\begin{aligned}
Supp(B) &= \{A_i | A_i \cap B \neq \emptyset\}, \\
f(B) &= \{A_i | A_i \subset B\}, \\
g(B) &= Supp(B) \setminus f(B), \\
\Gamma(T, a_1, \ldots, a_l) &= \{B \subset X | \ |B \cap C_i| = a_i \ \& \ g(B) = Supp(B) = T\}, \\
\mathcal{F}_m(T, a_1, \ldots, a_l) &= \{B \in P_k(X) | \ |B \cap C_i| = a_i \ \& \ g(B) = T\},
\end{aligned}$$

and let

$$\mathcal{P} = \{\mathcal{F}_m(T, a_1, \ldots, a_l) | l \geq 1, \ T \in P_l(Y), \ 1 \leq a_i < p, \ \& \sum_{i=1}^{l} a_i = k - mp\}.$$

Clearly, we have

$$\cup\{A | A \in \mathcal{P}\} = \{B \in P_k(X) | g(B) \neq \emptyset\}.$$

Therefore we have the following lemma.

Lemma 2.3.2 *(i) If $k \neq np$, then $\mathcal{P}$ is partition of $P_k(X)$, and (ii) if $k = np$, then $\mathcal{P}$ is a partition of $P_k(X) \setminus \phi(P_n(Y))$.* □

Lemma 2.3.3 *If $T \in P_l(Y)$, and $1 \leq a_i < p (1 \leq i \leq l)$, then $\Gamma(T, a_1, \ldots, a_l)$ is $(p, l-1)$ partitionable.*

Proof. Let $T = \{C_1, \ldots, C_l\}$ with $C_1 < \ldots C_l$. Then

$$\Gamma(T, a_1, \ldots, a_l) = \Gamma(T \setminus \{C_l\}, a_1, \ldots, a_{l-1}) * P_{a_l}(C_l).$$

Since p is prime, $p|\binom{p}{a_l}$, and so $P_{a_l}(C_l)$ is $(p, 0)$-partitionable. Now, the assertion follows by induction on l. □

Lemma 2.3.4 *If $T \in P_l(Y)$, and $1 \leq a_i < p$ $(1 \leq i \leq l)$, then*

(i) $\mathcal{F}_m(T, a_1, \ldots, a_l)$ is $(p, l-1)$-partitionable,

(ii) if a $LS(1/p; s, m, u-l)$ exists, then $\mathcal{F}_m(T, a_1, \ldots, a_l)$ is $(p, s+l)$-partitionable.

Proof. It is easy to check that

$$\mathcal{F}_m(T, a_1, \ldots, a_l) = \phi(P_m(Y \setminus T)) * \Gamma(T, a_1, \ldots, a_l).$$

Now, the assertion is an immediate consequence of the Lemmas 2.1.1, 2.3.1, and 2.3.3. □

Theorem 2.3.1 *If a* $LS(1/p; t, n, u)$ *exists, then a* $LS(1/p; t, pn, pu)$ *also exists.*

Proof. Let $k = np$ and $\mathcal{F}_m(T, a_1, \ldots, a_l) \in \mathcal{P}$. If $l \leq t$, then $(n-m)p = \sum_{i=1}^{l} a_i < lp$, so $m \geq n-l$, and then by Lemma 1.1.1 a $LS(1/p; t-l, m, u-l)$ exists. Therefore, by Lemma 2.3.3, $\mathcal{F}_m(T, a_1, \ldots, a_l)$ is (p, t)-partitionable. By the assumption and Lemma 2.3.1, $\phi(P_n(Y))$ is also (p, t)-partitionable. Now, the assertion follows by Lemmas 2.1.1, 2.3.2 and 2.3.3. □

Theorem 2.3.2 *If a* $LS(1/p; t, n, u-1)$ *exists and* $np < k < (n+1)p$, *then a* $LS(1/p; t+1, k, pu)$ *also exists.*

Proof. Let $\mathcal{F}_m(T, a_1, \ldots, a_l) \in \mathcal{P}$. If $l \leq t+1$, then $(n-m)p = \sum_{i=1}^{l} a_i < lp$, so $m > n-l$, and then by Lemma 1.1.1, a $LS(1/p; t+1-l, m, u-l)$ exists. Therefore, by Lemma 2.3.4, $\mathcal{F}_m(T, a_1, \ldots, a_l)$ is $(p, t+1)$-partitionable. Now, the assertion follows from the Lemmas 2.1.1, 2.3.2 and 2.3.3. □

Theorem 2.3.3 *If a* $LS(1/p; t, n, u-1)$ *exists and* $1 \leq j < i < p-1$, *then a* $LS(1/p; t+1, np+i, pu+j)$ *also exists.*

Proof. The assertion is an immediate consequence of Lemma 2.1.2 and Theorem 2.3.2. □

Now we apply Theorem 2.3.2 to find some infinite families of large sets of t-designs for all t.

Theorem 2.3.4 *If* $t \geq 6$ *and* $m \geq 2$, *then a* $LS(1/p; t, 2^{t-3}-1, m2^{t-3}-2)$ *exists.*

Proof. It is well known that if $m \geq 2$, then a $LS(1/2; 6, 7, 8m-2)$ exists [21, 28, 37]. Now, the result follows by induction on t (and applying Theorem 2.3.2). □

Theorem 2.3.5 *Let p be any odd prime, and $l,\ t, m,\ a_0, \ldots, a_{t-1}$ be positive integers such that $t, l, m \geq 1$ and $1 \leq a_i < p$. Then a $LS(1/p; t, \sum_{i=0}^{t-1} a_i p^i + mp^t, (l-1)p^{t+1} + \sum_{i=1}^{t} p^i)$ exists.*

Proof. Trivially for $1 \leq m < p$ a $LS(1/p; 0, m, lp)$ exists. Now, the assertion follows by induction on t. □

Chapter 3 Halving Complete Designs

In this chapter, we restrict ourselves to large sets of size 2. Applying recursive constructions which were developed in Chapter 2, we show that to prove the Hartman conjecture for given t and k, one only need to check the existence of finitely many designs.

For $k \leq 7$, all these auxiliary designs can be obtained by taking residual and derived designs of a $S(4; 6, 7, 14)$.

For $t = 2$ we give a direct construction for these designs, and so we prove the Hartman conjecture for $t = 2$. For $t = 3$ and $k < 16$, it is well known that these auxiliary designs exist.

For $t = 3$ and $k > 16$ we are not aware of any constructions for these designs. But instead we use some of our results on the existence of large sets of prime size to show that the necessary conditions are also sufficient as long as $v > 3k$, so there are at most finitely many exceptions. In fact, we show that for infinitely many values of k the Hartman conjecture is true. It must be noticed that the methods which we use for $t = 3$ can be used in general to obtain some partial results for $t > 3$.

3.1 Overview

In this section, we discuss a possible approach to Hartman Conjecture. To do this, it will be more convenient to express the necessary conditions as a system of congruence relations. For given m and l with $m \geq l$, we denote by $a(m,l)$, the largest integer n such that 2^n divides $\binom{m}{l}$, and the smallest positive integer n such that $l < 2^n$, will be denoted by $f(l)$. It is well known that

$$a(m,l) = \sum_{i \geq 1} \left(\left[\frac{m}{2^i} \right] - \left[\frac{m-l}{2^i} \right] - \left[\frac{l}{2^i} \right] \right),$$

in which $[x]$ denotes the largest integer smaller than or equal to x. Let $B(t,k)$ denote the set of all v's such that $\binom{v-i}{k-i}$ is even for $0 \leq i \leq t$. A triple (v,k,t) is called feasible if $v \in B(t,k)$.

Lemma 3.1.1 *Let m_1, m_2, and l be three positive integers such that $m_1, m_2 \geq l$, and $m_1 \equiv m_2 \pmod{2^{f(l)}}$. Then $\binom{m_1}{l}$ is even if and only if $\binom{m_2}{l}$ is even.*

Proof. Without loss of generality, $m_1 < 2^{f(l)} + l$, and so $m_2 = m_1 + j2^{f(l)}$ for some $j \geq 0$. An easy computation shows that $a(m_1,l) \leq a(m_2,l)$. Let $a(m_2,l) > 0$, and let i be the smallest positive integer such that

$$\left[\frac{m_2}{2^i} \right] - \left[\frac{m_2 - l}{2^i} \right] - \left[\frac{l}{2^i} \right] > 0.$$

If $i > f(l)$, then

$$\left[\frac{m_2}{2^{i-1}}\right] - \left[\frac{m_2 - l}{2^{i-1}}\right] - \left[\frac{l}{2^{i-1}}\right] \geq 2\left[\frac{m_2}{2^i}\right] - 2\left[\frac{m_2 - l}{2^i}\right] - 1 > 0,$$

which is in contradiction with the minimality of i. So $i \leq f(l)$, and

$$a(m_1, l) \geq \left[\frac{m_1}{2^i}\right] - \left[\frac{m_1 - l}{2^i}\right] - \left[\frac{l}{2^i}\right] = \left[\frac{m_2}{2^i}\right] - \left[\frac{m_2 - l}{2^i}\right] - \left[\frac{l}{2^i}\right] > 0. \ \square$$

Lemma 3.1.2 *A triple (v, k, t) is feasible if and only if $(v, v-k, t)$ is feasible.*

Proof. The assertion is an immediate consequence of the following combinatorial identity

$$\binom{v-m}{k} = \sum_{i=0}^{m} (-1)^i \binom{m}{i}\binom{v-i}{k-i}$$

which can be easily proved by the Inclusion-Exclusion principal. $\square$

Lemma 3.1.3 *A triple (v, k, t) is feasible if and only if one of the followings holds:*

(i) $v \equiv t, \ldots, k-1 \pmod{2^{f(k)}}$,

(ii) $v \equiv v_0 \pmod{2^{f(k)}}$, $k < v_0 < 2^{f(k)}$, *and* $(v_0, v_0 - k, t)$ *is feasible.*

Proof. Let $v \equiv v_0 \pmod{2^{f(k)}}$, $k \leq v_0 \leq 2^{f(k)} + k - 1$. By Lemma 3.1.1, (v, k, t) is feasible if and only if (v_0, k, t) is feasible. Now $\binom{2^{f(k)}-1}{i}$ is odd for all i, so if $0 \leq j \leq t$, then $(2^{f(k)} - 1 + j, k, t)$ is not feasible. On the other hand, if $v_0 = 2^{f(k)} + i$

for some $t \leq i < k$, then for $0 \leq j \leq t$ we have

$$a(v_0 - j, k - j) \geq \left[\frac{v_0 - j}{2^{f(k)}}\right] - \left[\frac{k - j}{2^{f(k)}}\right] - \left[\frac{v_0 - k}{2^{f(k)}}\right] = 1,$$

so (v_0, k, t) is feasible. Now, the assertion follows by Lemma 3.1.2. □

Notation 3.1.1 *For the sake of convenience, throughout this chapter we write* $A(t, k)$ *instead of* $A(t, k, 2)$.

Theorem 3.1.1 *Let* t, m, *and* l *be three positive integers such that* $m \leq l$ *and* $t < 2^m - 1$. *If* $2^{f(i)} + t \in A(t, i)$ *for* $t < i < 2^m$, *and* $2^{i+1} + t \in A(t, 2^i + j)$ *for* $m \leq i < l$ *and* $0 \leq j \leq [t/2]$, *then* $A(t, k) = B(t, k)$ *for* $k < 2^{l+1}$.

Proof. By assumption $2^{f(t+1)} + t \in A(t, t + 1)$, so by Lemma 3.1.3 and Theorem 2.2.2,

$$A(t, t + 1) = B(t, t + 1) = \{v | v \equiv t \pmod{2^{f(t+1)}}\}.$$

Let $t + 1 < k < 2^{l+1}$, and assume that $A(t, i) = B(t, i)$ for $t + 1 \leq i < k$. Denote $n = f(k)$, so $2^{n-1} \leq k < 2^n$. If $k > 2^n + [t/2]$, then by the induction hypothesis $2^n + t \in A(t, 2^n + t - k)$ which implies that $2^n + t \in A(t, k)$. Therefore, $2^n + t \in \cap_{i=t+1}^{k} A(t, i)$.

Let $v \in B(t, k)$, and $v \equiv v_0 \pmod{2^n}$ with $k \leq v_0 < 2^n + k$. If $v_0 < 2^n$, then by the induction hypothesis $v_0 \in A(t, v_0 - k)$ which implies that $v_0 \in A(t, k)$. On the other hand, if $v_0 \in \{2^n + i | t \leq i < k\}$, then by Lemma 2.1.2, $v_0 \in A(t, k)$. Therefore, by Theorem 2.2.2, $v \in A(t, k)$. □

Theorem 3.1.2 *If* $2 \leq t < k \leq 7$, *then* $A(t,k) = B(t,k)$.

Proof. In [9] it is shown that $8+t \in \cap_{k=t+1}^{7} A(t,k)$. Now, applying Theorem 3.1.1 gives rise to the result. □

3.2 The Case $t = 2$

As we promised earlier, in this section we will prove that the Hartman conjecture is true for $t = 2$. A major part of the proof is to establish the existence of a $LS(1/2, 2, 2^n, 2^{n+1}+2)$ for $n \geq 4$. Since our construction for these designs is very technical, we would like to postpone it for a while. So we assume these designs exist, and we prove our main result. Then we give an outline of our construction for these designs in term of trades. And then we present a rigorous proof. The reader who is not interested in technical details, can avoid the last part and only read the outline.

Theorem 3.2.1 $A(2,k) = B(2,k)$ *for* $k \geq 3$.

Proof. For $k = 3$, the assertion is a well known result [11, 17, 22]. In [9], it is shown that $10 \in \cap_{k=3}^{7} A(2,k)$. Thus by Lemma 2.1.2, we have $\{10, \ldots, 7+k\} \subset A(2,k)$ for $k = 3, \ldots, 7$. Now, by Theorem 2.2.2, the assertion is true for $k < 8$.

In [25], it is proved that a $S(910; 4, 8, 20)$ exists. Taking the residual of this design, we conclude that a $S(4004; 2, 8, 18)$ also exists. Hence $18 \in A(2,8)$. Also in [5] it is shown that $18 \in A(2,9)$. Since, the assertion is true for $k < 8$, then a $LS(1/2; 2, k, 18)$ exists for $3 \leq k \leq 7$, taking the complement of these designs we

obtain a $LS(1/2; 2, k, 18)$ for every $10 \leq k \leq 15$. Hence $18 \in \cap_{k=3}^{15} A(2, k)$, and then by Theorem 2.2.2, we have $A(2, k) = B(2, k)$ for $k < 16$.

Let $k \geq 16$. It is well known that if k is not a power of 2, then $2k \in A(2, k)$[5] and if k is a power of two, then $2k + 2 \in A(2, k)$ by Theorem 3.2.2 (which will be proved shortly). Now, by applying Theorem 3.1.1 with $m = 4$ and $l = k$, we will have $A(2, k) = B(2, k)$. □

Existence of Auxiliary Designs: An Outline

In this section, we describe briefly an outline of the proof of $2^{l+1} + 2 \in A(2, 2^l)$ for $l > 3$. To describe our proof, it will be more convenient to reformulate our problem in terms of trades. Let T be a simple (t, k)-trade of order v (i.e., $|\text{found}(T)| = v$) such that $\text{supp}(T) = P_k(\text{found}(T))$, then $\phi_t(T^+ - T^-) = 0$ and $\phi_t(T^+ + T^-) = \binom{v-t}{k-t} P_t(\text{found}(T))$. Therefore, both T^+ and T^- are $S(\binom{v-t}{k-t}/2; t, k, v)$ designs. On the other hand, if f is a $S(\binom{v-t}{k-t}/2; t, k, v)$ design, then $2f - P_k(\text{found}(f))$ is a simple (t, k)-trade with $\text{supp}(T) = P_k(\text{found}(T))$ and $T^+ = f$. Therefore, our problem can be reformulated in the following way:

> *A* $(2, 2^l, 2^{l+1} + 2, 1/2)$*-trade, i.e. a simple* $(2, 2^l)$*-trade* T *of order* $v = 2^{l+1} + 2$ *and volume* $\binom{v}{2^l}/2$*, exists for* $l > 3$.

Therefore, we must discuss which polynomials can be support of a simple trade. Clearly, if f and g are supports of simple trades, then $f + g$ is also support of a

trade if and only if f and g have the same blocksize and they are disjoint (i.e., $f+g$ is simple).

For simplicity, let $m = k+1 = 2^l+1$ and $v = 2m$. Let $V = \{x_i | 1 \leq i \leq v\}$ and $V_1 = \{x_{2i-1} | 1 \leq i \leq m\}$. For $1 \leq i \leq m$, we define $x^*_{2i-1} = x_{2i-1}x_{2i}$. Then we can extend this, in a natural way to the subsets of V_1 and then to all regular polynomials whose foundation is a subset of V_1. For example $(x_1x_3 + x_3x_5)^* = x_1x_2x_3x_4 + x_3x_4x_5x_6$. Let $1 \leq t \leq k/2$, and let T be a minimal $(2t-1,k)$-trade with found$(T) \subset V$. Then T is said to be normalized if there exists a permutation $\sigma \in S_m$ such that (i) $\sigma(i) < \sigma(j)$ if $1 \leq i < j \leq 2t$, and (ii)

$$T = (y_1 - y_2)\dots(y_{4t-1} - y_{4t})y_{4t+1}\cdots y_{k+2t},$$

in which $y_{2i-1} = x_{2\sigma(i)-1}$ and $y_{2i} = x_{2\sigma(i)}$. Let f_t be the sum of the supports of all normalized $(2t-1,k)$-trades, and define $f_0 = \sum_{B \in P_{k/2}(V_1)} B^*$. Then

$$P_k(V) = \sum_{i=0}^{k/2} f_t.$$

Now, it is easy to check that any two normalized trades are disjoint, so each f_t is the support of a simple $(2t-1,k)$-trade, therefore if $t > 1$, then f_t is the support of a simple $(2,k)$-trade. Now, if S is a 1-trade whose support is $P_{k/2}(V_1)$, then S^* is also a 1-trade, and supp$(S^*) = f_0$. Therefore, if we can find a simple 1-trade T whose support is f_1, and $\phi_2(T) = \phi_2(S^*)$, then $T - S^*$ is a 2-trade whose support

is $f_0 + f_1$. To construct T we need a further description of normalized 1-trades and $\phi_2(S)$.

For $1 \leq i < j \leq k+1$, we define

$$T_{ij} = (x_{2i-1} - x_{2i})(x_{2j-1} - x_{2j}).$$

Then if $B \in P_{k/2-1}(V_1 \setminus \{x_{2i-1}, x_{2j-1}\})$, then $T_{ij}B^*$ is a normalized 1-trade, and in fact every normalized 1-trade is of this form. Clearly $\phi_2(T_{ij}B^*) = T_{ij}$. Therefore, if $B, C \in P_{k/2-1}(V_1 \setminus \{x_{2i-1}, x_{2j-1}\})$, then $T_{ij}B^* - T_{ij}C^*$ is a 2-trade.

Let S be a 1-trade whose support is f_0. Then we can write $S = S_0 + \sum_{l=1}^{n_S} S_l$ in which S_0 is a 2-trade and S_l is a minimal 1-trade for $l > 0$. We say S is close to a 2-trade if n_S is relatively small. Clearly, $\phi_2(S^*) = \sum_{l=1}^{n_S} S_l^*$. Let $S_l = (x_i - x_j)(x_r - x_s)B$ in which i, j, r and s are distinct and $B \in P_{k-3}(V_1 \setminus \{x_i, x_j, x_r, x_s\})$. Then

$$S_l^* = (x_{2i-1}x_{2i} - x_{2j-1}x_{2j})(x_{2r-1}x_{2r} - x_{2s-1}x_{2s})B^*,$$

and

$$\phi_2(S_l^*) = \text{supp}(T_{ir}) + \text{supp}(T_{js}) - \text{supp}(T_{is}) - \text{supp}(T_{jr}).$$

Therefore, if we find S in such a way that $n_S < \binom{k-3}{k/2-1}$, and then we can find a 1-trade T with the desired property which proves $f_0 + f_1$ (and so $P_k(V)$) is the support of a simple 2-trade.

To establish the existence of S, we basically use the same method. We partition $P_{k/2}(V_1)$ into several sets such that all of them but one are support of a 2-trade, and the last one can be the support of a 1-trade. The only part we should actually work with is this set. If we manage to take this set to be very small, then n_S will satisfy the required inequality, as we can take n_S to be smaller than or equal to $\mathrm{Vol}(S-S_0)$.

Existence of Auxiliary Designs: Technical Details

Let $X = \{1, \ldots, 2u\}$, $A_i = \{2i-1, 2i\}$ for $1 \leq i \leq u$, and let $Y = \{A_1, \ldots, A_u\}$. We define a function ϕ from the power set of Y into the power set of X by $\phi(B) = \cup_{A_i \in B} A_i$, for $B \subset Y$. The following lemma is immediate.

Lemma 3.2.1 *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are j-wise equivalent subsets of $P_m(Y)$, then $\phi(\mathcal{B}_1)$ and $\phi(\mathcal{B}_2)$ are j-wise equivalent subsets of $P_{2m}(Y)$.* □

For $B \subset X$, $T \subset Y$ and $C \subset Y \setminus T$, we define

$$Supp(B) = \{A_i | A_i \cap B \neq \emptyset\},$$

$$f(B) = \{A_i | A_i \subset B\},$$

$$g(B) = Supp(B) \setminus f(B),$$

$$\Gamma(T) = \{B \subset X | f(B) = \emptyset \ \& \ g(B) = T\},$$

$$\Gamma(T, C) = \{B \subset X | f(B) = C \ \& \ g(B) = T\},$$

$$\Gamma_m(T) = \{B \in P_m(X) | g(B) = T\}.$$

Lemma 3.2.2 *Let $T \in P_j(Y)$, $C_1, C_2 \subset Y \setminus T$, $C_1 \neq C_2$, and $|C_1| = |C_2|$. Then (i) $\Gamma(T, C_i)$ is $(j-1)$-halvable, (ii) $\Gamma(T, C_1) \cup \Gamma(T, C_2)$ is j-halvable.*

Proof. For $l \in \{0, 1\}$ define

$$\Gamma^l(T) = \{B \in \Gamma(T) | \sum_{x \in B} x \equiv l \pmod 2\}.$$

Then, it is easy to see that $\{\Gamma^0(T), \Gamma^1(T)\}$ is a partition of $\Gamma(T)$ into two $(j-1)$-equivalent subsets. Hence by Lemma 2.1.1 $\Gamma(T, C_i) = \Gamma(T) * \{\phi(C_i)\}$ is $(j-1)$-halvable. To Prove (ii), let

$$\mathcal{F}_0 = \Gamma^0(T) * \{\phi(C_1)\} \cup \Gamma^1(T) * \{\phi(C_2)\},$$
$$\mathcal{F}_1 = \Gamma^0(T) * \{\phi(C_2)\} \cup \Gamma^1(T) * \{\phi(C_1)\}.$$

Then $\{\mathcal{F}_0, \mathcal{F}_1\}$ is a partition of $\Gamma(T, C_1) \cup \Gamma(T, C_2)$ into two j-wise equivalent subsets.□

Lemma 3.2.3 *If $|T| \geq 3$, then $\Gamma_m(T)$ is 2-halvable.*

Proof. If $\Gamma_m(T) \neq \emptyset$, then $m = 2l + |T|$ for some $l \geq 0$, and so $\{\Gamma(T, C) | C \in P_l(Y \setminus T)\}$ is a partition of $\Gamma_m(T)$. Now assertion follows from Remarks 2.1.1, 2.1.3 and Lemma 3.2.2. □

Lemma 3.2.4 *Let $n \geq 2$, $v = 2^{n+2} + 1$, $k = 2^{n+1}$, and let X_1 be a v-set. Then $P_k(X_1)$ has a partition $\{\mathcal{F}_1, \mathcal{F}_2\}$ into two 1-wise equivalent subsets such that*

$$\sum_{T \in P_2(X_1)} |n(T; \mathcal{F}_1) - n(T; \mathcal{F}_2)| < \binom{v-4}{k-1}/2.$$

Proof. Let $m = 2^n$, $u = 2m = k$, and form X, Y, and A_i's. Let $\infty \notin X$ and denote $X_1 = X \cup \{\infty\}$. Clearly $\{P_k(X), \{\infty\} * P_{k-1}(X)\}$ is a partition of $P_k(X_1)$.

If $|T| = 2$, then by Lemma 2.1.1,

$$\Gamma_{2m}(T) = \Gamma(T) * \phi(P_{m-1}(Y))$$

is 2-halvable. (Note that $\binom{2m-2}{m-1}$ is even.)

If $|T|$ is even and greater than 2, then due to Lemma 3.2.3, $\Gamma_{2m}(T)$ is 2-halvable.

If $|T|$ is odd and greater than 1, then due to Lemmas 2.1.1 and 3.2.3, $\{\infty\} * \Gamma_{2m-1}(T)$ is 2-halvable.

Therefore $P_k(X_1) \setminus ((\cup_{i=1}^{u}\{\infty\} * \phi(P_{m-1}(Y \setminus \{A_i\})) \cup \phi(P_m(Y)))$ is 2-halvable.

Let $1 \leq i \leq u$. Since $2m-1$ and $m-1$ are coprime, if σ_i is any cycle of length $u-1$ on $Y \setminus \{A_i\}$, then orbits of the cyclic group generated by σ_i on $P_{m-1}(Y \setminus \{A_i\})$ are 1-designs of index $m-1$, and the total number of orbits is $\binom{2m-1}{m-1}/(2m-1)$ which is an odd integer. Therefore, we can write $P_{m-1}(Y \setminus \{A_i\}) = D_i \cup E_i$, in which $D_i \cap E_i = \emptyset$, D_i is 1-halvable, and E_i is an orbit of some block $B_i \in P_{m-1}(Y \setminus A_i)$. Without loss of generality we may assume that

$$B_j = B_{m+j} = \{A_1, \ldots, A_m\} \setminus \{A_j\}, \text{ for } j = 1, \ldots, m,$$

and $|B_i \cap \sigma_i(B_i)| = m-2$. Let

$$E_{i1} = \{\sigma^2(B_i), \sigma^4(B_i), \ldots, \sigma^{2m-2}(B_i)\},$$
$$E_{i2} = \{\sigma^1(B_i), \sigma^3(B_i), \ldots, \sigma^{2m-3}(B_i)\}.$$

Then by Lemma 2.1.1, $\{\infty\} * \phi(D_i) * P_1(A_i)$ is 2-halvable, and if we define

$$H_{il} = \{\{\infty, 2i-1\} \cup \phi(B), \{\infty, 2i\} \cup \phi(C) | B \in E_{il}, \ \& \ C \in E_{i(3-l)}\}, \quad 1 \leq l \leq 2,$$

then $\{H_{i1}, H_{i2}\}$ is a partition of $\{\infty\} * P_1(A_i) * \phi(E_i \setminus B_i)$ into two 1-wise equivalent subsets, and it is easy to check that

$$\sum_{T \in P_2(X_1)} |n(T; H_{i1}) - n(T; H_{i2})| = 4(m-1).$$

Let $Y_1 = Y \setminus \{A_1\}$, and let $\{D_{11}, D_{12}\}$ be a partition of D_1 into two 1-wise equivalent subsets. For $l \in \{1, 2\}$ define

$$F_l = \{B \cup \{A_1\}, \ Y_1 \setminus C | B \in D_{1l} \ \& \ C \in D_{1(3-l)}\}.$$

It is straightforward to check that F_1 and F_2 are 2-wise equivalent. Hence by Lemma 3.2.1, $\phi(F_1)$ and $\phi(F_2)$ are 2-wise equivalent. Let

$$F_3 = \{B \cup \{A_1\}, \ Y_1 \setminus B | B \in E_1\} = P_m(Y_1) \setminus (F_1 \cup F_2).$$

Now, we have $P_{m-1}(Y \setminus \{A_i\}) = D_i \cup Y_i \setminus \{B_i\} \cup \{b_i\}$ and $P_m(Y) = F_1 \cup F_2 \cup F_3$. Therefore, in view of the above remarks, to prove the assertion we must show that

$$\mathcal{B} = \phi(F_3) \cup (\cup_{i=1}^{2m} \{\infty\} * P_1(A_i) * \phi(B_i))$$

has a partition $\{K_1, K_2\}$ into two 1-wise equivalent subsets such that

$$\sum_{T \in P_2(X_1)} |n(T; K_1) - n(T; K_2)| < \binom{4m-3}{2m-1}/2 - 8m(m-1).$$

Now, we remark that F_3 is the union of $2m-1$ Steiner 1-designs (each consisting of a block and its complement), so $F_3 \setminus \{B_1 \cup \{A_1\}, Y_1 \setminus B_1\}$ is the union of $(2m-2)$ Steiner 1-designs, and so it has a partition $\{F_{31}, F_{32}\}$ into two 1-wise equivalent subsets each consisting of $2m-2$ blocks. Let

$$K_1 = \phi(F_{31}) \cup (\cup_{i=1}^{m} \{\infty\} * P_1(A_i) * \phi(B_i)) \cup \{\{2m+1, \ldots, 4m\}\},$$
$$K_2 = \phi(F_{32}) \cup (\cup_{i=m+1}^{2m} \{\infty\} * P_1(A_i) * \phi(B_i)) \cup \{\{1, \ldots, 2m\}\}.$$

Since $B_i = B_{m+i}$ for $i = 1, \ldots, m$, K_1 and K_2 are 1-wise equivalent. Therefore, $\{K_1, K_2\}$ is a partition of $\mathcal{B}$ into two 1-wise equivalent subsets, and it is straightforward to check that

$$\begin{aligned} \textstyle\sum_{T \in P_2(X_1)} |n(T; K_1) - n(T; K_2)| &\leq 2(2m-2)\binom{2m}{2} + 4m(2m-1) + 2\binom{2m}{2} \\ &< \binom{4m-3}{2m-1}/2 - 8m(m-1), \end{aligned}$$

(noting that $m \geq 4$) which completes the proof. □

In the remainder of this section, we assume $v = 2u = 2^{n+1} + 2$, $k = 2m = 2^n$, and $n \geq 4$. By Lemma 3.2.4, $P_m(Y)$ has a partition $\{\mathcal{F}_1, \mathcal{F}_2\}$ into 1-wise equivalent subsets such that

$$b = \sum_{T \in P_2(Y)} |n(T; \mathcal{F}_1) - n(T; \mathcal{F}_2)| < \binom{u-4}{m-1}/2.$$

We form two disjoint collections $\mathcal{H}_1$ and $\mathcal{H}_2$ of the elements of $P_2(Y)$ by the following rule: $\mathcal{H}_l$ contains $T \in P_2(Y)$ exactly m times if $n(T; \mathcal{F}_2) - n(T; \mathcal{F}_1) = (-1)^l m$. Therefore, $(\mathcal{H}_1, \mathcal{H}_2)$ is a $(1, 2, u)$-trade of volume $b/2$, and so it can be written as a sum of s minimal trades for some $s \leq b/2$. In other words, for $1 \leq i \leq s$, we can find a 4-subset $E_i = \{C_{i1}, C_{i2}, C_{i3}, C_{i4}\}$ of Y such that if we let

$$T_{i1} = \{\{C_{i1}, C_{i2}\}, \{C_{i3}, C_{i4}\}\}, \; T_{i2} = \{\{C_{i1}, C_{i3}\}, \{C_{i2}, C_{i4}\}\},$$

then for $S \in P_2(Y)$,

$$\begin{aligned} n(S; \textstyle\sum_{i=1}^{s} T_{i1}) - n(S; \textstyle\sum_{i=1}^{s} T_{i2}) &= n(S; \mathcal{H}_1) - n(S; \mathcal{H}_2) \\ &= n(S; \mathcal{F}_1) - n(S; \mathcal{F}_2). \end{aligned}$$

Therefore,

$$\sum_{i=1}^{s} (n(S; \phi(T_{i1})) - n(S; \phi(T_{i2}))) = n(S; \phi(\mathcal{F}_1)) - n(S; \phi(\mathcal{F}_2)).$$

Now, since $s < \binom{u-4}{m-1}/4$, we can find s distinct subsets $B_1, \ldots, B_s$ of $P_{m-1}(Y)$ such that $B_i \cap E_i = \emptyset$. For $1 \leq i \leq s$ and $1 \leq l \leq 2$ define $F_{il} = \cup_{S \in T_{i(3-l)}} \Gamma(T, B_i)$. The proof of the following lemma is straightforward and so it does not appear here.

Lemma 3.2.5 *F_{i1} and $F_{i2}(1 \leq i \leq s)$ are 1-wise equivalent, and for $S \in P_2(X)$,*

$$n(S; F_{i2}) - n(S; F_{i1}) = n(S; \phi(T_{i1})) - n(S; \phi(T_{i2})). \ \square$$

Let $\mathcal{B}_0 = \phi(P_m(Y)) \cup (\cup_{i=1}^{s} \cup_{l=1}^{2} \cup_{S \in T_{il}} \Gamma(S, B_i))$ and for $T \in P_2(Y)$ define

$$A_T = P_{m-1}(Y \setminus T) \setminus \{B_i | 1 \leq i \leq s \ \& \ T \in T_{i1} \cup T_{i2}\},$$
$$\mathcal{B}_T = \cup_{B \in A_T} \Gamma(T, B).$$

Clearly $\{\mathcal{B}_0, \mathcal{B}_T | T \in P_2(Y)\}$ is a partition of $\phi(P_m(Y)) \cup (\cup_{T \in P_2(Y)} \Gamma_{2m}(T))$.

Lemma 3.2.6 *$\mathcal{B}_0$ is 2-halvable.*

Proof. Let $\mathcal{G}_l = \phi(\mathcal{F}_l) \cup (\cup_{i=1}^{s} F_{il})$ for $1 \leq l \leq 2$. Then $\{\mathcal{G}_1, \mathcal{G}_2\}$ is a partition of $\mathcal{B}_0$ and by Lemma 3.2.5 for $S \in P_2(X)$ we have

$$\begin{aligned} n(S; \mathcal{G}_1) - n(S; \mathcal{G}_2) &= n(S; \phi(\mathcal{F}_1)) - n(S; \phi(\mathcal{F}_2)) + \textstyle\sum_{i=1}^{s} (n(S; F_{i1}) - n(S; F_{i2})) \\ &= \textstyle\sum_{i=1}^{s} (n(S; \phi(T_{i1})) - n(S; \phi(T_{i2}))) + \sum_{i=1}^{s} (n(S; \phi(T_{i2})) - n(S; \phi(T_{i1}))) = 0. \end{aligned}$$

Therefore, $\mathcal{G}_1$ and $\mathcal{G}_2$ are 2-wise equivalent. $\square$

Lemma 3.2.7 *For $T \in P_2(Y)$, $\mathcal{B}_T$ is 2-halvable.*

Proof. Let $A'_T = P_{m-1}(Y \setminus T) \setminus A_T$. Clearly we have

$$|A'_T| = \sum_{i=1}^{s}((n(T;T_{i1}) + n(T;T_{i2})) \equiv_2 \sum_{i=1}^{s}((n(T;T_{i1}) - n(T;T_{i2}))$$
$$\equiv_2 n(T;\mathcal{F}_1) - n(T;\mathcal{F}_2) \equiv_2 n(T;\mathcal{F}_1) + n(T;\mathcal{F}_2) = \binom{2^n-1}{2^{n-1}-1} \equiv_2 1.$$

Therefore, $|A_T|$ is even and the assertion follows from Lemma 3.2.2. □

Theorem 3.2.2 *For $n \geq 4$, an $LS(1/2; 2, 2^n, 2^{n+1}+2)$ exists.*

Proof. Clearly $\{\mathcal{B}_0, \mathcal{B}_T, \Gamma_k(S) | T \in P_2(Y),\ S \in P_{2l}(Y),\ 2 \leq l \leq 2^{n-1}\}$ is a partition of $P_k(X)$. By Lemmas 3.2.3, 3.2.6 and 3.2.7, each element of this partition is 2-halvable, and hence by Lemma 2.1.1, $P_k(X)$ is 2-halvable. □

3.3 The Case $t = 3$

In this section, we restrict ourselves to the case $t = 3$. Our main goal is to prove that if $v \in B(3,k)$ and $v > 3k$, then $v \in A(3,k)$, and $A(3,k) = B(3,k)$ for infinitely many k.

Theorem 3.3.1 *$A(3,k) = B(3,k)$ for $k \leq 15$.*

Proof. In [9] it is shown that $11 \in \cap_{k=4}^{7} A(3,k)$ and $19 \in \cap_{k=8}^{15} A(3,k)$. Now, the assertion is an immediate consequence of Theorem 3.1.1. □

Notation 3.3.1 *For $k > 3$ we define $C(k) = \{2^{f(k)} + i | 3 \leq i < 3.2^{f(k)-4}\}$.*

Theorem 3.3.2 *Let $k > 8$, $n = f(k)$. Then*

(i) $B(3,k) \setminus A(3,k) \subset C(k)$,

(ii) $A(3,k) = B(3,k)$ *if* $2^{n-1} + 3.2^{n-4} < k < 2^n$.

Proof. We prove the assertion by induction on n. By Theorem 3.3.1 the assertion is true for $n \leq 4$. In the next section, through a series of Lemmas we prove that if $n \geq 5$, and the assertion is true for $n-1$, then it is also true for n which completes the proof. □

The Induction Step

In the rest of this section, we assume $n \geq 5$, $f(k) = n$, and Theorem 3.3.2 is true for $n-1$. For simplicity of the notation, we let $r = 3.2^{n-4}$.

Lemma 3.3.1 *If* $u \in A(3,k_0)$, *then* $\{2u, 2u+1\} \subset A(3,2k_0) \cap A(3,2k_0+1)$.

Proof. By Theorem 2.3.1, $2u \in A(3,2k_0)$. Also by Lemma 1.1.1, we have $u-1 \in A(2,k_0)$, so by Theorem 2.3.2, $2u \in A(3,2k_0+1)$. By Theorem 2.3.2, $2u+2 \in A(4,2k_0+1)$. Now, by Lemma 1.1.1, we have $2u+1 \in A(3,2k_0) \cap A(3,2k_0+1)$. □

Corollary 3.3.1 $\{2^n + i | r \leq i < k\} \subset A(3,k)$.

Proof. Let $k_0 = [k/2]$. By Lemma 3.3.1, $\{2^n + i | r \leq i < 2k_0 - 1\} \subset A(3,2k_0) \cap A(3,2k_0+1)$. If $k = 2k_0 + 1$, then $2^n + 2k_0 - 1 \in A(3,2k_0) \cap A(3,2k_0+1)$, so by Lemma 2.1.2, $2^n + 2k_0 \in \cap A(3,2k_0+1)$. □

Lemma 3.3.2 *If* $u \in A(3,k)$, *then* $\{v | v \equiv u \pmod{2^n} \ \& \ v > u\} \subset A(3,k)$.

Proof. Let $v_1 = 2^n + r$, $v_2 = u$, $s = r$ and $a = k - 1 - s$. Then, by the induction hypothesis $v_1 \in \cap_{i=s+1}^{k} A(3,i)$ and $v_1 - l \in A(3, s+1-l)$ for $1 \leq l \leq s-3$ (notice that $f(s+1-l) \leq f(s) = n-2$). By Theorem 2.2.1 with $b = d = 0$, we will have $u + 2^n \in A(3,k)$. Now, the assertion follows by induction. □

Lemma 3.3.3 *If* $k > 2^{n-1} + r$, *then* $C(k) \subset A(3,k)$.

Proof. Let $3 \leq i < r$ and $v = 2^n + i$. Let $m = f(v-k)$. Then $m \leq f(r) = n-2$ which implies $v > 2^m + 3.2^{m-4}$. On the other hand $v \equiv i \pmod{2^{f(v-k)}}$ and $3 \leq i < v-k$, so $(v, v-k, t)$ is feasible. Therefore, $v \in A(3, v-k)$ and consequently $v \in A(3,k)$. □

Lemma 3.3.4 *If* $k > 2^{n-1} + r$, *then* $2^{n+1} + i \in A(3,k)$ *for* $3 \leq i < r$.

Proof. The assertion is an immediate consequence of Lemmas 3.3.2 and 3.3.3. □

Lemma 3.3.5 *If* $k < 2^{n-1} + 2^{n-3} + 3$, *then* $\{2^{n+1} + i | 3 \leq i < r\} \subset A(3,k)$.

Proof. Let $i \in \{3, \ldots, r-1\}$, $t = 3$, $v_1 = 2^n + r$, $v_2 = 2^n + r + i$, $a = k - 2^{n-1}$, $b = 2^{n-3} + 2$, $c = d = r - 3$ and $s = k - 1 - a - b = c + d + t = 2r - 3$.

For $2^{n-1} = k - a \leq j \leq k$, we have $r < j$, so $(v_1, j, 3)$ is feasible. Clearly, $f(j) \leq f(k) = n$, so $v_1 \notin C(j)$ which implies $v_1 \in A(3,j)$. A similar argument shows that $v_2 \in \cap_{j=k-b}^{k} A(3,j)$.

Let $1 \leq l \leq c$. Then $k-a-l < 2^{n-1}-l$, so $f(k-a-l) < n$. Now, we have $v_1 - l \equiv r - l \pmod{2^{f(k-a-l)}}$ and $r - l < 2^{n-1} - l = k - a - l$. Clearly, $v_1 - l > 2^{f(k-a-l)+1}$, so $v_1 - l \notin C(k-a-l)$ which implies $v_1 - l \in A(3, k-a-l)$.

A similar argument shows that $v_2 - l \in A(3, k-b-l)$ for $1 \leq l \leq c$.

Now, the assertion follows by Theorem 2.2.1. □

Lemma 3.3.6 $\{2^{n+1}+i | 3 \leq i \leq r\} \subset A(3,k)$.

Proof. If either $k \leq 2^{n-1}+2^{n-3}+2$ or $2^{n-1}+r \leq k$, then the assertion is proved in Lemmas 3.3.4 and 3.3.5.

Let $2^{n-1}+2^{n-3}+2 < k < 2^{n-1}+r$, and $1 \leq i \leq 2^{n-3}$. Clearly, we have $i < 2^n + i - k$, and $2^n + i - k < 2^{n-1}$ which implies $(2^n+i, 2^n+i-k, 3)$ is feasible, and $2^n + i \notin C(2^n+i-k)$. Therefore, $2^n + i \in A(3, 2^n+i-k)$ which implies $2^n + i \in A(3,k)$. Now, by Lemma 3.3.2,

$$\{2^{n+1}+i | 3 \leq i \leq 2^{n-3}\} \subset A(3,k).$$

By Lemma 3.3.5, we have

$$2^{n+1}+3 \in \bigcap_{j=2^{n-1}}^{2^{n-1}+2^{n-3}} A(3,j),$$

and then by Lemma 2.1.2, we have

$$\{2^{n+1}+i | 2^{n-3}+3 < i \leq r\} \subset A(3,k),$$

which completes the proof. □

Corollary 3.3.2 *If* $v \equiv 3, \ldots k-1 \pmod{2^n}$ *and* $v \notin C(k)$, *then* $v \in A(3,k)$.

Proof. The assertion follows by Corollary 3.3.1 and Lemmas 3.3.2 and 3.3.6. □

Lemma 3.3.7 *If* $v \in B(3,k) \setminus C(k)$, *then* $v \in A(3,k)$.

Proof. In view of Lemmas 3.1.3, 3.3.2 and Corollary 3.3.2 we only need to consider the case $v < 2^n$. But in this case $(v, v-k, 3)$ is also feasible, and clearly $v-k < 2^{n-1}$, so $m = f(v-k) < n$. If $v \in C(v-k)$, then $m = n-1$, and $v-k \geq 2^{n-2}$ which implies $v \geq k + 2^{n-2} > 2^m + 3.2^{m-4}$- a contradiction. So $v \notin C(v-k)$. Then $v \in A(3, v-k)$ and consequently $v \in A(3,k)$. □

Chapter 4 The Case $k = t + 1$

4.1 Teirlinck's Construction

As we discussed in Chapter 1, $S(\lambda; t, k, v)$ designs are equivalent to the nonnegative integer solutions of the following nonhomogeneous system of linear equations

$$\phi_{tk}(v)F = \lambda \mathbf{1}, \tag{4.1}$$

in which $\mathbf{1}$ is the all one vector, and $\phi_{tk}(v)$ is the incidence matrix of t-subsets and k-subsets of a v-set X, in which incidence is defined by inclusion. Unfortunately, the size of $\phi_{tk}(v)$ grows very rapidly, which makes it impossible to check all different possibilities for solutions of this system. Therefore, one may try to find a way to shrink this matrix. One possible way to do so, is to define an equivalence relationship on the subsets of X which preserves the size of a subset (i.e. all members of an equivalence class have the same cardinality), and is consistent with the inclusion. More precisely, if $\mathcal{T} = \overline{T}$ and $\mathcal{K}$ are two equivalence classes of t-subsets and k-subsets, respectively, then $n(T; \mathcal{K})$ (the number of blocks in $\mathcal{K}$ which contain T) only depends on the equivalence class $\mathcal{T}$ (not the particular representative). Then, we can define a matrix $\bar{\phi}_{tk}(v)$ whose rows and columns are indexed by the equivalence classes of t-subsets and k-subsets, respectively, and the entry at row $\mathcal{T}$ and column

$\mathcal{K}$ is $n(T; \mathcal{K})$ in which T is any representative of $\mathcal{T}$. Now, a solution of

$$\tilde{\phi}_{tk}(v)g = \lambda \mathbf{1} \tag{4.2}$$

is equivalent to a $S(\lambda; t, k, v)$ whose block set is a union of equivalence classes. One common way to find such an equivalence relationship is the group action. If G is a finite group which acts on X, then this action can be naturally extended to the $P(X)$, and then two subsets of X are equivalent if and only if they are in the same orbit. Any solution of 4.2 will provide a $S(\lambda; t, k, v)$ design with G as an automorphism group. This idea has been successfully used by many different authors to produce t-designs with a given automorphism group. Notice that this method can reduce the size of the original system of equations at most by a factor of $|G|$, and for a given group G there is no guarantee that a $S(\lambda; t, k, v)$ design with G as an automorphism group exists(In fact, there are many t-designs with trivial automorphism group.), and so for large values of v this method is not practical. Therefore, it comes necessary to find another equivalence relationship which enables us to approach the existence problem recursively. For this, we need to take an extra look at the necessary conditions. In the rest of this chapter, we restrict ourselves to the case $k = t + 1$. Then, the necessary conditions can be rewritten in the form

$$\lambda(t, t+1, v) = \gcd\left(\text{l.c.m.}\{1, \ldots, t+1\}, v - t\right) \mid \lambda.$$

Therefore, to make sure that at any step of our constructions the necessary conditions are satisfied, we may take $v = t + uw$, in which l.c.m$\{1, \ldots, t+1\}$ divides u and w is a nonnegative integer. Then, a natural candidate for a v-set would be

$$X = \{\infty_1, \ldots, \infty_t\} \cup I_u \times I_w.$$

These representations of X and v immediately suggest that t elements of X, namely ∞_i's, must be treated differently from the others. For $1 \leq i \leq u$, let $Y_i = \{i\} \times I_w$, and let $Y = \{Y_1 \ldots, Y_u\}$. Now, for a subset B of X we may define

$$\mathit{Supp}(B) = \{Y_i \mid Y_i \cap B \neq \emptyset\}.$$

Then two subsets B and C of X are said to be equivalent if and only if (i) they have the same cardinality, and (ii) $\mathit{Supp}(B) = \mathit{Supp}(C)$. We show that this equivalence relationship is consistent with the inclusion. Let $T \in P_t(X)$, $B \in P_{t+1}(X)$, $T \subset B$, and $w > t + 1$. We denote by $\mathcal{B}$ the equivalence class of B. Now, either $\mathit{Supp}(B) = \mathit{supp}(T)$ or $|\mathit{Supp}(B) \setminus \mathit{supp}(T)| = 1$. In the first case, we have

$$n(T; \mathcal{B}) = w|\mathit{Supp}(B)|,$$

while in the second case

$$n(T; \mathcal{B}) = w(|\mathit{Supp}(B)| + 1).$$

Therefore, our equivalence relationship is consistent with the inclusion of t-subsets in $(t+1)$-subsets, and we may define $\tilde{\phi}_{tk}(v)$. Since for this equivalence relationship each entry of $\tilde{P}_{tk}(v)$ is divisible by w, we replace it by

$$M_t(u) = \frac{1}{w}\tilde{P}_{tk}(v),$$

and then solutions of

$$M_t(u)g = \lambda \mathbf{1} \tag{4.3}$$

are equivalent to the $S(\lambda w; t, t+1, uw+t)$ designs whose block set can be partitioned into equivalence classes.

Before we proceed any further, we would like to take a further look at the $M_t(u)$ and equation 4.3, so we can describe them from an abstract point of view. Let B be a m-subset of X, then $\max\{0, m-t\} \leq |Supp(B)| \leq m$. Therefore, equivalence classes of t-subsets and $(t+1)$-subsets can be identified with $P_{0,t}(Y)$ and $P_{1,t+1}(Y)$, respectively. Then, for $T \in P_{0,t}(Y)$, $B \in P_{1,t+1}(Y)$, we have

$$M_t(u)(T,B) = \begin{cases} |T| & \text{if } T = B, \\ 1 & \text{if } T \subset B \ \& \ |B \setminus T| = 1, \\ 0 & \text{otherwise.} \end{cases}$$

If g is a rational solution of 4.3, then for $S \in P_{0,t}(Y)$ we have

$$|S|g(S) + \sum_{x \in Y \setminus S} g(S \cup \{x\}) = \sum_{x \in Y} g(S \cup \{x\} = \lambda.$$

Let $Z = \{\infty_1, \ldots, \infty_t\}$ and $V = Y \cup Z$. If $g(S)$ is a nonnegative integer for all $S \in P_{0,t}(Y)$, then we can define a collection f of $(t+1)$-subsets of V by

$$f(B) = g(B \setminus Z).$$

It is easy to see that f is actually a $S(\lambda; t, t+1, u+t)$ design which has the symmetric group on Z as an automorphism group. Conversely, any design with this property is equivalent to a solution of system 4.3. Such designs are very important for our discussion, so we would like to give them a name.

Definition 4.1.1 *Let $D = (X, \mathcal{B})$ be a $S(\lambda; t, k, v)$ and $Z \subset X$. D is called Z-trivial if it has the symmetric group on Z as an automorphism group. D is called r-trivial if it is Z-trivial for some $Z \in P_r(X)$. Similarly, a $LS(\lambda; t, k, v)$, say $\mathcal{F} = \{D_i = (X, \mathcal{B}_i) | 1 \leq i \leq n\}$, is called Z-trivial if each D_i is Z-trivial, and it is called r-trivial if it is Z-trivial for some $Z \in P_r(X)$.*

At this moment, it may look like that we have reduced the problem of the existence of t-designs to the more difficult problem of the existence of t-designs with a prescribed automorphism group. We will see shortly that this is not the case, but even if we can't go any further, we have found the following recursive construction.

Theorem 4.1.1 *If a t-trivial (large set of) $S(\lambda; t, t+1, u+t)$ exists, then a (large set of) $S(w\lambda; t, t+1, uw+t)$ exists for all $w \geq 1$.* □

In the rest of this section we deal with the rational solutions of 4.3. Therefore, it comes necessary to describe such solutions in term of designs. Let $g_1, \ldots, g_m$ be nonnegative rational solutions of 4.3 such that $\sum_{i=1}^{n} g_i = 1$. Then we can choose a such that ag_i is an integer vector for all i. Then $ag_1, \ldots, ag_n$ are integer vectors and

$$M_t(U).(ag_i) = a\lambda\mathbf{1}.$$

We define n collections $\mathcal{B}_1, \ldots, \mathcal{B}_n$ of elements of $P_{t+1}(X)$ as follows: $\mathcal{B}_i$ include the equivalence class of a block B exactly $ag_i(Supp(B))$ times. Then, each $\mathcal{B}_i$ is a $S(a\lambda; t, t+1, v)$ design and $\sum_{i=1}^{n} \mathcal{B}_i = aP_{t+1}(X)$.

Definition 4.1.2 *A λ-factorization of $mTS(t, t+1, v)$ on a v-set X, which is denoted by $FS(\lambda, t, m, v)$, is a collection $\mathcal{F} = \{D_i = (X, \mathcal{B}_i) | 1 \leq i \leq n = m(v-t)/\lambda\}$ such that $\sum_{i=1}^{n} \mathcal{B}_i = mP_{t+1}(X)$ and each D_i is a $S(\lambda, t, t+1, v)$. If $Z \subset X$, we call $\mathcal{F}$ Z-trivial if D_i is Z-trivial for all i. $\mathcal{F}$ is called r-trivial if it is Z-trivial for some $Z \in P_r(X)$.*

Let $S \in P_{1,t+1}(X)$. We can find an integer a_S such that $a_S g_i(S)$ is an integer for all i. Let

$$\overline{S} = \{B \in P_{t+1}(X) \mid Supp(B) = S\}.$$

Suppose $\overline{S}$ has a partition $\mathcal{P}_S$ into a_S t-wise equivalent subsets. Since $\sum_{i=1}^{n} a_S g_i(S) =$

a_S, we can partition $\overline{S}$ into n parts(some of them may be empty), say $\overline{S}_1, \ldots, \overline{S}_n$, such that $\overline{S}_i$ is union of $a_S g_i(S)$ parts of $\mathcal{P}$. Then, for $T \in P_{t+1}(X)$, we have

$$n(T; \overline{S}_i) = g_i(S) n(T; \overline{S}).$$

Therefore, in the definition of the $\mathcal{B}_i$'s we can replace $a g_i(S) \overline{S}$ with $a\overline{S}_i$. If we do this for all $S \in P_{1,t+1}(Y)$, then the $\mathcal{B}_i$'s will be a-uniform and disjoint. And we still have $\sum_{i=1}^{n} \mathcal{B}_i = a P_{t+1}(X)$. Therefore, if we ignore all multiplicities, we obtain a $LS(\lambda w; t, t+1, uw+t)$, namely $\mathcal{F} = \{\frac{1}{a}\mathcal{B}_i | 1 \leq i \leq n\}$. In particular, if $\mathcal{P}_S$ is Z-trivial for all S, then all $\mathcal{B}_i$'s and consequently $\mathcal{F}$ are also Z-trivial. We state this result as a theorem.

Theorem 4.1.2 *Let $\{g_1, \ldots, g_n\}$ be a t-trivial $FS(\lambda; t, a, u+t)$. Assume, for $S \in P_{1,t+1}(Y)$, there exists an integer b_S such that b_S divides $g_i(S)$ for all i, and the equivalence class $\overline{S}$ has a (t-trivial) partition into $a_S = a/b_S$ t-wise equivalent subsets. Then a (t-trivial) $LS(a\lambda; t, t+1, au+t)$ exists.* □

Remark 4.1.1 *Let S, $S' \in P_{1,t+1}(X)$ and $|S| = |S'|$. Then, $\overline{S}$ has a (Z-trivial) partition into l mutually t-wise equivalent subsets if and only if $\overline{S'}$ has a (Z-trivial) partition into l mutually t-wise equivalent subsets.*

Now, it is time to take another look at the equivalence classes, so we can find w such that a given equivalence class has a (t-trivial) partition into l mutually t-wise equivalent subsets. Let $B \in P_{t+1}(X)$, $C = Supp(B) \in P_{1,t+1}(Y)$, and let $\mathcal{C}$ be the

equivalence class of B. Then

$$\mathcal{C} = \{D \in P_{t+1}(X) \mid Supp(D) = Supp(B) = C\}.$$

If $C = \{Y_i\}$, then $\mathcal{C} = P_{t+1}(Y_i \cup Z_1)$. Hence, $\mathcal{C}$ is (l, t)-partitionable if and only if a $LS(w/l; t, t+1, w+t)$ exists.

Lemma 4.1.1 *Let* $|C| = m > 1$, *and let*

$$\mathcal{P} = \{(x_1, \ldots, x_m) | x_1 + \ldots + x_m = t + 1 - m \ \ \& \ \ x_i \geq 0\}.$$

Then $\mathcal{C}$ *has a partition* $\{\Gamma_S | S \in \mathcal{P}\}$ *in which* $\Gamma_{(x_1,\ldots,x_m)}$ *is of form* $\Pi_{i=1}^{m} \binom{u+x_i}{x_i+1}$.

Proof. Let $(x_1 \ldots, x_m) \in \mathcal{P}$, and define

$$E_i = \{\infty_j | \sum_{l=1}^{i-1}(x_l + 1) \leq j < \sum_{l=1}^{i}(x_l + 1)\},$$

$$\Gamma_{(x_1,\ldots,x_m)} = \Pi_{l=1}^{m} P_{x_i+1}(Y_i \cup E_i).$$

Clearly, $\Gamma_{(x_1,\ldots,x_m)}$ is of the desired form.

Let $S_1 = (x_1, \ldots, x_m)$ and $S_2 = (y_1, \ldots, y_m)$ be two distinct elements of $\mathcal{P}$. Then, we can find j such that $x_i = y_i$ for $i < j$, and $x_j \neq y_j$. Without loss of generality,

we may assume $x_j < y_j$. Let

$$p = \sum_{i=1}^{j}(x_i + 1) - 1,$$

$$q = \sum_{i=1}^{j}(y_i + 1) - 1,$$

$$V_1 = (\cup_{i=1}^{j} Y_i) \cup \{\infty_l | 1 \leq l \leq p\},$$

$$V_2 = (\cup_{i=1}^{j} Y_i) \cup \{\infty_l | 1 \leq l \leq q\}.$$

If $D \in \Gamma_{S_1}$, then $|D \cap V_1| = p+1$ and $\infty_{p+1} \notin D$, so $|D \cap V_2| < p+1+y_j-x_j = q+1$, while for $E \in \Gamma_{S_2}$, we have $|E \cap V_2| = q + 1$. Therefore Γ_{S_1} and Γ_{S_2} are disjoint.

Let $E \in C$ and $1 \leq i \leq m$, then there exists a unique $1 \leq j = f(i) \leq t$ such that

$$|E \cap \left[\{\infty_l | l < j\} \cup (\cup_{l=1}^{i} Y_l)\right]| = j \ \ \& \ \ \infty_j \notin E.$$

Let $f(0) = 0$, and $x_i = f(i)-f(i-1)-1$, then $\sum_{i=1}^{m} x_i = t+2-m$, and $E \in \Gamma_{(x_1,\ldots,x_m)}$ which completes the proof. □

Example 4.1.1 *Let $t = 4$ and $C = \{Y_1, Y_2, Y_3\}$. Then we have*

$$\Gamma_{(2,0,0)} = P_3(Y_1 \cup \{\infty_1, \infty_2\}) * P_1(Y_2) * P_1(Y_3),$$

$$\Gamma_{(0,2,0)} = P_1(Y_1) * P_3(Y_2 \cup \{\infty_2, \infty_3\}) * P_1(Y_3),$$

$$\Gamma_{(0,0,2)} = P_1(Y_1) * P_1(Y_2) * P_3(Y_3 \cup \{\infty_3, \infty_4\}),$$

$$\Gamma_{(1,1,0)} = P_2(Y_1 \cup \{\infty_1\}) * P_2(Y_2 \cup \{\infty_3\}) * P_1(Y_3),$$

$$\Gamma_{(1,0,1)} = P_2(Y_1 \cup \{\infty_1\}) * P_1(Y_2) * P_2(Y_3 \cup \{\infty_4\}),$$

$$\Gamma_{(0,1,1)} = P_1(Y_1) * P_2(Y_2 \cup \{\infty_2\}) * P_2(Y_3 \cup \{\infty_4\}).$$

Lemma 4.1.2 *Let $|C| = m$. If a $LS(w/l; t+1-m, t+2-m, w+t+1-m)$ exists, then C is (l,t)-partitionable.*

Proof. The assertion follows by Lemmas 2.1.1 and 4.1.1 (notice that by Lemma 1.1.1, a $LS(w/l; i, i+1, w+i)$ exists for $1 \leq i \leq t+1-m$). □

Corollary 4.1.1 *If a $LS(w/l; t, t+1, w+t)$ exists, then all equivalence classes are (l,t)-partitionable.* □

Theorem 4.1.3 *If a $LS(w/n; t, t+1, w+t)$ exists, then a $LS(uw/n; t, t+1, uw+t)$ exists for all $u \geq 1$.*

Proof. Let $g_i(S) = 1/n$ for $S \in P_{1,t+1}(Y)$ and $1 \leq i \leq n$. Then $M_t(u)g_i = u/n$ for $1 \leq i \leq n$ and $\sum_{i=1}^{n} g_i = 1$. Now, the assertion follows by Corollary 4.1.1 and Theorem 4.1.2. □

Lemma 4.1.3 *Let $|C| = m$. If a $(t+1-m)$-trivial $LS(w/l; t+1-m, t+2-m, w+t+1-m)$ exists, then C has a Z-trivial partition into l mutually t-wise equivalent subsets.*

Proof. Without loss of generality, we may take $C = \{Y_1, \ldots, Y_m\}$. By assumption for $1 \leq i \leq m$ $P_{1,t+2-m}(Y_i)$ has a partition $\{g_{i1}, \ldots, g_{il}\}$ such that for $A \in P_{0,t+1-m}(Y)$, we have

$$|A| g_{ij}(A) + \sum_{x \in Y_i \setminus A} g_{ij}(A \cup \{x\}) = w/l, \text{ for } 1 \leq j \leq n.$$

Let $B \in \mathcal{C}$. Then $B_i = B \cap Y_i \in P_{1,t+2-m}(Y_i)$ for $i \leq m$. We form a partition $\{\mathcal{C}_1, \ldots, \mathcal{C}_l\}$ of $\mathcal{C}$ as follows:

Given $B \in \mathcal{C}$, B is included in $\mathcal{C}_p$ if and only if there exist $x_1, \ldots, x_m \in I_l$ such that $g_{ix_i}(B) \neq 0$ and $\sum_{i=1}^{l} x_i = p$ in I_l. Clearly, $\mathcal{C}_p$'s form a Z-trivial partition of $\mathcal{C}$. We show that $\mathcal{C}_p$'s are t-wise equivalent. Let $T \in P_t(X)$, $n(T;\mathcal{C}) \neq 0$, and let $T_i = T \cap Y_i$. If $T_i \neq \emptyset$, we choose y_i such that $T_i \in g_{iy_i}$. We consider two different cases:

Case (i): $Supp(T) = C$, i.e. all T_i's are nonempty. Let $r = \sum_{i=1}^{m} y_i$. Now,

$$n(T;\mathcal{C}_p) = \sum_{i=1}^{m} \sum_{x \in Y_i} g_{i(p-r+y_i)}(T \cup \{x\}) = \sum_{j=1}^{m} w/l = mw/l = n(T;\mathcal{C})/l.$$

Case (ii): $Supp(T) = C \setminus \{Y_j\}$, for some $1 \leq j \leq m$. Let $r = \sum_{i \neq j} y_i$. Then

$$n(T;\mathcal{C}_p) = \sum_{x \in Y_j} g_{j(p-r+y_j)}(\{x\}) = w/l = n(T;\mathcal{C})/l. \ \square$$

Theorem 4.1.2 and Lemma 4.1.3 provide a recursive method to construct large sets of t-designs. Clearly, in this recursive construction we need a large set of t-designs only if there is $S \in P_1(Y)$ such that $a_S \neq 1$. Let $a_i = \text{l.c.m}\{a_S | S \in P_i(X)\}$ for $1 \leq i \leq t+1$. Then we need a large set of $(t+1-i)$-designs only if $a_i \neq 1$. Therefore, λ-factorizations with this property that $a_t = 1$ are of particular interest.

Definition 4.1.3 *Let $\mathcal{G} = \{g_1, \ldots, g_n\}$ be a D-trivial $FS(\lambda, t, m, v)$ with $|D| \geq t$. $\mathcal{G}$ is called r-regular if every block which intersects D in more than r points appears in exactly one of $\mathcal{B}_j$'s (with multiplicity m).*

Theorem 4.1.4 *Let t, λ and u be positive integers such that l.c.m.$\{1, \ldots, t+1\} | \lambda | u$, and let $a = $ l.c.m.$\{\binom{t}{i} | i = 0, \ldots, t\}$. Then a $(t-1)$-regular t-trivial $FS(a\lambda, t, a, u+t)$ exists.*

Proof. Let $1 \leq l \leq t+1$ and $C = \{x_1, \ldots, x_l\} \in P_l(I_u)$. For $1 \leq j \leq u/\lambda$, we denote by $g_i(C)$ the number of solutions of the following system of equations:

$$\begin{cases} \sum_{j=1}^{l} a_j = t+1, \ a_j\text{'s are positive integers,} \\ \sum_{j=1}^{l} a_j x_j \in \{(i-1)\lambda + 1, \ldots, i\lambda\} \text{ in } I_u. \end{cases}$$

Let $f_i(S) = ag_i(S)/\binom{t}{|S|-1}$ for $1 \leq i \leq u/\lambda$. We claim that f_i's form a $FS(a\lambda, t, a, u+t)$.

Let $0 \leq l \leq t$ and $S = \{x_1, \ldots, x_l\} \in P_l(I_u)$. Given nonnegative integers $a_1, \ldots, a_l$ such that $\sum_{j=1}^{l} a_j < t+1$, the equation

$$\sum_{j=1}^{l} a_j x_j + (t+1 - \sum_{j=1}^{l} a_j)x \in \{(i-1)\lambda + 1, \ldots, i\lambda\} \text{ in } I_u$$

has exactly λ solutions $x \in I_u$. We need to know how many of these solutions are

in S. Let x be a solution. Then $x = x_m \in S$ if and only if

$$\sum_{j=1}^{l} b_j x_j \in \{(i-1)\lambda + 1, \ldots, i\lambda\} \text{ in } I_u \tag{4.4}$$

in which $b_j = a_j$ for $j \neq m$ and $b_m = a_m + a_{l+1}$. There are exactly $g_i(S)$ solution for 4.4 and for each of them we can form a_i's in exactly $(t + 1 - l)$ different ways. Therefore

$$\sum_{x \notin S} g_i(S \cup \{x\}) + (t + 1 - l)g_i(S) = \lambda \binom{t}{l},$$

and consequently

$$\begin{aligned} |S| f_i(S) + \textstyle\sum_{x \notin S} f_i(S \cup \{x\} &= al g_i(S) / \binom{t}{l-1} + a \textstyle\sum_{x \notin S} g_i(S \cup \{x\} / \binom{t}{l} \\ &= a(g_i(S \cup \{x\}) + (t + 1 - l)g_i(S)) / \binom{t}{l} = a\lambda. \ \square \end{aligned}$$

Theorem 4.1.5 *Let $\lambda(0) = 1$ and define $\lambda(i)$'s, $1 \leq i$, recursively by*

$$\lambda(t) = l.c.m.\{1, \ldots, t + 1\} l.c.m.\{\binom{t}{j} | 1 \leq j \leq t\} \lambda(t - 1).$$

Then the necessary conditions for the existence of a $LS(\lambda; t, t+1, v)$ are also sufficient whenever $\lambda(t)$ divides λ.

Proof. The assertion follows by induction on t and applying Lemma 4.1.1 and Theorems 4.1.2 and 4.1.4. $\square$

4.2 $(t+1)$-Trivial t-Designs

In this section, we follow Teirlinck's approach to find some new large sets of t-designs (for all t), some of which have order smaller than those which were constructed in Theorem 4.1.5. The main idea is to work with $(t+1)$-trivial large sets of t-designs which enables us to replace $(t-1)$-regularity (in Teirlinck's construction) by a much stronger condition of 1-regularity.

Remark 4.2.1 *Let $\mathcal{D} = \{D_i = (X, \mathcal{B}_i) | 1 \leq i \leq n\}$ be a Z-trivial $LS(\lambda, t, t+1, v)$ with $Z \in P_{t+1}(X)$. Let $X_1 = X \setminus Y$. For $1 \leq i \leq n$, we can define a collection g_i of elements of $P_{0,t+1}(X_1)$ as follows: g_i contain $C \in P_{0,t+1}(X_1)$ if and only if there is $B \in \mathcal{B}_i$ such that $B \setminus Z = C$. Since D_i's are Z-trivial, g_i's are well defined and then it is easy to see that $\sum_{i=1}^{n} g_i = \mathbf{1}$, and for $S \in P_{0,t+1}(X_1)$, we have*

$$(|S| + 1)g_i(S) + \sum_{x \in X_1 \setminus S} g_i(S \cup \{x\}) = \lambda. \tag{4.5}$$

Let $v = uw + t$, $Z_1 = \{\infty_1, \ldots, \infty_t\}$, $X = I_u \times I_w \cup Z_1$, $I_u^* = I_u \setminus \{0\}$, $\infty_0 = (0,0) \in X$, $Z = Z_1 \cup \{\infty_0\}$ and $X_1 = X \setminus Z$. For $B \in P_{t+1}(X)$ we define

$$\mathrm{supp}(B) = \{i \in I_u^* | (\{i\} \times I_w) \cap B \neq \emptyset\},$$

so $\mathrm{supp}(B) \in P_{0,t+1}(I_u^*)$. Two subsets of X are called equivalent if they are of the same cardinality and they have the same support. For $C \in P_{0,t+1}(I_u^*)$ we define

$\Gamma(C) = \{B \in P_{t+1}(X) | \text{supp}(B) = C\}$, so $\Gamma(C)$ is the equivalence class of B. It is easy to see that if $\bar{\phi}_{t(t+1)}(v)$ is the t-set inclusion matrix $\phi_{t(t+1)}(v)$ modulo this equivalence relationship and $N_t(v-t-1) = \frac{1}{w}\bar{\phi}_{t(t+1)}(v)$, then g is a solution of

$$N_t(v-t-1)g = \lambda \mathbf{1} \tag{4.6}$$

if and only if g satisfies 4.5. Then, utilizing a similar argument one can prove the following analogue of Theorem 4.1.2.

Theorem 4.2.1 *Let $\{g_1, \ldots, g_n\}$ be a $(t+1)$-trivial $FS(\lambda; t, a, u+t)$. Assume, for $S \in P_{0,t+1}(Y)$, there exists an integer b_S such that b_S divides $g_i(S)$ for all i, and the equivalence class $\Gamma(S)$ has a ($(t+1)$-trivial) partition into $a_S = a/b_S$ t-wise equivalent subsets. Then a ($(t+1)$-trivial) $LS(a\lambda; t, t+1, au+t)$ exists.* □

Remark 4.2.2 *Notice that the equivalence relationships defined here and in the last section are different, so Lemma 4.1.2 does not provide a partition of $\Gamma(C)$ into t-wise equivalent subsets.*

Lemma 4.2.1 *If $|C| = t$, then $\Gamma(C)$ has a Z-trivial partition $\{\Gamma_i(C) | 1 \leq i \leq w/\delta\}$ into t-wise equivalent subsets in which $\delta = 2$ if w is even and $\delta = 1$ otherwise.*

Proof. Let $C = \{x_1, \ldots, x_t\}$. Let $\{F_l | l \in \delta I_w\}$ be a δ-factorization of K_{w+1} on $I_w \cup \{\infty\}$ such that $\{\{\infty, l+i\} | i = 0, \ldots, \delta - 1\} \in F_l$ for $l \in \delta I_w$. Now, for $l \in \delta I_w$ let $\Gamma_l(C)$ be the set of all blocks of form $\{(x_1, y_1), \ldots, (x_t, y_t), z\}$ such that y_j's are in I_w, and one of the followings holds (i) $z = \infty_i$, and $\sum_{i=1}^{t} y_i \in \{l, l+\delta-1\}$, (ii)

$z = (x_i, t_i)$ and $\sum_{j \neq i} y_j + m \in \{l, l+\delta-1\}$ in which $m \in \delta I_w$ and $\{y_i, t_i\} \in F_m$, (iii) $z = (0, y_0)$, $y_0 \in I_w$, and $\sum_{i=0}^{t} y_i \in \{l, l+\delta-1\}$. It is easy to check that $\Gamma_j(C)$'s are Y-trivial and t-wise equivalent. □

Theorem 4.2.2 *Let $a = w/\delta$ in which $\delta = 2$ if w is even and $\delta = 1$ otherwise. If a 1-regular $(t+1)$-trivial $FS(\lambda, t, a, u+t)$ exists, then a $(t+1)$-trivial $LS(\delta\lambda, t, t+1, \delta uw + t)$ also exists.*

Proof. We adopt notation of Theorem 4.2.1. Let $\mathcal{F} = \{(I_u \cup Z_1, \mathcal{B}_i) | i = 1, \ldots, n\}$ be a 1-regular Z-trivial $FS(\lambda, t, w, u+t)$. Let $S \in P_{0,t+1}(I_u^*)$. Since $\mathcal{F}$ is 1-regular, we can take

$$a_S = \begin{cases} 1 & \text{if } |S| < t, \\ a & \text{otherwise.} \end{cases}$$

By Theorem 4.2.1 and Lemma 4.2.1, we only need to prove that $\Gamma(S)$ is (a, t)-partitionable whenever $|C| = t+1$ (notice that in this case every block of $\Gamma(C)$ is disjoint from Z, so every partition is Z-trivial.).

Let $C = \{x_1, \ldots, x_{t+1}\} \in P_{t+1}(I_u^*)$, then

$$\Gamma(C) = \Pi_{i=1}^{t+1} P_1(Y_i)$$

and the assertion follows by Lemma 2.1.1. □

Theorem 4.2.3 *Let a, b and t be three nonnegative integers such that $t < a \leq b$. If a t-trivial $LS(\lambda, t-1, t, u+t-1)$ and a $FS(\lambda w, t, w, u+t)$ exist, then a 1-regular a-trivial $FS(\lambda wab, t, wa, ub+t)$ exists.*

Proof. Let $S = \{\infty_1, \ldots, \infty_t\}$, $X = I_u \times I_b \cup S$ and $n = u/\lambda$. Let ∞_0 be an arbitrary element of I_u and let $I_u^* = I_u \setminus \{\infty_0\}$, $Y = \{\infty_j | 0 \leq j \leq t-1\}$, $Y_1 \in P_a(\{\infty_0\} \times I_b)$ and $A_j = I_u \times \{j\}$ for $j \in I_b$.

First, we use a $FS(\lambda w, t, w, u+t)$ to form t-wise equivalent collections $\mathcal{G}_i$ $(i \in I_n)$ such that

$$\sum_{i \in I_n} \mathcal{G}_i = \sum_{j \in I_b} wP_{t+1}(A_j \cup S).$$

Let $\Gamma = P_{t+1}(X) \setminus \cup_{i \in I_b} P_{t+1}(A_i \cup S)$, and suppose we can partition Γ into t-wise equivalent subsets $\Gamma_1, \ldots, \Gamma_n$ such that if $B \in \Gamma_i$ $(1 \leq i \leq n)$ and $|B \cap Y_1| > 1$, then $\tau(B) \in \Gamma_i$ for $\tau \in S(Y_1)$. Let η be any a-cycle in $S(Y_1)$, and define

$$\mathcal{H}_i = \sum_{j=1}^{a} \eta^j (w\Gamma_i + \mathcal{G}_i), \ i \in I_n.$$

Obviously $\mathcal{H}_i$'s are t-wise equivalent, therefore $\mathcal{H} = \{(X, \mathcal{H}_i) | i \in I_n\}$ is a $FS(\lambda wab, t, wa, uab + t)$. We prove that it is Y_1-trivial and 1-regular. Let $B \in P_{t+1}(X)$ and $\sigma \in S(Y_1)$. If $|B \cap Y_1| = 1$, then B and $\sigma(B)$ have the same multiplicity in each $\mathcal{H}_i$ as the group generated by σ is transitive on Y_1. If $|B \cap Y_1| > 1$, then $B \in \Gamma$, so there exists a unique $j \in I_n$ such that $B \in \Gamma_j$, and by our assumptions on Γ_i's $\tau(B) \in \Gamma_j$ for $\tau \in S(Y_1)$. Therefore, if $i \neq j$, then neither B nor $C = \sigma(B)$ belongs to $\mathcal{H}_i$, which implies B and $\sigma(B)$ appear with the same multiplicity aw in $\mathcal{H}_j$. Thus, $\mathcal{H}$ is 1-regular and Y_1-trivial.

Now, we establish the existence of Γ_i's. If $C \subset X$, then we can write $C = C_\infty \cup (\cup_{j \in I_b} C_j \times \{j\})$ in which $C_j \subset I_u^*$ and $C_\infty = C \cap (S \cup (\{\infty_0\} \times I_b))$. Let

$\mathcal{F} = \{(I_u^* \cup Y, \mathcal{F}_i) | i \in I_n\}$ be a Y-trivial $LS(\lambda, t-1, t, u+t-1)$. Let $C \in P_{0,t}(I_u^*)$, and $\overline{C}$ be a $(t-|C|)$-subset of Y, then there exists a unique $j \in I_n$ (independent of $\overline{C}$) such that $C \cup \overline{C} \in \mathcal{F}_j$. We denote j by $f(C)$. Let

$$\Gamma_j = \{B \in \Gamma | \sum_{i \in I_b} f(B_i) = j\}, \ j \in I_n.$$

Clearly, $\{\Gamma_j | j \in I_n\}$ is a partition of Γ. Let $T \in P_t(X) \setminus \{S\}$, and

$$A_T = \begin{cases} I_b \setminus \{j\} & \text{if } T \in P_t(A_j \cup S) \text{ for some } j \in I_b, \\ I_b & \text{otherwise.} \end{cases}$$

Clearly $n(T, \Gamma) = w|A_T|$, and $T \cup \{(x, j)\} \in \Gamma$ for $x \in I_u^* \setminus T_j$ and $j \in A_T$. Let $m = \sum_{i \in I_b} f(T_i)$, $B \in \Gamma$ and $T \subset B$. If $B \setminus T \in (\{\infty_0\} \times I_b) \cup S$, then $B \in \Gamma_m$. Therefore, for $l \in I_n \setminus \{0\}$, we have

$$\begin{aligned} n(T; \Gamma_{m+l}) &= \sum_{j \in A_T} |\{x \in I_u^* \setminus T_j | T \cup \{(x, j)\} \in \Gamma_{m+l}\}| \\ &= \sum_{j \in A_T} |\{x \in I_u^* \setminus T_j | T_j \cup \{x\} \in \mathcal{F}_{f(T_j)+l}\}| \\ &= \sum_{j \in A_T} \lambda = |A_T|\lambda = n(T; \Gamma)/n, \end{aligned}$$

which implies $n(T; \Gamma_j) = n(T; \Gamma)/n$ for $j \in I_n$. Finally, let $B \in \Gamma$, $|B \cap Y_1| > 1$ and $\sigma \in S(Y_1)$. Let $C = \sigma(B)$. Then $|C \cap Y_1| = |B \cap Y_1| > 1$, so $C \in \Gamma$, and obviously $C_j = B_j$ for $j \in I_{t+1}$. Therefore $B, C \in \Gamma_l$ in which $l = \sum_{j \in I_b} f(B_j)$ which completes the proof. □

Now, we apply Theorems 4.2.2 and 4.2.3 to construct some infinite families of large sets.

Theorem 4.2.4 *Suppose a $(t+1)$-trivial $LS(\lambda, t, t+1, u+t)$ exists. If either $w = u/\lambda$ or $w = l.c.m.\{\binom{t+1}{i} | 1 = 0, \ldots, t+1\}$ and $l.c.m.\{1, \ldots, t+2\}$ divides u, then a $(t+2)$-trivial $LS(2abw\lambda, t+1, t+2, 2abuw+t+1)$ exists whenever $b \geq a > t+1$.*

Proof. Applying Theorems 4.2.3 and 4.1.4 we can find a 1-regular $(t+2)$-trivial $FS(\lambda abw, t+1, aw, abuw+t+1)$(If $w = u/\lambda$, then a trivial $FS(u, t+1, w, u+t+1)$ exists). Now, the assertion follows by Theorem 4.2.2. □

Theorem 4.2.5 *Let $\lambda(0) = 1$, and $\lambda(m) = 2(m+1)(m+2)l.c.m\{\binom{m}{i} | i = 0, \ldots, m\}\lambda(m-1)$ for $m \geq 1$. Then the necessary conditions for the existence of a $LS(\lambda, t, t+1, v)$ are also sufficient whenever $\lambda(t)$ divides λ.*

Proof. The result follows by induction on t and applying Theorems 4.2.4 and 4.2.3. □

Theorem 4.2.6 *Let m and n be two positive integers, then for $t \geq 0$, a $LS(m(2n)^t\{(t+1)!\}^2, t, t+1, m2^t n^{t+1}\{(t+1)!\}^2 + t)$ exists.*

Proof. The result follows by induction on t and applying Theorem 4.2.4. □

4.3 Halving Complete Designs:An Asymptotic Solution

In this section, we apply Theorems 3.2 to obtain some results on the existence of large sets of size 2. For this, we will need the following theorem which is a restatement of Theorem 2.2.2.

Theorem 4.3.1 *If a* $LS(\lambda_1, t, t+1, n\lambda_1 + t)$ *and a* $LS(\lambda_2, t, t+1, n\lambda_2 + t)$ *exist, then a* $LS((\lambda_1 + \lambda_2), t, t+1, n(\lambda_1 + \lambda_2) + t)$ *also exists.* □

Corollary 4.3.1 *If a* $LS(\lambda_1, t, t+1, n\lambda_1+t)$ *and a* $LS(\lambda_2, t, t+1, n\lambda_2+t)$ *exist, then a* $LS(\lambda, t, t+1, n\lambda + t)$ *also exists whenever* $gcd(\lambda_1, \lambda_2)$ *divides* λ *and* $\lambda > 2\lambda_1\lambda_2$.

Proof. If $\gcd(\lambda_1, \lambda_2) \mid \lambda$ and $\lambda > 2\lambda_1\lambda_2$, then we can write $\lambda = m\lambda_1 + l\lambda_2$ for some nonnegative integers m and l. Now, the result follows by induction on $m + l$. □

Lemma 4.3.1 *Let* t, λ *and* l *be positive integers such that* $2^{l-1} \leq t + 1 < 2^l$ *and* $2^{l-1} | \lambda$. *Then a* $FS((2u+1)\lambda, t, 2u+1, 2\lambda + t)$ *exists for all sufficiently large* u.

Proof. First notice that for $m \geq 1$, the necessary conditions for the existence of a $S(m\lambda, t, t+1, 2\lambda + t)$ hold, so if m is sufficiently large odd integer, then by Lemma 1.3.4, a $S(m\lambda, t, t+1, 2\lambda + t)$ exists. Let $(X, \mathcal{B})$ be a $S(m\lambda, t, t+1, 2\lambda + t)$ and let w be the maximum of the frequencies of the blocks of $\mathcal{B}$. Let

$$\mathcal{B}_1 = \mathcal{B} + wP_{t+1}(X)$$

$$\mathcal{B}_2 = (w + m)P_{t+1}(X) - \mathcal{B}.$$

Then it is straightforward to check that $\{(X, \mathcal{B}_1), (X, \mathcal{B}_2)\}$ is a $FS((2w+m)\lambda, t, 2w+m, 2\lambda + t)$. □

Theorem 4.3.2 *The necessary conditions for the existence of a $LS((v-t)/2, t, t+1, v)$ are also sufficient for v sufficiently large.*

Proof. For $t \leq 6$, the assertion is proved in Theorem 3.1.2. Now, it is easy to see that the necessary conditions can be rewritten in a compact form $v \equiv t \pmod{2^l}$ in which l is defined by $2^{l-1} \leq t + 1 < 2^l$. By Corollary 4.3.1 we only need to find λ_1 and λ_2 such that (i) $\gcd(\lambda_1, \lambda_2) = 2^{l-1}$ and (ii) a $LS(\lambda_1, t, t+1, 2\lambda_1 + t)$ and a $LS(\lambda_2, t, t+1, 2\lambda_2 + t)$ exist.

By Theorem 4.2.6 we can take $\lambda_1 = 2^{2t}[(t+1)!]^2$. Let p be a prime number greater than $t+1$. Let $w_0 = 1$. By Lemma 4.3.1, we can find odd numbers $w_1, \ldots, w_t$ such that (i) w_j and $(t+1)!$ are coprime, and (ii) a $FS(2^{l-1}\Pi_{i=1}^{j-1}(p^2 w_i); j, w_j, 2^l \Pi_{i=1}^{j-1}(p^2 w_i) + j)$ exists. Then, by Theorems 4.2.2 and 4.2.3, we can take $\lambda_2 = 2^{l-1}\Pi_{i=1}^{t}(p^2 w_i)$ which proves the assertion. □

Bibliography

[1] S. Ajoodani-Namini, All block designs with $b = \binom{v}{k}/2$ exist, ***Discrete Math.***, to appear.

[2] S. Ajoodani-Namini, Extending large sets of t-designs, *J. Combin Theory Ser. A* **76** (1996), 139-144.

[3] S. Ajoodani-Namini, On the large sets of t-designs, Preprint.

[4] S. Ajoodani-Namini and G.B. Khosrovshahi, More on halving the complete designs, *Discrete Math.* **135** (1994), 29-37.

[5] W.O. Alltop, Extending t-designs, *J. Combin. Theory Ser. A* **18** (1975),177-186.

[6] Z. Baranyai, On the factorizations of complete uniform hypergraph, Finite and Infinite Sets, *Colloq. Math. Soc. Janos Bolyai* **10** (1975) 91-108. North Holland, Amesterdam.

[7] A. Cayley, On the triadic arrangments of seven and fifteen things, *London, Edinburgh and Dublin Philos. Mag. and J. Sci.* **37** (1850), 50-53.

[8] Y.M. Chee, C.J. Colbourn, S.C. Furino and D.L. Kreher, Large sets of disjoint t-designs, *Austral. J. Combin.* **2** (1990), 111-120.

[9] Y.M. Chee, C.J. Colbourn, and D.L. Kreher, Simple t-designs with $v \leq 30$, *Ars Combinatoria* **29** (1990), 193-258.

[10] L.G. Chouinard II, Partitions of the 4-subsets of a 13-set into disjoint projective planes, *Discrete Math.* **45** (1983), 297-300.

[11] M. Dehon, On the existence of the 2-designs $S_\lambda(2, 3, v)$ without repeated blocks, *Discrete Math.* **43** (1983), 155-171.

[12] M. Dehon, Non-existence d'un 3-designs de parameters $\lambda = 2$, $k = 5$ et $v = 11$, *Discrete Math.* **15** (1976), 23-25.

[13] R.H.F. Denniston, A small 4-design, *Annals of Discrete Math.* **18** (1983), 291-294.

[14] R.H.F. Denniston, Some packings with Steiner triple systems, *Discrete Math.* **9** (1974), 213-227.

[15] J. Doyen, Construction of disjoint Steiner triple systems, *Proc. Amer. Math. Soc.* **32** (1972), 409-416.

[16] J.E. Graver and W.B. Jourkat, The module structure of integral designs, *J. Combin Theory Ser. A* **15** (1973), 75-90.

[17] A . Hartman, Halving the complete design, *Annals of Discrete Math.* **34** (1987), 207-224.

[18] A.S. Hedayat, The theory of trade-off for t-design, in D.Ray-Chaudhuri (ed.), *Coding Theory and Design Theory, Part II, Design Theory, IMA Vol Math. Appl.* **21**, Springer-Verlag, 1990, 101-126.

[19] A.S. Hedayat, G.B. Khosrovshahi, and D. Majumdar, A prospect for a general method for constructing t-designs, *Discrete Appl. Math.* **42** (1993), 31-50.

[20] H.L. Hwang, On the structure of (v, k, t) trades, *J. Statist. Plann. Inference* **13** (1986), 179-191.

[21] G.B. Khosrovshahi and S. Ajoodani-Namini, An infinite family of 6-designs exists, *Sankhyā* **54** (1992), 259-264.

[22] G.B. Khosrovshahi and S. Ajoodani-Namini, A new basis for trades, *SIAM J. Discrete Math.* **3** (1990), 364-372.

[23] G.B. Khosrovshahi and S. Ajoodani-Namini, Combining t-designs, *J. Combin. Theory Ser. A* **58** (1991), 26-34.

[24] T.P. Kirkman, Note on an unanswered prize question, *Cambridge and Dublin Math. Journal* **5** (1850), 255-262.

[25] E.S. kramer, D.W. Leavitt and S.S. Magliveras, Construction Procedures for t-designs and the existence of new simple 6-designs, *Annals of Discrete Math.* **26** (1985), 247-274.

[26] E.S. kramer, S.S. Magliveras and D.R. Stinson, Some small large sets of t-designs, *Austral. J. Combin.* **3** (1991), 191-205.

[27] E.S. kramer and D.M. Mesner, Intersections among Steiner systems, *J. Combin. Theory Ser. A* **16** (1973), 273-285.

[28] D.L. Kreher and S.P. Radsznowski, The existence of simple 6-(14,7,4) designs, *J. Combin. Theory Ser. A* **43** (1986), 237-243.

[29] J.X. Lu, On large sets of disjoint Steiner triple systems, I,II,III, *J. Combin. Theory Ser. A* **34** (1983), 140-146, 147-155, 156-182.

[30] J.X. Lu, On large sets of disjoint Steiner triple systems, IV, V, VI, *J. Combin. Theory Ser. A* **37** (1984), 136-163, 164-188, 189-192.

[31] N.S. Mendelson and S.H.Y. Hung, On the Steiner systems $S(3,4,14)$ and $S(4,5,15)$, *Utilitas Math.* **1** (1972), 5-95.

[32] A. Rosa, A theorem on the maximum number of disjoint Steiner triple systems, *J. Combin. Theory Ser A*, **18** (1975), 305-312.

[33] S. Scheriber, Covering all triples on n marks by disjoint Steiner triple systems, *J. Combin. Theory Ser A* **18** (1973), 347-350.

[34] S. Schreiber, Some balanced complete block designs, *Israel J. Math.* **8** (1974), 31-37.

[35] L. Teirlinck, A completion of Lu's determination of the spectrum for large sets of Steiner triple systems, *J. Combin. Theory Ser. A* **57** (1991), 302-305.

[36] L. Teirlinck, large sets of disjoint designs and related structures, In J.H. Dinitz and D.R. Stinson: ***Contemporary design theory: A collection of surveys***, Wiley, New York, 1992, 561-592.

[37] L. Teirlinck, Locally trivial t-designs and t-designs without repeated blocks, *Discrete Math.*, **77** (1989), 345-356.

[38] L. Teirlinck, On large sets of disjoint quadruple systems, *Ars Combinatoria*, **17** (1984), 173-176.

[39] L. Teirlinck, On the maximum number of disjoint Steiner triple systems, *Discrete Math.*, **6** (1973), 299-300.

[40] L. Teirlinck, On the maximum number of disjoint triple systems, *J. Geometry*, **6** (1975), 93-96.

[41] L. Teirlinck, Non-trivial t-designs without repeated blocks exist for all t, *Discrete Math.*, **65** (1987), 301-311.

[42] Tran Van Trung, On the construction of t-designs and the existence of some new infinite families of simple 5-designs, *Arch. Math.* **47** (1986), 187-192.

[43] R.M. Wilson, Some partitions of all triples into Steiner triple systems, *Hypergraph Seminar, Ohio State University*, 1972. *Lect. Notes Math.* **411** Springer, Berlin, 1974, 267-277.

[44] R.M. Wilson, The necessary conditions for t-designs are sufficient for something, *Utilitas Math.*, **4** (1973), 207-215.