75-18,576

KESTENBAND, Barbu Costin, 1938-
RANK 3 MATROID DESIGNS OF PRIME POWER INDEX AND ASSOCIATED DESIGNS.

The City University of New York, Ph.D., 1975
Mathematics

RANK 3 MATROID DESIGNS OF PRIME POWER INDEX AND ASSOCIATED DESIGNS

by

BARBU C. KESTENBAND

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1975

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

March 19, 1975
date

Chairman of Exam. Committee

March 19, 1975
date

Executive Officer

Professor H. P. Young

Professor A. Hoffman

Professor L. Auslander

Supervisory Committee

TABLE OF CONTENTS

INTRODUCTION

A Matroid $M = (E, \mathcal{I})$ is a finite set E together with a nonempty family $\mathcal{I}$ of subsets of E, called independent sets, such that:

(i) Every subset of an independent set is independent.

(ii) For every $A \subseteq E$, all maximal independent subsets of A have the same cardinality, called the rank of A and denoted by $r(A)$.

The above axiomatization is due to Edmonds [8].

Evidently, matroids generalize the notion of linear independence in vector spaces ([19]). They also have proved particularly useful in generalizing certain theorems about graphs ([18]) and theorems in combinatorial optimization ([9]). On the other hand, one may view matroids as primarily geometric structures by studying the relations among the closed sets ([6]).

Thus matroids provide a unifying theme for many areas of combinatorics. In this dissertation we will show some interesting connections between matroids and the theory of Balanced Incomplete Block Designs (BIBD's), following Young ([21]).

Any maximal independent subset of a set $A \subseteq E$ is called a basis of A. A basis of M is just a basis of E.

A k - flat is a maximal set having rank k.

A hyperplane is an $(r(E) - 1)$ - flat, i.e. a maximal subset of E containing no basis of E.

$M = (E, \mathcal{I})$ is called a Matroid Design (MD) if all hyperplanes have the same cardinality, denoted by k.

M is a Perfect Matroid Design if for every h, all h - flats are equicardinal; for short we refer to them as PMD's.

MD's and PMD's provide an interesting generalization of classical projective and affine geometries.

Other examples of PMD's: t - designs ($\lambda = 1$) and affine triple systems ([22]). Perfect matroid designs are highly complex and beautiful structures, but very difficult to find. Murty, in [15], posed the problem of characterizing all MD's on a set of cardinality v, having rank r and cardinality k. In [21], Young developed methods for solving this problem

and gave a complete solution for the case $v - k = p$, p^2 or pq, where p and q are primes and $p < 2q/3 + 1$ (except for $pq = 6$ or 15) and all ranks r. The prime factorization of the number $v - k$ turns out to be a critical parameter of the problem, and will be called the index of the matroid design.

Our main objective is to extend Young's work by characterizing all matroid designs having rank 3 and prime power index. Matroid designs with prime power index are particularly interesting because they include the class of classical projective geometries. Specifically, every projective geometry of dimension n and order q is a perfect matroid design of rank $n + 1$ and index q^n. Thus matroid designs of prime power index are a rather special generalization of projective geometries, and it is of interest to ask what other structures might they encompass?

In Chapter I we shall answer this question for rank 3, and in so doing we find that all such MD's are either trivial matroids or arise from particular classes of BIBD's and Partially Balanced Incomplete Block Designs.

Both of these classes turn out to be closely related to unitals constructed from finite fields. In the second chapter we consider certain properties of unitals and present a method for constructing a certain unital on $5^3 + 1$ points, which is not isomorphic to the one arising in the context of unitary polarities. This method of constructing unitals is quite general, but it has not been possible so far to carry it out for larger cases.

The third chapter deals with the construction of certain classes of designs needed to realize the MD's found in Chapter I. Composition theorems of considerable generality for transversal designs are developed. These are used to construct certain series of transversal designs and BIBD's which appear to be new, and which include as particular cases, some of the designs used in constructing matroid designs of prime power index. This series of BIBD's actually provides an interesting generalization of the classical finite projective geometries. Finally, some particular constructions of transversal designs are described.

CHAPTER I

RANK 3 MATROID DESIGNS OF PRIME POWER INDEX

We use the methods of Young [21].

We first mention the following basic facts about flats:

Theorem 1.1 If M is a rank n matroid and F^i, F^k are two flats of M having ranks i, k, respectively, where $0 \leqq i < k \leqq n$ and $F^i \subset F^k$, then $F^k - F^i$ is partitioned by the sets of form $F^{i+1} - F^i$, where F^{i+1} is an $(i+1)$-flat containing F^i and contained in F^k.

For proof, see [21], p. 5.

A circuit in a matroid, is a minimal dependent set.

Given a matroid $M = (E, \mathcal{I})$ with basis family $\mathfrak{B}$, the dual of M, denoted by $M^* = (E, \mathcal{I}^*)$, is the matroid with basis family:

$$\mathfrak{B}^* = \left\{E - B : B \in \mathfrak{B}\right\}$$

It is clear that $A^* \in \mathcal{I}^*$ iff $E - A^*$ contains a basis $B \in \mathfrak{B}$. Therefore a circuit of M^*, i.e. a minimal dependent set in M^*, is precisely the complement of a hyperplane in M. The circuits of M^* are also called cocircuits of M.

In a matroid design, all cocircuits have the same cardinality, which we call the index of the matroid design and denote by γ.

Matroid designs may be axiomatized as follows (this is a consequence of the usual hyperplane axioms for matroids, [21], p. 3):

A collection $\mathcal{H}$ of subsets of a finite set E is the hyperplane family of a matroid design on E, if and only if:

(1) For some $k < |E|$, $|H| = k$ for every $H \in \mathcal{H}$.

(2) For every distinct $H_1, H_2 \in \mathcal{H}$ and $x \notin H_1 \cap H_2$, there exists $H \in \mathcal{H}$ such that $H \supseteq \left\{x\right\} \cup (H_1 \cap H_2)$.

We will denote the hyperplane family of a matroid by $\mathcal{H}$.

Let $E' \subseteq E$ and let $\mathcal{I}' = \{J' \subseteq E' : J' \cup J \in \mathcal{I}\}$ for some basis J of $E - E'$. $(E', \mathcal{I}')$ is also a matroid, called the contraction of M to E' and denoted by $M \cdot E'$.

A separator of a matroid $M = (E, \mathcal{I})$ is a subset $S \subseteq E$ such that $S \subseteq H$ or $E - S \subseteq H$ for any $H \in \mathcal{H}$.

It is evident from the definition that the intersection of any number of separators is a separator and the complement of a separator is a separator. Hence the minimal nonempty separators of M partition E.

Where S is a separator, $M \cdot S$ is called a component of M. M is said to be connected if M is its sole component.

If M has the components $M_1, M_2, \ldots, M_r$, then any hyperplane of M is a union of type $M_1 \cup M_2 \cup \ldots \cup H_i \cup \ldots \cup M_r$, where H_i is a hyperplane of M_i.

If M is a matroid design with hyperplane cardinality k and $E' \subseteq E$, then $M \cdot E'$ is a matroid design with hyperplane cardinality $k - |E - E'|$. Hence every component of a matroid design is a matroid design. Since, on the other hand, a matroid is easily determined by its components, it suffices to restrict our attention to connected matroid designs.

We will denote by $\mathfrak{M}_n(\gamma)$, the family of all connected matroid designs having rank n and index γ.

Let M be a matroid. The 0 - flat of M is unique and consists of all elements not contained in any basis of M. Such elements are called loops. The set of all loops is a subset of every flat. Hence we may exclude all loops from M without essentially altering the set-relationships among the flats. We shall always assume in the sequel that M has no loops.

The 1 - flats, or points of M, partition every flat of M. An m - point is a point having cardinality m, and it is said to be a simple point if $m = 1$.

A 2 - flat is called a line.

In general, a simple flat is a flat whose cardinality equals its rank. A simple matroid is a matroid all of whose points are simple.

Simple matroids have been called "Combinatorial Geometries" by Crapo and Rota [6], who relegate matroids to the role of "pregeometries". They take the view that there is no loss of generality in studying only the class of simple matroids; but that this is not the case is seen from

the simple fact that this class is not closed under the operation of contraction. Contraction turns out to be one of the most useful techniques for studying matroid designs, and of course, the cardinalities of the points obtained is essential in describing the matroid as a matroid design.

Let M be a matroid on a set E, with hyperplane family $\mathcal{H}$, and α a positive integer.

For each $x \in E$ we choose an α - set S_x, such that $S_x \cap S_{x'} = \emptyset$ for any distinct $x, x' \in E$. Then we have a matroid M' on the set $E' = \bigcup_{x \in E} S_x$, with hyperplane family $\mathcal{H}' = \left\{ \bigcup_{x \in H} S_x : H \in \mathcal{H} \right\}$.

M' is called an <u>α - inflation</u> of M and we will denote it by αM. M is an <u>α - deflation</u> of M'.

For every pair of integers v, k, such that $v > k \geq 0$, there exists a perfect matroid design M on v elements, with hyperplane size k: let E be a v - set and $\mathcal{J}$ the collection of all subsets of E having cardinalities at most $k + 1$. Then $M = (E, \mathcal{J})$ is a perfect matroid design. Its hyperplanes are all the k - subsets of E.

Any α - inflation of such a matroid is called an <u>(α, k, v) - trivioid</u>, denoted by $\sigma(\alpha, k, v)$.

We will denote by $\tilde{\mathfrak{M}}_n(\gamma)$, the subfamily of $\mathfrak{M}_n(\gamma)$ consisting of nontrivial matroids.

The problem of completely describing the structure of all matroid designs with given rank and index is called <u>the characterization problem for matroid designs</u> ([21]).

Let now M be a rank n matroid on a set E and let $P(m)$ be a rank 1 matroid consisting of a single m - point, where $P(m) \cap E = \emptyset$. If $\mathfrak{F}_{n-2}$ is the family of $(n - 2)$ - flats of M, the hyperplane family of a rank n matroid on $E \cup P(m)$ consists of the hyperplane family of M and of all sets of form:

$$\left\{ P(m) \cup F : F \in \mathfrak{F}_{n-2} \right\}$$

This matroid is called the <u>one - point extension</u> of M by $P(m)$ and denoted by $M \oplus P(m)$.

Every connected rank 1 matroid design is a trivioid, since $\emptyset$ is the only hyperplane. Likewise, every connected rank 2 matroid design is a trivioid, for the hyperplanes are the points. Therefore, for every γ, $\tilde{\mathfrak{M}}_1(\gamma) = \tilde{\mathfrak{M}}_2(\gamma) = \emptyset$.

On the other hand, it is known that $\tilde{\mathfrak{M}}_n(\gamma) = \emptyset$ for some $n \geq 3$ implies $\tilde{\mathfrak{M}}_m(\gamma) = \emptyset$ for any $m \geq n$ ([21], p. 11). Hence $\bigcup_{n=3}^{\infty} \tilde{\mathfrak{M}}_n(\gamma) = \emptyset$ iff $\tilde{\mathfrak{M}}_3(\gamma) = \emptyset$.

More generally, it was shown in [21] that if there exist a few nonisomorphic matroids in $\mathfrak{M}_3(\gamma)$, then it is frequently possible to describe completely the members of $\tilde{\mathfrak{M}}_n(\gamma)$ for every n.

This justifies studying the structure of $\mathfrak{M}_3(\gamma)$ in detail. In [21], the structure of matroids in $\mathfrak{M}_3(pq)$ has been studied, where p and q are primes.

We turn our attention now to the study of the class $\mathfrak{M}_3(p^n)$, where $p > 1$ is a prime.

As we have mentioned in the Introduction, this class contains the projective planes.

PG(n, q) and AG(n,q) will mean, throughout this paper, the projective and affine geometry, respectively, of order q and dimension n, over the finite field GF(q).

It turns out that the class $\mathfrak{M}_3(p^n)$ can be exhaustively described in terms of trivioids, BIBD's and transversal designs.

By a Balanced Incomplete Block Design (BIBD) with parameters v, k, λ $\left((v, k, \lambda)\text{ - BIBD for short}\right)$, is meant a v - set E and a system $\mathfrak{B}$ of k - subsets of E, called blocks, such that any two elements of E occur together in λ blocks. By a system we mean an indexed collection of sets with repetitions allowed.

In [21], p. 27, a Transversal Design is defined:

Let $\mathcal{S}$ be a collection of nonempty subsets partitioning a finite set E. A subset T of E such that $|T \cap S| \leq 1$ for every $S \in \mathcal{S}$ is said to be a partial transversal (PT) of $\mathcal{S}$ and $|T|$ is its length.

A triple $(E, \mathcal{S}, \mathcal{T})$ is a transversal design with parameters t, v, s, k, λ, where $v \geq k \geq t \geq 2$, $s \geq 1$, $\lambda \geq 1$, if:

(i) $\mathcal{S}$ is a family of v nonempty disjoint subsets, called groups, that partition the finite set E and $|S| = s$ for all $S \in \mathcal{S}$.
(ii) $\mathcal{T}$ is a system of PT's of $\mathcal{S}$ such that $|T| = k$ for every $T \in \mathcal{T}$.
(iii) every PT of length t is contained in exactly λ members of $\mathcal{T}$.

For short we refer to any such triple $(E, \mathcal{S}, \mathcal{T})$ as a $TD_t(v, s, k, \lambda)$ and to any transversal design ingeneral as a TD_t or just TD. The members of $\mathcal{T}$ are called blocks.

For any rank 3 matroid, the hyperplanes are the 2 - flats, i.e. the lines. In the following discussion we shall consistently refer to hyperplanes as "lines".

For any point a of a matroid $M \in \mathfrak{M}_3(\gamma)$ on a set E, let $\mathcal{H}_a$ be the set of lines containing a. Then, by theorem 1.1, the sets $H - \{a\}$ where $H \in \mathcal{H}_a$, partition $E - \{a\}$. Hence:

$(k - |a|) \mid (|E| - |a|)$, or, noting that $|E| - k = \gamma$, $(k - |a|) \mid \gamma$.

But $k - |a| \neq \gamma$. To see this, suppose $k - |a| = \gamma$ for some point a. Then $(|E| - |a|)/(k - |a|) = 2$, so a is contained in precisely two lines of M, say H_1 and H_2.

Let $H_1 = \{a, a_1, \ldots, a_u\}$ and $H_2 = \{a, b_1, \ldots, b_v\}$.

$H_1 \cup H_2 = E$ and since every two points are contained in a unique line, $\{a_i, b_j\}$ is a line for all i, j.

Thus:

$$k = |a| + |a_1| + \ldots + |a_u| = |a| + |b_1| + \ldots + |b_v| = |a_i| + |b_j|,$$

for $i = 1, 2, \ldots, u$ and $j = 1, 2, \ldots, v$.

From these equalities it follows that:

$|a_1| = \ldots = |a_u| = \alpha$ (say) and $|b_1| = \ldots = |b_v| = \beta$ (say). Then:

$$k = |a| + u\alpha = |a| + v\beta = \alpha + \beta .$$

Thus: $\beta = |a| + (u - 1)\alpha$ and:

$|a| + u\alpha = |a| + v\beta = |a| + v|a| + v(u - 1)\alpha$, whence:

$u\alpha = v|a| + v(u - 1)\alpha$, which implies $u > v(u - 1)$. But this inequality is true only if $u = 1$ or/and $v = 1$.

If $u = 1$, the hyperplanes of M are: $H_1 = \{a, a_1\}$, $H_2 = \{a, b_1, \ldots, b_v\}$, $\{a_1, b_1\}$, $\ldots$, $\{a_1, b_v\}$ and it follows immediately that $\{a_1\}$ is a separator of M , contrary to the hypothesis that M is connected.

Similarly if $v = 1$, which completes the proof.

Therefore, if for every line H and number d , where $1 \leq d \leq k$, we let x_d^H denote the number of $(k - d)$ - points contained in H , we get:

$$|H| = k = \sum_{\substack{d|\gamma \\ d\neq\gamma}} (k - d)x_d^H \tag{1.1}$$

If $\gamma = p^n$, (1.1) becomes:

$$(k - 1)x_1 + (k - p)x_2 + \ldots + (k - p^{n-1})x_n = k \tag{1.2}$$

where x_i denotes the number of $(k - p^{i-1})$ - points contained in H.

For every line H , there exists a solution $(x_1, \ldots, x_n)$ to (1.2). Hence, in order to establish $\mathfrak{m}_3(p^n)$, we will pursue a diophantine analysis of (1.2).

We first note that $x_1 > 2$ is impossible, because (1.2) yields $k \geq (k - 1)x_1$, or $x_1 > 2$ would imply $k > 2(k - 1)$, i.e. $k < 2$, which is impossible.

So let $x_1 = 2$. As before, we obtain from (1.2):

$k \geq (k - 1)x_1 = 2k - 2$, whence $k \leq 2$ and hence $k = 2$. (1.2) reduces to:

$$2 + (2 - p)x_2 + \ldots + (2 - p^{n-1})x_n = 2$$

Hence $x_2 = \ldots = x_n = 0$ and H consists of 2 simple points. But then all points of M must be simple, because any line contains at

least two points and has cardinality 2.

Therefore we have obtained a $\sigma(1, 2, p^n + 2)$.

Let now $x_1 = 1$. (1.2) becomes:

(1.3) $(k - p)x_2 + (k - p^2)x_3 + \ldots + (k - p^{n-1})x_n = 1$

If $k \leq p$, (1.3) becomes $0 = 1$, absurd. Hence $k > p$. Let t be the largest natural number such that $p^t < k$ and let:

$$m = \min(t, n - 1) .$$

Hence $p^m < k$ and (1.3) reduces to:

(1.4) $(k - p)x_2 + (k - p^2)x_3 + \ldots + (k - p^m)x_{m+1} = 1$

(1.4) shows that only one of $x_2, x_3, \ldots, x_{m+1}$ can be non-zero; moreover, the nonzero x_j must equal 1. So we obtain:

$(k - p^{j-1})x_j = 1$, i.e. $k = p^{j-1} + 1$, where j satisfies $1 \leq j \leq m + 1$.

On the other hand, $k > p^m$, i.e. $p^{j-1} + 1 > p^m$, which in turn implies $j \geq m+1$. Therefore $j = m + 1$ and we conclude that the only solution of (1.4) is: $x_2 = \ldots = x_m = 0$, $x_{m+1} = 1$.

Hence $k = p^m + 1$ and the line H consists of one p^m - point and one simple point.

Now M cannot contain any other nonsimple point, because any two points lie in one line, and the common cardinality of all lines must be $p^m + 1$. Hence M is of form:

$(p^n + 1, p^m + 1, 1)$ - BIBD $\oplus$ $P(p^m)$, for each $m = 1, 2, \ldots, n - 1$ for which the BIBD exists.

Lastly, let $x_1 = 0$. (1.2) becomes:

(1.5) $(k - p)x_2 + (k - p^2)x_3 + \ldots + (k - p^{n-1})x_n = k$, or:

(1.6) $p(x_2 + px_3 + \ldots + p^{n-2}x_n) = k(x_2 + x_3 + \ldots + x_n - 1)$

Hence $p|k$ or $p|x_2 + x_3 + \ldots + x_n - 1$.

Let first $p|k$, i.e. $k = k_1 p$ (k_1 an integer).

(1.6) becomes:

$x_2 + px_3 + \ldots + p^{n-2}x_n = k_1(x_2 + x_3 + \ldots + x_n - 1)$, or:

(1.7) $\quad (k_1 - 1)x_2 + (k_1 - p)x_3 + \ldots + (k_1 - p^{n-2})x_n = k_1$

(1.7) is similar to (1.2), as can be readily seen. As in that case, $x_2 \leq 2$, because $x_2 > 2$ leads to $k_1 < 2$, i.e. $k_1 = 1$ and $k = k_1 p = p$. But the latter equality contradicts (1.5).

So we let $x_2 = 2$ and obtain $k_1 = 2$, whence $k = 2p$ and the line H is the union of two p - points.

All other points of M might have cardinality:

$k - 1 = 2p - 1$ or $k - p = 2p - p = p$.

The $(2p - 1)$ - points must be ruled out because:

$(2p - 1) + p > 2p$. Thus all points of M are p - points and M is a $\sigma(p, 2, p^{n-1} + 2)$.

If $x_2 = 1$, (1.7) reduces to:

(1.8) $\quad (k_1 - p)x_3 + \ldots + (k_1 - p^{n-2})x_n = 1$, where $k_1 > p$, i.e. $k > p^2$.

Let, as before, t be the largest natural number such that $p^t < k_1$ and let $m = \min(t, n - 2)$. Hence $p^m < k_1$. Then (1.8) becomes:

(1.9) $\quad (k_1 - p)x_3 + \ldots + (k_1 - p^m)x_{m+2} = 1$

As in the case of equation (1.4), we find that the only solution of (1.9) is: $x_3 = \ldots = x_{m+1} = 0$ and $x_{m+2} = 1$.

Hence $k_1 = p^m + 1$ and $k = p^{m+1} + p$. H consists of one p^{m+1} - point, say a , and one p - point.

Other points of M might have cardinality $k - p^j = p^{m+1} + p - p^j$, $(0 \leq j \leq m + 1)$.

So let b be a $(p^{m+1} + p - p^j)$ - point.

We must have $|\{a, b\}| = |a| + |b| = p^{m+1} + |b|$.

But $|\{a, b\}| \leq k = p^{m+1} + p$ and thus $|b| \leq p$, i.e. $p^{m+1} + p - p^j \leq p$, whence $j \geq m+1$, i.e. $j = m+1$.

Hence all points of M except α, are p - points and there are $1 + p^n/p = 1 + p^{n-1}$ such points.

Therefore M is a $(p^{n-1} + 1, p^m + 1, 1)$ - BIBD $\oplus$ $P(p^m)$, inflated by p, for each $m = 1, 2, \ldots, n - 2$ for which the BIBD exists.

If $x_2 = 0$, we obtain a new case, similar to the one we have just analyzed. Thus we get a steady pattern of the proof. All possibilities are summed up in the following scheme:

$$x_1 = \begin{cases} 2 \to \sigma_1 \\ 1 \to B_1 \\ 0 \end{cases}$$

$$\searrow \begin{cases} p \mid x_2+\ldots+x_n-1 \text{ (yet to be studied)} \\ p \mid k \end{cases}$$

$$\searrow x_2 = \begin{cases} 2 \to \sigma_2 \\ 1 \to B_2 \\ 0 \end{cases}$$

$$\searrow \begin{cases} p \mid x_3+\ldots+x_n-1 \text{ (yet to be studied)} \\ p \mid k_1 \end{cases}$$

$$\searrow x_3 = \begin{cases} 2 \to \sigma_3 \\ 1 \to B_3 \\ 0 \end{cases}$$

$$\vdots$$

$$\searrow \begin{cases} p \mid x_{n-1}+x_n-1 \text{ (yet to be studied)} \\ p \mid k_{n-3} \end{cases}$$

$$\searrow x_{n-1} = \begin{cases} 2 \to \sigma_{n-1} \\ 1 \to B_{n-1} \\ 0 \end{cases}$$

$$\searrow \begin{cases} p \mid x_n-1 \text{ (yet to be studied)} \\ p \mid k_{n-2} \end{cases} \to x_n = 2 \to \sigma_n .$$

Here, $k = pk_1 = p^2k_2 = \ldots = p^{n-1}k_{n-1}$ and:

$\sigma_i = \sigma(p^{i-1}, 2, p^{n-i+1} + 2)$, $i = 1, 2, \ldots, n$;

$B_i = (p^{n-i+1} + 1, p^m + 1, 1)$ - BIBD $\oplus$ $P(p^m)$, inflated by p^{i-1}, for each $m = 1, 2, \ldots, n - i$ for which the corresponding BIBD exists ($i = 1, 2, \ldots, n-1$).

*

Returning now to (1.5):

(1.5) $(k - p)x_2 + (k - p^2)x_3 + \ldots + (k - p^{n-1})x_n = k$

Let again $m = \min(t, n - 1)$, where t is the largest natural number such that $p^t < k$. Hence $p^m < k$. The range of m is:

(1.10) $$1 \leq m \leq n - 1 ,$$

because $k \leq p$ would render (1.5) meaningless.

(1.5) reduces to:

(1.11) $$(k - p)x_2 + \ldots + (k - p^m)x_{m+1} = k$$

We now have to study the case $p \mid x_2 + \ldots + x_n - 1$, which, by (1.11), reduces to:

(1.12) $$p \mid x_2 + \ldots + x_{m+1} - 1$$

(1.11) can be rewritten as:

(1.13) $$p(x_2 + px_3 + \ldots + p^{m-1}x_{m+1}) = k(x_2 + \ldots + x_{m+1} - 1)$$

(1.12) means:

(1.14) $$x_2 + \ldots + x_{m+1} - 1 = hp$$

h is a nonnegative integer, for if $h = 0$ we obtain that H contains only one point. Hence:

$$x_{m+1} = hp - x_2 - \ldots - x_m + 1$$

Upon substituting this expression in (1.13), we get, with the help of (1.14):

$p[x_2 + px_3 + \ldots + p^{m-2}x_m + p^{m-1}(hp - x_2 - x_3 - \ldots - x_m + 1)] = khp$, or:

$x_2(1 - p^{m-1}) + x_3(p - p^{m-1}) + \ldots + x_m(p^{m-2} - p^{m-1}) + hp^m + p^{m-1} = kh$,

whence:

(1.15) $$(k - p^m)h = p^{m-1} + x_2(1 - p^{m-1}) + \ldots + x_m(p^{m-2} - p^{m-1})$$

But $k > p^m$ implies $(k - p^m)h > 0$, so (1.15) yields:

(1.16) $p^{m-1} > (p^{m-1} - 1)x_2 + (p^{m-1} - p)x_3 + \ldots + (p^{m-1} - p^{m-2})x_m$

On the other hand, for any i, j, such that $0 \le i \le j < m-1$ we have:

$p^i + p^j \le p^{m-1}$ (proof: $p^i + p^j \le 2p^j \le p^{j+1} \le p^{m-1}$), which is equivalent to:

(1.17) $$p^{m-1} \le (p^{m-1} - p^i) + (p^{m-1} - p^j)$$

(1.17) shows that in (1.16) at most one of the numbers x_2, x_3, ..., x_m may be nonzero and that that number must be 1.

Let us first study the case $x_2 = x_3 = \ldots = x_m = 0$.

Then (1.11) reduces to:

$(k - p^m)x_{m+1} = k$, where, by (1.14), $x_{m+1} = 1 + hp$. Hence:

$(k - p^m)(1 + hp) = k$, or:

(1.18) $$h(k - p^m) = p^{m-1}$$

(1.18) shows that $h = p^r$ for some r such that:

$0 \le r \le m - 1$.

Hence (1.18) becomes:

(1.19) $$k = p^m + p^{m-r-1}$$

$$x_{m+1} = 1 + hp = 1 + p^{r+1}$$

Therefore our line H consists of $1 + p^{r+1}$ p^{m-r-1} - - points. All other points of M may have cardinality:

$k - p^i = p^m + p^{m-r-1} - p^i$, where $0 \le i \le m$, since $p^m + p^{m-r-1} - p^i \le 0$ for $i > m$.

Those i's should be ruled out for which:

(1.20) $$p^m + p^{m-r-1} - p^i > p^m,$$

because a point a such that $|a| > p^m$ would give rise, together with a p^{m-r-1} - point, to a line having cardinality larger than $p^m + p^{m-r-1}$, which must not happen.

(1.20) yields immediately: $i < m - r - 1$.

Hence all other points of M may have cardinality:

$p^m + p^{m-r-1} - p^i$, where $m - r - 1 \leq i \leq m$.

But, on the other hand, if i satisfies $m - r - 1 \leq i \leq m - 1$ there cannot be more than one $(p^m + p^{m-r-1} - p^i)$ - point, for if there were two, they would generate a line H' of cardinality:

$$|H'| \geq (p^m + p^{m-r-1} - p^i) + (p^m + p^{m-r-1} - p^j) , \tag{1.21}$$

where $m - r - 1 \leq i \leq j \leq m - 1$.

But (1.21) implies $|H'| > p^m + p^{m-r-1} = k$

(proof: $|H'| \geq 2(p^m + p^{m-r-1}) - (p^i + p^j) \geq 2(p^m + p^{m-r-1}) - 2p^j \geq 2(p^m + p^{m-r-1}) - p^{j+1} \geq 2(p^m + p^{m-r-1}) - p^m > p^m + p^{m-r-1}$) and this is a contradiction.

Therefore there is at most one $(p^m + p^{m-r-1} - p^i)$ - point for $m - r - 1 \leq i \leq m - 1$, but there can be, of course, several $p^m + p^{m-r-1} - p^m = p^{m-r-1}$ - points, namely $p^{r+1} + 1 + p^n/p^{m-r-1} = 1 + p^{r+1} + p^{n-m+r+1}$ of those, where $n - m + r + 1 > r + 1$ because $n - m \geq 1$.

Thus, under the assumption that all points of M have the same cardinality, we obtain M in the form of a:

$(1 + p^{r+1} + p^{n-m+r+1}, 1 + p^{r+1}, 1)$ - BIBD, inflated by p^{m-r-1} ,

where $1 \leq m \leq n - 1$, $0 \leq r \leq m - 1$, whenever the required BIBD exists.

If $m = n - 1$ and $r = 0$, these are $PG(2, p)$.

Under the assumption that there is one $(p^m + p^{m-r-1} - p^i)$ - point, say a , there will be $(p^n + p^i)/p^{m-r-1} = p^{n-m+r+1} + p^{i-m+r+1}$ p^{m-r-1} - points.

If $\mathcal{H}' = \{H : H \in \mathcal{H} , a \in H\}$, then any $H' \in \mathcal{H}'$ is the union of a and $p^i/p^{m-r-1} = p^{i-m+r+1}$ p^{m-r-1} - points.

The set $E - \{a\}$ is partitioned by the sets of form $H' - \{a\}$ into $1 + p^{n-i}$ subsets, each consisting of $p^{i-m+r+1}$ p^{m-r-1} - points.

Hence M is of the form:

$TD_2(1 + p^{n-i}, p^{i-m+r+1}, 1 + p^{r+1}, 1)$, inflated by p^{m-r-1} and an extra

$(p^{m-r-1} + p^m - p^i)$ - point, attached to each group, where:

$1 \le m \le n-1$, $0 \le r \le m-1$, $m-r-1 \le i \le m-1$, whenever the TD_2 exists.

We have thus exhausted the case $x_i = 0$, $i = 1, 2, \ldots, m$, $p \mid x_2 + \ldots + x_{m+1} - 1$.

Now, in order to be done with the case $x_1 = 0$, we still have to consider the situation where $x_j \neq 0$ for some $j = 2, \ldots, m$ and $p \mid x_2 + \ldots + x_{m+1} - 1$.

But we have already seen that $x_j \neq 0$ implies $x_j = 1$ and $x_t = 0$ for all $t \neq j, m+1$.

It turns out, however, that this case has been covered already: consider again the $(p^m + p^{m-r-1} - p^i)$ - point α and a line H' containing it. H' consists of α and $p^{i-m+r+1}$ p^{m-r-1} - points, thus corresponding to the following solution of (1.11):

$x_t = 0$ for $t \neq i+1, m+1$; $x_{i+1} = 1$; $x_{m+1} = p^{i-m+r+1}$, where i satisfies $1 \le i \le m-1$.

But this is precisely the problem we are dealing with now, if we identify j with $i+1$.

This exhausts the case $x_1 = 0$.

The remaining possibilities are of the form:

$x_1 = x_2 = \ldots = x_s = 0$ and $p \mid x_{s+1} + \ldots + x_n - 1$, for all $s = 2, 3, \ldots \ldots, n-1$.

Thus, (1.2) becomes:

$$(k - p^s)x_{s+1} + \ldots + (k - p^{n-1})x_n = k$$

If, as before, we let $m = \min(t, n-1)$, where t is the largest natural number such that $p^t < k$, we conclude that at most one of the numbers $x_{s+1}, \ldots, x_m$, may be nonzero and that that number must equal 1.

But all these cases have been studied when we analyzed the different possibilities arising from the fact that at most one of $x_2, \ldots, x_m$ can be nonzero.

This completely exhausts the problem.

* * *

Summing up, the class $\mathfrak{M}_3(p^n)$ consists of the following four types of matroids:

Type I: $\sigma(p^{i-1},\ 2,\ p^{n-i+1}+2)$, $i = 1, 2, \ldots, n$.

Type II: $(p^{n-i+1}+1,\ p^m+1,\ 1)$ - BIBD $\oplus$ $P(p^m)$ inflated by p^{i-1} , $i = 1, 2, \ldots, n-1$; $m = 1, 2, \ldots, n-i$.

Type III: $(1 + p^{r+1} + p^{n-m+r+1},\ 1 + p^{r+1},\ 1)$ - BIBD , inflated by p^{m-r-1} , $m = 1, 2, \ldots, n-1$; $r = 0, 1, \ldots, m-1$.

Type IV: $TD_2(1 + p^{n-i},\ p^{i-m+r+1},\ 1 + p^{r+1},\ 1)$, inflated by p^{m-r-1} and an extra $(p^{m-r-1} + p^m - p^i)$ - point attached to each group , $m = 1, 2, \ldots, n-1$, $r = 0, 1, \ldots, m-1$, $i = m-r-1, m-r, \ldots, m-1$. If $i = m-r-1$, however, type IV reduces to type II.

We want now to find necessary conditions for the existence of these designs.

The following elementary relations hold among the parameters of a BIBD ([10], p. 101):

(1.22) $$bk = vr$$

(1.23) $$r = \frac{\lambda(v-1)}{k-1}$$

(1.24) $$b = \frac{\lambda v(v-1)}{k(k-1)}$$

Here, by r (replication number) we denote the number of blocks containing any given element.

In a TD_t , the number of blocks containing any length - i transversal is (by [21], p. 29):

$$\lambda_i = \lambda\binom{v-i}{t-i}s^{t-i}/\binom{k-i}{t-i} \quad , \quad 0 \le i \le t \ .$$

The number of blocks is therefore:

$$b = \lambda_o = \lambda\binom{v}{t}s^t/\binom{k}{t}$$

In a TD_2:

(1.25) $$b = \frac{\lambda v(v-1)s^2}{k(k-1)}$$

(1.26) $$r = \frac{bk}{sv} = \frac{\lambda(v-1)s}{k-1}$$

Hence, for a $(p^{n-i+1}+1,\ p^m+1,\ 1)$ - BIBD (type II) we get by (1.24) and (1.23):

$$b = \frac{p^{n-i+1}+1}{p^m+1}\, p^{n-i-m+1}$$, which is an integer iff $n-i+1$ is an odd multiple of m.

$$r = p^{n-i-m+1}$$

For the $(1 + p^{r+1} + p^{n-m+r+1},\ 1 + p^{r+1},\ 1)$ - BIBD (type III) we obtain:

$$b = \frac{(1 + p^{r+1} + p^{n-m+r+1})(1 + p^{n-m})}{1 + p^{r+1}}$$, which

shows that $n-m$ must be an odd multiple of $r+1$.

$$r = 1 + p^{n-m}$$

As regards the $TD_2(1 + p^{n-i},\ p^{i-m+r+1},\ 1 + p^{r+1},\ 1)$, we get by (1.25) and (1.26):

$$b = \frac{1 + p^{n-i}}{1 + p^{r+1}}\, p^{i-2m+n+r+1}$$, hence $n-i$ must be an odd multiple of $r+1$.

$$r = p^{n-m}$$

*

We will now show that we can represent all members of $\mathfrak{M}_3(p^n)$ (i.e. the types II - IV) by a uniform symbol. By unifying all types of rank 3 matroid designs of prime power index into a single entity, we gain further insight into the structure of matroid designs in general.

Where $(E, \mathcal{S}, \mathcal{I})$ is a $TD_2(v, s, k, 1)$ and P a point not in E, we let the hyperplane family of a rank 3 matroid be:

$$\mathcal{H} = \mathcal{I} \cup_{S \in \mathcal{S}} (S \cup \{P\})$$

We denote an α - inflation of such a matroid by $\alpha M(v, s, k)$ and if it is a matroid design, by $\alpha MD(v, s, k)$. We note that the parameters α, v, s, k, are sufficient to fully define the matroid design, because the cardinality of P must be $k - s$.

Then the following theorem unifies the matroid designs of types II - IV:

Theorem 1.2

$$\mathbb{m}_3(p^n) = \{p^{n-(2t+1)m-h}\ MD(p^{(2t+1)m} + 1,\ p^h,\ p^m + 1) : 0 \le h \le m\ ;\ n \ge (2t + 1)m + h\}.$$

The type II MD's correspond to $h = 0$

The type III MD's correspond to $h = m$

The type IV MD's correspond to $0 < h < m$.

CHAPTER II

UNITALS AND DERIVED DESIGNS

In order to actually construct the designs required by chapter I, it turns out that the basic BIBD we need study is the $(1 + q^3, 1 + q, 1)$ - BIBD, where q is a prime power.

A BIBD was defined in chapter I.

A BIBD on the set E is said to be resolvable if the b blocks can be divided into r classes, each consisting of v/k blocks, and such that the blocks of each class contain among themselves, all elements of E (the r classes are also called parallel classes).

A similar definition holds for resolvable transversal designs.

The purpose of this chapter is to summarize the essential facts that are known about the construction of $(1 + q^3, 1 + q, 1)$ - BIBD's and to present a new construction.

Any BIBD with these parameters is called a unital.

This notion is arrived at in the following fashion ([7]):

A correlation of a projective geometry $\mathcal{G}$ is a permutation δ of its subspaces which inverts inclusion, i.e.:

(2.1) $S \subseteq T$ implies $S^\delta \supseteq T^\delta$ for all subspaces S, T of $\mathcal{G}$.

A subspace S of $\mathcal{G}$ is termed totally isotropic, isotropic, or nonisotropic with respect to the correlation δ, according as $S \cap S^\delta$ is S, nonempty or empty, respectively.

It is clear that for the points of $\mathcal{G}$, "totally isotropic" has the same meaning as "isotropic" and we can use the latter term consistently. Such points are also called absolute.

Given a (not necessarily commutative) field $\mathfrak{F}$, an anti-automorphism α of $\mathfrak{F}$ is a 1-1 correspondence among the elements of $\mathfrak{F}$ such that $(x + y)^\alpha = x^\alpha + y^\alpha$ and $(xy)^\alpha = y^\alpha x^\alpha$.

Let V be a left vector space of finite rank over a field $\mathfrak{F}$. By $\mathcal{P}(V)$ we denote the projective geometry consisting of the non-zero subspaces of V. Every desarguesian projective geometry is isomorphic to some $\mathcal{P}(V)$.

Let α be an anti-automorphism defined on $\mathfrak{F}$. A sesquilinear form s with companion anti-automorphism α is then a mapping from $V \times V$ into $\mathfrak{F}$, such that:

i) $s(x + x', y + y') = s(x, y) + s(x, y') + s(x', y) + s(x', y')$ for all $x,x',y,y' \in V$;

ii) $s(fx, gy) = fs(x, y)g^\alpha$ for all $f,g \in \mathfrak{F}$ and $x,y \in V$.

Given a sesquilinear form s on V, we associate with every subspace S of V, the set:

(2.2) $$S^\delta = \{x \in V : s(x, S) = 0\},$$ where $s(x, S) = 0$ means $s(x, y) = 0$ for all $y \in S$.

Given S, S^δ is a subspace of V and (2.1) is clearly satisfied. Hence the mapping δ defined by (2.2) is a correlation of $\mathcal{P}(V)$ iff it is a permutation of the subspaces of V. This is the case iff the sesquilinear form s is nondegenerate, i.e. if $s(x, y) = 0$ for all $y \in V$ iff $x = 0$.

Thus for every nondegenerate sesquilinear form on V, (2.2) defines a correlation of $\mathcal{P}(V)$.

Conversely, if δ is a correlation of the projective geotry $\mathcal{P}(V)$, then there exists a nondegenerate sesquilinear form s on V such that δ is given by (2.2).

A correlation of order 2 is called a polarity: δ is a polarity of a projective geometry if $(S^\delta)^\delta = S$ for all subspaces S.

In the desarguesian case, a nondegenerate sesquilinear form s on V represents a polarity of $\mathcal{P}(V)$ iff $s(x, y) = 0$ implies $s(y, x) = 0$ for all $x, y \in V$.

Let s be a polarity of $\mathcal{P}(V)$ with companion anti-automorphism α. Then we must have $\alpha^2 = 1$. If $\alpha \neq 1$, we also have

$s(x, y) = s(y, x)^{\alpha}$ and the polarity is called unitary.

PG(n, q) , where q is a prime power, admits unitary polarities if and only if q is a square.

If $q = s^2$ and π is a unitary polarity of $PG(n, s^2)$, a line of $PG(n, s^2)$ consists entirely of isotropic points with respect to π iff it is totally isotropic. Every other line contains either at most one or exactly $s + 1$ isotropic points.

In the case of a projective plane $PG(2, s^2)$, there cannot exist totally isotropic lines. Also, the number of isotropic points is $s^3 + 1$ and these, together with the nonisotropic lines, as blocks, form a $(s^3 + 1, s + 1, 1)$ - BIBD.

BIBD's with these parameters are generally known as unitals, because the only complete class of designs with these parameters come from unitary polarities of a $PG(2, s^2)$.

A slightly different, though essentially the same, treatment of unitals, can be found in [1]. It is also shown there that unitals obtained as in the foregoing discussion are resolvable.

In [1], the curve $\mathcal{C}$ with equation:

$$x_1^{s+1} + x_2^{s+1} + x_3^{s+1} = 0 \tag{2.3}$$

is considered in $PG(2, s^2)$, where s is a prime power and $x_i \in GF(s^2)$, $i = 1, 2, 3$.

Given a point $P(p_1, p_2, p_3) \in PG(2, s^2)$, the line:

L_p: $p_1^s x_1 + p_2^s x_2 + p_3^s x_3 = 0$ is called the polar of P with respect to $\mathcal{C}$.

The construction of a unital then proceeds through the following lemmas whose proofs are given in [1]:

Lemma 2.1 $\mathcal{C}$ contains $s^3 + 1$ points.

Lemma 2.2 Given a point $A(a_1, a_2, a_3)$ on $\mathcal{C}$, its polar L_A intersects $\mathcal{C}$ at exactly one point.

By virtue of lemma 2.2, the polars of points on $\mathcal{C}$ are also

tangents to C. If a line meets C at two distinct points, it is called a secant to C.

Lemma 2.3 Any secant to C has $s + 1$ points in common with C.

It follows from these lemmas that an $(s^3 + 1, s + 1, 1)$ - - BIBD has been obtained on the set of points of C ; the blocks are the sets obtained as intersections between C and the secants to C.

Essentially, C is the set of isotropic points with respect to the unitary polarity π which maps each point (a_1, a_2, a_3) onto the line $a_1^s x_1 + a_2^s x_2 + a_3^s x_3 = 0$ and each line $b_1 x_1 + b_2 x_2 + b_3 x_3 = 0$ onto the point $(b_1^{1/s}, b_2^{1/s}, b_3^{1/s})$.

The polar of any point is therefore its image under π.

Also, the tangents and secants to C are the isotropic and nonisotropic lines, respectively.

Lemma 2.4 Any unital obtained as in lemmas 2.1 - 2.3 is resolvable.

For the proof, see [1], p. 348.

The unitals discussed so far enjoy a further property which will play an important role in the sequel.

By a Pasch Configuration in a BIBD with $\lambda = 1$ on a set E, is meant a set of four distinct blocks such that each of them intersects the other three at three distinct points (fig. 1).

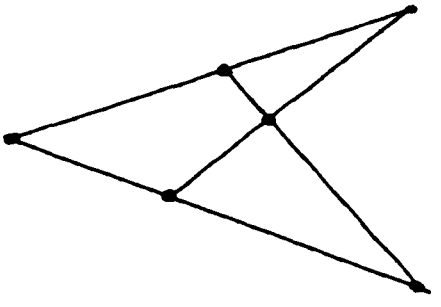

Fig. 1

The Pasch Configuration exists in any projective geometry, by definition of the latter (we regard the geometry as a BIBD with the lines as blocks).

It turns out that the same configuration can be of much help in deciding whether two given BIBD's with identical parameters are isomorphic: if one of them does and the other does not contain a Pasch Configuration, they are obviously nonisomorphic.

The usefulness of this method for the problem under consideration was pointed out to the author by Prof. J. J. Seidel.

Specifically, we can prove the following:

Lemma 2.5 The Pasch Configuration does not exist in the unitals constructed in lemmas 2.1 - 2.3.

Proof We have to demonstrate that: if $A(a_1, a_2, a_3)$, $B(b_1, b_2, b_3)$ and $C(c_1, c_2, c_3)$ are any three noncollinear points on the curve $\mathcal{C}$ and $D \in L_{AB} \cap \mathcal{C}$, $E \in L_{AC} \cap \mathcal{C}$, then the intersection point M between L_{CD} and L_{BE} does not lie on $\mathcal{C}$.

Throughout this proof, summations will be understood to be from $i = 1$ to $i = 3$.

Let $D(a_1 + yb_1, a_2 + yb_2, a_3 + yb_3)$; $y \neq 0$;

and $E(a_1 + zc_1, a_2 + zc_2, a_3 + zc_3)$; $z \neq 0$;

Then $M(a_1 + yb_1 + zc_1, a_2 + yb_2 + zc_2, a_3 + yb_3 + zc_3)$.

Since D lies on $\mathcal{C}$, we have by (2.3):

$$\Sigma(a_i + yb_i)^{s+1} = 0 \tag{2.4}$$

But:

$$(a_i + yb_i)^{s+1} = (a_i^s + y^s b_i^s)(a_i + yb_i) = a_i^{s+1} + y^{s+1} b_i^{s+1} + y^s a_i b_i^s + y a_i^s b_i$$

Substituting in (2.4) gives:

$y^s \Sigma a_i b_i^s + y \Sigma a_i^s b_i = 0$ (all other terms vanish because A and B are on $\mathcal{C}$).

Similarly:

$$z^s \Sigma a_i c_i^s + z \Sigma a_i^s c_i = 0 \tag{2.5}$$

Hence:

$$y^{s-1} = -\frac{\Sigma a_i^s b_i}{\Sigma a_i b_i^s} = -\frac{(\Sigma a_i b_i^s)^s}{\Sigma a_i b_i^s} = -(\Sigma a_i b_i^s)^{s-1} \tag{2.6}$$

$$z^{s-1} = -(\Sigma a_i c_i^s)^{s-1} \tag{2.7}$$

We assume now that M lies on C . This means:

$\Sigma(a_i + yb_i + zc_i)^{s+1} = 0$, or, by expanding the left hand side:

$$\Sigma(a_i + yb_i)^{s+1} + (a_i^s + y^s b_i^s)zc_i + (a_i + yb_i)z^s c_i^s + (zc_i)^{s+1} = 0$$

Here, the first and last terms are 0, because D, C, respectively, are on C.

Hence:

$\Sigma(a_i^s + y^s b_i^s)zc_i + (a_i + yb_i)z^s c_i^s = 0$, or:

$z\Sigma a_i^s c_i + z^s \Sigma a_i c_i^s + y^s z \Sigma b_i^s c_i + yz^s \Sigma b_i c_i^s = 0$, or, by (2.5):

$$y^{s-1}\Sigma b_i^s c_i + z^{s-1}\Sigma b_i c_i^s = 0 \tag{2.8}$$

By (2.6) and (2.7), (2.8) becomes:

$$(\Sigma a_i b_i^s)^{s-1}(\Sigma b_i^s c_i) + (\Sigma a_i c_i^s)^{s-1}(\Sigma b_i c_i^s) = 0 \tag{2.9}$$

But $\Sigma b_i^s c_i = (\Sigma b_i c_i^s)^s$ and also:

$$(\Sigma a_i c_i^s)^{s-1} = (\Sigma a_i^s c_i)^{s(s-1)} = (\Sigma c_i a_i^s)^{(s^2-1)+(1-s)} = (\Sigma c_i a_i^s)^{1-s}$$

Upon substituting in (2.9), we obtain:

$(\Sigma a_i b_i^s)^{s-1}(\Sigma b_i c_i^s)^s + (\Sigma c_i a_i^s)^{1-s}(\Sigma b_i c_i^s) = 0$, or:

$$(\alpha\beta\gamma)^{s-1} = -1 \text{ , where:} \tag{2.10}$$

$\alpha = \Sigma b_i c_i^s$; $\beta = \Sigma c_i a_i^s$; $\gamma = \Sigma a_i b_i^s$

On the other hand, by the noncollinearity of A, B, C, we have:

$$\Delta = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \neq 0 \tag{2.11}$$

We now evaluate Δ^{s+1} by using (2.10):

$$\Delta^{s+1} = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \begin{vmatrix} a_1^s & b_1^s & c_1^s \\ a_2^s & b_2^s & c_2^s \\ a_3^s & b_3^s & c_3^s \end{vmatrix} = \left| \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} \begin{pmatrix} a_1^s & b_1^s & c_1^s \\ a_2^s & b_2^s & c_2^s \\ a_3^s & b_3^s & c_3^s \end{pmatrix} \right|$$

$$= \begin{vmatrix} \Sigma a_i^{s+1} & \gamma & \beta^s \\ \gamma^s & \Sigma b_i^{s+1} & \alpha \\ \beta & \alpha^s & \Sigma c_i^{s+1} \end{vmatrix} = \begin{vmatrix} 0 & \gamma & \beta^s \\ \gamma^s & 0 & \alpha \\ \beta & \alpha^s & 0 \end{vmatrix} =$$

$$= \alpha^s\beta^s\gamma^s + \alpha\beta\gamma = 0 \ , \quad \text{by (2.10).}$$

This result contradicts (2.11) and we conclude that $M \not\in C$, QED.

This has also been proved, for example, in [16], p. 507.

Lemmas 2.1 - 2.5 can be summed up in the form of:

Theorem 2.1 For any prime power s , there exists a resolvable $(s^3 + 1, s + 1, 1)$ - BIBD, not containing any Pasch Configuration.

The only other known class of unitals has $s = 3^{2r+1}$ and they are obtained from groups of Ree ([12]). In addition, Hanani (in a private communication to Ray-Chaudhuri) has exhibited a unital with $s = 5$:

The base blocks are:

$\{(0, t^{6\alpha}), (0, t^{6\alpha+12}), (1, t^{6\alpha+1}), (1, t^{6\alpha+13}), (2, t^{6\alpha+3}), (2, t^{6\alpha+15})\}$

$\{(0, t^{6\alpha+2}), (0, t^{6\alpha+14}), (1, t^{6\alpha+4}), (1, t^{6\alpha+16}), (3, t^{6\alpha+11}), (3, t^{6\alpha+23})\}$

$\alpha = 0, 1$ and : $\{(0,0), (1,0), (2,0), (3,0), (4,0), \infty\}$

Here, t is a primitive root of GF(25), namely $t^2 + 3t + 3 = 0$ over GF(5). The first two base blocks must be developed cyclically, the first index mod 5 and the second over the additive group of GF(25). The last block must be developed over the additive group of GF(25), the second index only.

We will now give a construction which is similar to Hanani's and which in principle might be used to obtain a new class of unitals; however, we have only been able to actually carry it out for $s = 5$.

At this point some definitions are needed.

By a difference family modulo v , we mean a collection $\{E_1,$

$E_2, \ldots, E_n\}$ of sets of numbers such that $|E_i| = k_i$, $i = 1, 2, \ldots, n$ and the $\sum_{i=1}^{n} k_i(k_i - 1)$ differences of type $a - b$, where $\{a, b\}$ ranges through all ordered pairs from each E_i, constitute λ copies of a reduced residue system modulo v.

We must then have: $\sum_{i=1}^{n} k_i(k_i - 1) = \lambda(v - 1)$.

A <u>(v, k, λ) - perfect difference set</u> (or, for brevity, a <u>difference set</u>) is a difference family with only one member, say E, such that $|E| = k$. We have in this case: $k(k - 1) = \lambda(v - 1)$.

Difference families are often used for constructing BIBD's.

A <u>base</u> of a BIBD with parameters v, k, λ, with respect to an additive group G is a collection $\{E_1, E_2, \ldots, E_n\}$, where $E_i = \{e_{i1}, e_{i2}, \ldots, e_{ik}\}$ is called a <u>base block</u> (for $i = 1, 2, \ldots, n$) and such that the collection:

$\mathfrak{B} = \{E_i + j = \{e_{i1}+j, \ldots, e_{ik}+j\} : i = 1, 2, \ldots, n\}$ is the block family of the required BIBD.

Here, if $e_{im} = \infty$, then $e_{im} + j = e_{im} = \infty$ for any j.

A difference family with $k_i = k$ for all i and in particular a (v, k, λ) - difference set, forms a base of a BIBD with parameters v, k, λ, with respect to the additive group of residues modulo v ([10], p. 121).

If $GF_1, GF_2, \ldots, GF_m$ are m copies of a $GF(q)$ and $t_1, t_2, \ldots, t_m$ are the respective primitive roots (t_i satisfying the same irreducible equation, regardless of i), then the difference $t_i^a - t_j^b$ is called a <u>pure</u> or a <u>mixed difference</u>, according as $i = j$ or $i \neq j$. The actual value of this difference is understood to be simply $t^a - t^b$, where t is the primitive root of $GF(q)$ satisfying the given irreducible equation.

In constructing the block family of a BIBD from a given collection of base blocks, the expression $t_i^a + t^b$, where t_i is a primitive root of GF_i, will mean t_i^c, where $t^c = t^a + t^b$ in the

given GF(q). Similarly, $0_i + t^b = t_i^b$, where 0_i is the zero of GF_i.

The method used in constructing a new unital with $s = 5$ is a generalization of the following ([10], p. 234, Theorem 15.3.6):

Theorem 2.2 Let $4x + 1 = p^n$, p a prime and let t be a primitive root of $GF(p^n)$. Then there exists a pair of odd integers c, d, such that $(t^c + 1)/(t^c - 1) = t^d$. Then the blocks:

$\{t_1^{2i}, t_1^{2x+2i}, t_2^{2i+c}, t_2^{2x+2i+c}\}$;

$\{t_2^{2i}, t_2^{2x+2i}, t_3^{2i+c}, t_3^{2x+2i+c}\}$;

$\{t_3^{2i}, t_3^{2x+2i}, t_1^{2i+c}, t_1^{2x+2i+c}\}$; $i = 0, 1, \ldots, x - 1$;

$\{\infty, 0_1, 0_2, 0_3\}$ form a base with respect to the additive group of $GF(p^n)$, of a $(12x + 4, 4, 1)$ - BIBD.

For $x = 2$, these are the parameters of a unital ($s = 3$), which turns out to be different from the one provided by theorem 2.1.

One shortcoming of the method is that it is inapplicable to powers of 2; it will emerge clearly from the propositions given below that s has to be odd.

We proceed to the description of the method.

s will denote an odd prime power throughout the discussion.

Let $D = \{d_1, d_2, \ldots, d_{\frac{s-1}{2}}\}$ be the set of nonzero squares in GF(s) and $D' = \{d_1', d_2', \ldots, d_{\frac{s-1}{2}}'\}$ be the set of nonsquares.

Then the following result is known:

Lemma 2.6

a) If $s \equiv 3 \bmod 4$:

D and D' are perfect difference sets with parameters:

$$v = s \quad ; \quad k = \frac{s-1}{2} \quad ; \quad \lambda = \frac{s-3}{4}$$

$D \cup \{0\}$ and $D' \cup \{0\}$ are perfect difference sets with parameters:

$$v = s \quad ; \quad k = \frac{s+1}{2} \quad ; \quad \lambda = \frac{s+1}{4}$$

b) If $s \equiv 1 \bmod 4$:

The differences from D are: each square, $\frac{s-5}{4}$ times, and each

nonsquare, $\frac{s-1}{4}$ times;

The differences from $D \cup \{0\}$ are: each square, $\frac{s+3}{4}$ times, and each nonsquare, $\frac{s-1}{4}$ times;

The differences from D' are: each square, $\frac{s-1}{4}$ times, and each nonsquare, $\frac{s-5}{4}$ times;

The differences from $D' \cup \{0\}$ are: each square, $\frac{s-1}{4}$ times, and each nonsquare, $\frac{s+3}{4}$ times.

Proof a) This is Theorem 8.3, p. 89, [14].

b) This part is a rephrasing of Lemma 6(a), p. 30, [17].

Corollary 2.1

a) If $s \equiv 3 \bmod 4$:

D, $D \cup \{0\}$ and $\{D \cup \{0\}, D' \cup \{\infty\}\}$ are bases with respect to the additive group of $GF(s)$, of BIBD's with the following parameters:

$$v = s \quad ; \quad k = \frac{s-1}{2} \quad ; \quad \lambda = \frac{s-3}{4} \quad ,$$

$$v = s \quad ; \quad k = \frac{s+1}{2} \quad ; \quad \lambda = \frac{s+1}{4} \quad ,$$

$$v = s+1 \quad ; \quad k = \frac{s+1}{2} \quad ; \quad \lambda = \frac{s-1}{2} \quad , \text{ respectively.}$$

The same holds if we interchange D and D'.

b) If $s \equiv 1 \bmod 2$:

$\{D, D'\}$, $\{D \cup \{0\}, D' \cup \{0\}\}$ and $\{D \cup \{0\}, D \cup \{\infty\}\}$ are bases of BIBD's with the following parameters:

$$v = s \quad ; \quad k = \frac{s-1}{2} \quad ; \quad \lambda = \frac{s-3}{2} \quad ,$$

$$v = s \quad ; \quad k = \frac{s+1}{2} \quad ; \quad \lambda = \frac{s+1}{2} \quad ,$$

$$v = s+1 \quad ; \quad k = \frac{s+1}{2} \quad ; \quad \lambda = \frac{s-1}{2} \quad , \text{ respectively.}$$

The same holds if we interchange D and D'.

The proof relies entirely on Lemma 2.6 and is straightforward.

Let now t be a primitive root of $GF(s^2)$ and let us denote:

$$D_j = \{t^{j+k(s+1)} : k = 0, 1, \ldots, s-2\} \quad \text{for } j = o, 1, \ldots, s.$$

When we require several copies of $GF(s^2)$ we will let t_i be a primitive root of the i-th copy and 0_i, the corresponding zero, We also let:

$$(2.12)\quad D_{ji} = \{t_i^{j+k(s+1)} : k = 0, 1, \ldots, s-2\} \quad \text{for } j = 0, 1, \ldots, s.$$

Let Z_s and Z_{s+1} be complete residue systems modulo s, $s+1$, respectively, and let (i, j) be the elements of the cartesian product $Z_s \times Z_{s+1}$, $i = 0, 1, \ldots, s-1$; $j = 0, 1, \ldots, s$.

Theorem 2.3 If there exists a configuration $\mathcal{K}_s$ on the set $Z_s \times Z_{s+1}$, consisting of $2s$ blocks, each having cardinality $(s+1)/2$ and such that:

i) The configuration induced by $\mathcal{K}_s$ on Z_s is a BIBD with parameters $v = s$; $k = \lambda = \frac{s+1}{2}$;

ii) Each pair $(i, j) \in Z_s \times Z_{s+1}$ is represented in a (necessarily unique) block of $\mathcal{K}_s$;

iii) For each fixed i, $k \in Z_s$ and each pair $\{(i, j), (k, h)\}$ occurring in a block of $\mathcal{K}_s$, no two of $s+1$ numbers $t^j \pm t^h$ belong to the same D_j $(j = 0, 1, \ldots, s)$, where j and h are two fixed representatives of their residue classes mod $s+1$,

then we can obtain a resolvable unital by replacing each block $\{(i_1, j_1), (i_2, j_2), \ldots, (i_{\frac{s+1}{2}}, j_{\frac{s+1}{2}})\}$ of $\mathcal{K}_s$ by $(s-1)/2$ blocks of type:

$$(2.13)\quad \{t_{i_1}^{j_1+m(s+1)}, -t_{i_1}^{j_1+m(s+1)}, \ldots, t_{i_{(s+1)/2}}^{j_{(s+1)/2}+m(s+1)}, -t_{i_{(s+1)/2}}^{j_{(s+1)/2}+m(s+1)}\},$$

$m = 0, 1, \ldots, \frac{s-3}{2}$.

These blocks, together with $\{\infty, 0_o, 0_1, \ldots, 0_{s-1}\}$ form a base

with respect to the additive group of $GF(s^2)$, of a resolvable unital on the set $GF_o \cup GF_1 \cup \ldots \cup GF_{s-1} \cup \{\infty\}$, the GF_i's being copies of $GF(s^2)$.

Proof A necessary and sufficient condition for a given family to be the family of base blocks of a BIBD with respect to the additive group of $GF(q)$ is that the given family yield all nonzero pure differences and all mixed differences, λ times each. ([10], p. 232).

Hence we have to verify that the given family of subsets yields all the appropriate differences, once each.

We first observe that for each fixed i, each pair of type:

(2.14) $\{t_i^{j+m(s+1)}, -t_i^{j+m(s+1)}\}$, where $m = 0, 1, \ldots, \frac{s-3}{2}$ and

j ranges through Z_{s+1}, appears exactly once in the base blocks (2.13). This follows from ii).

The pairs (2.14) give rise to pure differences $\pm 2t_i^{j+m(s+1)}$; if j is also fixed, these differences are:

(2.15) $\pm 2t_i^{j}$, $\pm 2t_i^{j+s+1}$, $\ldots$, $\pm 2t_i^{j+((s-3)/2)(s+1)}$.

But in $GF(s^2)$ we have $2 = t_i^{w(s+1)}$ for some integral w, so that (2.15) becomes:

(2.16) $\pm t_i^{j+w(s+1)}$, $\pm t_i^{j+(w+1)(s+1)}$, $\ldots$, $\pm t_i^{j+[w+(s-3)/2](s+1)}$.

(2.16) is precisely D_{ji} as defined in (2.12) because:

$$-1 = t_i^{[(s-1)/2](s+1)}$$

Hence all nonzero pure differences occur exactly once.

To check the mixed differences, we fix i and k $(i \neq k)$ in Z_s.

Each base block (2.13) yields four differences involving i and k, namely:

(2.17) $\pm t_i^{j+m(s+1)} \quad \pm t_k^{h+m(s+1)} \quad (m = 0, 1, \ldots, \frac{s-3}{2})$, for each

$j, h \in Z_{s+1}$ such that (i, j), (k, h) occur together in a block of $\mathcal{H}_s$.

If j, h are fixed, the numbers $\pm[t^{j+m(s+1)} + t^{h+m(s+1)}]$ and $\pm[t^{j+m(s+1)} - t^{h+m(s+1)}]$ constitute D_r and D_u for some $r \neq u$, if we let $m = 0, 1, \ldots, (s - 3)/2$.

Combining this with iii) shows that all nonzero mixed differences occur once.

As regards the zero mixed differences, the base block $\{\infty, 0_o, 0_1, \ldots, 0_{s-1}\}$ takes care of them.

The same block shows that all pairs involving ∞ appear once.

Resolvability follows immediately from the fact that the base blocks constitute a complete replication, QED.

Theorem 2.4 For $s = 3$ and 5, there exist resolvable unitals which contain the Pasch Configuration, thereby being nonisomorphic to the unitals of theorem 2.1.

Proof For $s = 3$ theorem 2.3 gives the same construction as theorem 2.2. It is an easy check that the conditions of theorem 2.3 are satisfied in this case. We have also found out by inspection that these unitals contain the Pasch Configuration.

For $s = 5$ one may construct a unital in the following manner:

Let t be a primitive root of GF(25), satisfying:

(2.18) $$t^2 + t + 2 = 0 \quad \text{over GF(5)}.$$

We construct the configuration $\mathcal{K}_5$ on $Z_5 \times Z_6$ as follows:

(2.19)

B1: $\{(0,2), (1,6), (4,1)\}$ B6: $\{(0,3), (2,1), (3,6)\}$

B2: $\{(1,8), (2,3), (0,4)\}$ B7: $\{(1,1), (3,4), (4,3)\}$

B3: $\{(2,2), (3,1), (1,11)\}$ B8: $\{(2,4), (4,11), (0,1)\}$

B4: $\{(3,2), (4,10), (2,6)\}$ B9: $\{(3,5), (0,6), (1,10)\}$

B5: $\{(4,8), (0,5), (3,3)\}$ B10: $\{(4,6), (1,3), (2,5)\}$

$\mathcal{K}_5$ induces on Z_5 a (5, 3, 3) - BIBD, as required by theorem 2.3 i).

Condition ii) is easy to check.

Condition iii) must be checked for all pairs $i, k \in Z_5$.

As an illustration we will check the pair $i = 0$, $k = 1$.

According to (2.19), we have to evaluate the following, where t is given by (2.18):

$$t^2 + t^6 = t^{13} \in D_1 \qquad t^6 - t^{10} = t^2 \in D_2$$

$$t^2 - t^6 = t^{22} \in D_4 \qquad t^4 + t^8 = t^{15} \in D_3$$

$$t^6 + t^{10} = t^{17} \in D_5 \qquad t^4 - t^8 = t^{24} \in D_o$$

We check all pairs in the same fashion.

Hence all the conditions of theorem 2.3 have been satisfied.

The Pasch Configuration can be obtained, for example, in the following manner:

The blocks B1, B2, B4, B8 (see (2.19)) of $\mathcal{H}_5$ respectively, give rise, among other base blocks of the unital, to the following (see (2.13)):

$$C1: \{t_o^2, -t_o^2, t_1^6, -t_1^6, t_4^1, -t_4^1\} \quad (\text{for } m = 0)$$

$$C2: \{t_1^8, -t_1^8, t_2^3, -t_2^3, t_o^4, -t_o^4\} \quad (\text{for } m = 0)$$

$$C4: \{t_3^8, -t_3^8, t_4^{16}, -t_4^{16}, t_2^{12}, -t_2^{12}\} \quad (\text{for } m = 1)$$

$$C8: \{t_2^{10}, -t_2^{10}, t_4^{17}, -t_4^{17}, t_o^7, -t_o^7\} \quad (\text{for } m = 1)$$

Here, all t_i's satisfy (2.18).

We now add: 0, t^{19}, t^3, t^{15}, to C1, C2, C4, C8, respectively, thereby obtaining the blocks in fig. 2, which obviously contain the Pasch Configuration.

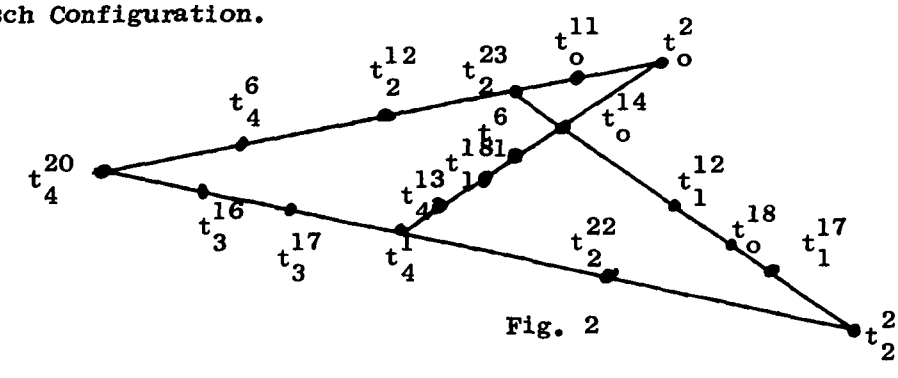

Fig. 2

This completes the proof, QED.

We note the following facts concerning $\mathcal{K}_5$ (2.19):

Obs. 1 $\mathcal{K}_5$ induces on Z_6 a BIBD with parameters $v = 6$, $k = 3$, $\lambda = 2$, which is precisely the third BIBD given by Corollary 2.1 b (for $s = 5$).

Obs. 2 For each fixed i, $k \in Z_5$, if we consider the three pairs of type:

$$\{(i,j_1), (k,h_1)\} \; ; \; \{(i,j_2), (k,h_2)\} \; ; \; \{(i,j_3), (k,h_3)\} \; ,$$

we have:

$$h_1 \equiv j_2 \quad , \quad h_2 \equiv j_3 \quad , \quad h_3 \equiv j_1 \quad \text{modulo } 6 \; .$$

Neither of these two facts is required by theorem 2.3, though.

On the other hand, the BIBD required by theorem 2.3 i), as well as a $(s + 1, \frac{s+1}{2}, \frac{s-1}{2})$ - BIBD, exist for any odd prime power s.

Based on these facts, we have been trying to obtain a general method whereby unitals could be gotten for any odd prime power s, so far unsuccessfully, though.

While lemma 2.6 and corollary 2.1 might make it possible to satisfy i) and ii) for any s, condition iii) however, turns out to be difficult to satisfy.

*

We shall now show that the existence of a resolvable unital for some prime power s leads to the existence of a resolvable BIBD with parameters $v = s^{2t+1} + 1$, $k = s + 1$, $\lambda = 1$, for any $t \geq 0$. This will exhaust the problem of constructing the type II matroid designs (see Chapter I).

We shall prove a more general statement:

Theorem 2.5 If there exists a resolvable $(w, u, 1)$ - BIBD and a resolvable $(nu + 1, n + 1, 1)$ - BIBD, then there exists a resolvable $(nw + 1, n + 1, 1)$ - BIBD.

Proof Aside from resolvability, this has been proved in [11], prop. 3.10, p. 365.

Proving resolvability:

Let $A = \{z\} \cup \left(\bigcup_{i=1}^{n} E_i \right)$, where $|E_i| = w$, $i = 1, 2, \ldots, n$

and $E_i \cap E_j = \emptyset$ for $i \neq j$, $z \notin E_i$ for any i, so that $|A| = nw + 1$.

We introduce the following notations:

$$\frac{w - 1}{u - 1} = r \quad ; \quad \frac{w}{u} = s \quad ; \quad \frac{nu + 1}{n + 1} = t$$

Let the block family of a resolvable $(w, u, 1)$ - BIBD on E_i be $\mathcal{B}_i$. By resolvability:

$\mathcal{B}_i = \bigcup_{j=1}^{r} \mathcal{B}_{ij}$, where $\mathcal{B}_{ij}$ are the parallel classes of blocks:

$$\mathcal{B}_{ij} = \{B_{ij}^1, B_{ij}^2, \ldots, B_{ij}^s\} \quad \text{and:}$$

(2.20) $$|B_{ij}^k| = u \quad \text{for all } i, j, k. \quad \text{Also:}$$

(2.21) $$\bigcup_{k=1}^{s} B_{ij}^k = E_i \quad \text{for all } j.$$

Consider the set $F_j^k = \{z\} \cup \left(\bigcup_{i=1}^{n} B_{ij}^k \right)$ for $j = 1, 2, \ldots, r$.

$$|F_j^k| = nu + 1 \quad \text{, by (2.20).}$$

We construct now on each F_j^k a resolvable $(nu + 1, n + 1, 1)$ - BIBD with block family C_j^k, in such a way that for any i, j, k:

(2.22) $$|C \cap B_{ij}^k| = 1 \quad \text{for any } C \in C_j^k \text{ such that } z \in C.$$

If $\mathfrak{D}_j^k$ is the subfamily of C_j^k consisting of all blocks containing z, then $\bigcup_{k=1}^{s} \mathfrak{D}_j^k$ can be made to be the same collection of blocks, regardless of j. This can be achieved by virtue of (2.21).

By resolvability, $C_j^k = \bigcup_{h=1}^{u} C_{jh}^k$, where C_{jh}^k are the parallel classes of blocks.

Now for any block C such that $z \in C$ and any fixed j there exists a unique k such that $C \in C_j^k$ and since for any fixed j, k and any $C \in C_j^k$ there exists a unique h such that $C \in C_{jh}^k$, we see that:

For any C such that $z \in C$ and any fixed j there is a unique pair k, h, such that:

(2.23) $$C \in C_{jh}^{k}$$

We now obtain the parallel classes of the required design on A as follows: we choose a block C such that $z \in C$, then determine for each j the unique k and h such that (2.23) holds and consider:

$$\mathfrak{P}_C = \bigcup_{j=1}^{r} C_{jh}^{k}$$

Claim: $\mathfrak{P}_C$ is a parallel class of blocks of the BIBD on A.

To prove this, we observe that for any fixed j, the blocks in $C_{jh}^{k} \subset \mathfrak{P}_C$ contain all points of F_j^k, each once. For a different j, say j', the blocks in $C_{j'h'}^{k'} \subset \mathfrak{P}_C$ account for all points of $F_{j'}^{k'}$, each once.

But $F_j^k \cap F_{j'}^{k'} = C$ and it follows that the blocks in $\mathfrak{P}_C$ account for the following number of different points of A:

$$r(|F_j^k| - |C|) + |C| = r(nu + 1 - n - 1) + n + 1 = nw + 1 \quad ,$$

i.e. all points of A, QED.

Corollary 2.2 Where s is any prime power, there exist resolvable $(s^{2t+1} + 1, s + 1, 1)$ - BIBD's for any $t \geq 0$.

Proof There exist resolvable $(s^3 + 1, s + 1, 1)$ - BIBD's, by theorem 2.1. Also, there exist resolvable $(s^{2t}, s^2, 1)$ - BIBD's, $AG(t, s^2)$ being such a design.

Apply now theorem 2.5 with $w = s^{2t}$, $u = s^2$, $n = s$, to obtain the desired BIBD, QED.

CHAPTER III

TRANSVERSAL DESIGNS

We have seen in Chapter I that rank 3 matroid designs of prime power index may be described entirely in terms of a certain class of TD_2's, namely those with parameters of type $v = p^{(2t+1)m} + 1$, $s = p^h$, $k = p^m + 1$, $\lambda = 1$, where $0 \leq h \leq m$.

In chapter II we showed that these always exist when $h = 0$, i.e. when the TD_2 reduces to a BIBD.

In this chapter we shall show that TD_2's with the above parameters always exist when $h = m$. In the latter case, we have the type III matroid designs, consisting essentially of $(1 + p^m + p^{(2t+2)m}, 1 + p^m, 1)$ - BIBD's or $(1 + q + q^{2t+2}, 1 + q, 1)$ - BIBD's.

We shall actually show the existence of a much larger series of TD_2's that contain the above mentioned classes of BIBD's as special cases. In addition, we shall present a number of results about transversal designs that are interesting in themselves.

The TD_t's with $t = 2$ are of particular interest and they appear often in the literature. They have been used by Hanani as an essential tool in constructing BIBD's with $k = 3$, 4 and 5 ([11] , [12]), besides their use in the design of experiments ([5]).

In using them, however, various authors name them in different ways.

In [11], a <u>T - system</u> is a special case of a TD_2 , namely a TD_2 with $v = k$, $t = 2$, $\lambda = 1$.

In [12], p. 185, the notion of a <u>group divisible design</u> (GD design) is introduced. According to this definition, a GD design is a special case of a TD_t , namely with $t = 2$.

In [20], p. 228, a GD design is defined as a more general incidence structure, where $t = 2$, but neither the groups nor the blocks need be equicardinal. According to [20], what we have called a TD_2 is a uniform group divisible design with equicardinal blocks.

In [5], p. 602, a group divisible design is defined as a particular case of a Partially Balanced Incomplete Block Design (PBIBD) with two associate classes.

A PBIBD was first defined in[2] (see also [3], p. 367):

Definition 3.1 Let a v - set be given, together with an association scheme defined as follows:

a) Any two elements of E are i-th associates, $i = 1, 2, \ldots, m$, the relation of association being symmetrical.

b) Each element has n_i i-th associates.

c) For any pair of elements which are i-th associates, the number of elements which are j-th associates of one and k-th associates of the other is p^i_{jk} $(j, k = 1, 2, \ldots, m)$ and is independent of the pair of i-th associates with which we start (in particular, $p^i_{jk} = p^i_{kj}$).

Given the set E with an association scheme defined on it, a PBIBD on E consists of a collection $\mathfrak{B}$ of subsets of E, called blocks ($|\mathfrak{B}| = b$), each block containing k elements of E and such that:

1) Any element in E occurs r times in the blocks of $\mathfrak{B}$;

2) If $a, b \in E$ are i-th associates, the pair $\{a, b\}$ appears in λ_i blocks.

Connor then defines a GD design on a set E:

Definition 3.2 A GD design is a PBIBD with two associate classes and such that:

i) The relation "a is either i-th associate or identical with b" is an equivalence relation among the elements of E for $i = 1$ or 2 but not both.

ii) $\lambda_1 \neq \lambda_2$.

It is apparent that TD_2's , as defined in chapter I, are GD designs with $\lambda_i = 0$ $(i = 1 \text{ or } 2)$.

In the sequel we will be concerned with transversal designs only. We will use the notion of "transversal design" throughout, and the corresponding notations, too. Thus we want to emphasize the difference between GD designs as defined in Def. 3.2 and the TD_2's defined in Chapter I.

*

A TD_t with $v = k$ is called a full TD_t. The number of blocks in a full TD_2 is, by (1.25):

$$b = \lambda s^2$$

The next theorem represents known properties of TD_2's (see, for ex., [10].

Theorem 3.1 The following statements are equivalent:

i) There exists a $TD_2(n + 1, n, n + 1, 1)$.

ii) There exists an orthogonal array of order n and depth $n + 1$.

iii) There exists a $PG(2, n)$.

iv) There exists a complete set of mutually orthogonal Latin squares of order n.

Theorems 3.2 - 3.5 are "composition theorems", enabling one to obtain new TD's from known ones.

Theorem 3.2 If there exists a $TD_t(w, s', v, \lambda')$ and a $TD_t(v, s, k, \lambda)$, then there exists a $TD_t(w, ss', k, \lambda\lambda')$. Moreover, resolvability of the first two designs entails resolvability of the last.

Proof The first statement is a slight modification of ([21], p. 30, (133)). As for the second statement, that is a straightforward consequence of the method of construction, QED.

Theorem 3.3 If there exists a $TD_2(w + 1, s, k, \lambda)$ and a $TD_2(v, sw, k, \lambda)$, then there exists a $TD_2(vw + 1, s, k, \lambda)$.

Proof Let E be an $s(vw + 1)$ - set partitioned by the

collection $\mathcal{S} = \{S_1, S_2, \ldots, S_{vw+1}\}$, where $|S_h| = s$ for $h = 1, 2, \ldots, vw + 1$.

To obtain the required TD_2 , we first construct for $i = 1, 2, \ldots, v$, a design $(E_i, \mathcal{S}_i, \mathcal{J}_i) \equiv TD_2(w + 1, s, k, \lambda)$, where:

$$\mathcal{S}_i = \{S_{(i-1)w+j} : j = 1, 2, \ldots, w\} \cup \{S_{vw+1}\} \quad \text{and} \quad E_i = \bigcup_{S_h \in \mathcal{S}_i} S_h .$$

Let now $F_i = \bigcup_{j=1}^{w} S_{(i-1)w+j}$, $i = 1, 2, \ldots, v$; $|F_i| = sw$ for all i.

We construct an $(E - S_{vw+1}, \mathcal{F}, \mathcal{J}) \equiv TD_2(v, sw, k, \lambda)$, where $\mathcal{F} = \{F_1, F_2, \ldots, F_v\}$.

Now, $(E, \mathcal{S}, \bigcup_{i=1}^{v} \mathcal{J}_i \cup \mathcal{J})$ is the desired $TD_2(vw + 1, s, k, \lambda)$, QED.

Theorem 3.4 If there exists a $TD_2(w, ss', k, \lambda)$ and a $TD_2(s', s, k, \lambda)$, then there exists a $TD_2(ws', s, k, \lambda)$.

Proof Let E be a $ws's$ - set partitioned by the collection $\mathcal{S} = \{S_1, S_2, \ldots S_{ws'}\}$, where $|S_h| = s$ for $h = 1, 2, \ldots, ws'$.

We construct an $(E, \mathcal{S}', \mathcal{J}) \equiv TD_2(w, ss', k, \lambda)$, where:

$$\mathcal{S}' = \{ \bigcup_{j=0}^{s'-1} S_{i+jw} : i = 1, 2, \ldots, w\}$$

Next, for each $i = 1, 2, \ldots, w$, we construct an $(E_i, \mathcal{S}_i, \mathcal{J}_i) \equiv TD_2(s', s, k, \lambda)$, where $\mathcal{S}_i = \{S_i, S_{i+w}, \ldots, S_{i+(s'-1)w}\}$ and $E_i = \bigcup_{S_h \in \mathcal{S}_i} S_h$.

Then $(E, \mathcal{S}, \bigcup_{i=1}^{w} \mathcal{J}_i \cup \mathcal{J})$ is the required $TD_2(ws', s, k, \lambda)$, QED.

Theorem 3.5 If the following TD_2's exist:

$TD_2(w + 1, s, k, \lambda\lambda')$;

$TD_2(n, w, k', \lambda)$, resolvable ;

$TD_2(k' + 1, s, k, \lambda')$;

$TD_2(v + 1, s, k, \lambda\lambda')$, where $v = \frac{(n - 1)w}{k' - 1}$, then there exists a $TD_2(nw + v + 1, s, k, \lambda\lambda')$.

Proof Let E be an $s(nw + v + 1)$ - set, partitioned by the collection $\mathcal{S} = \{S_1, S_2, \ldots, S_{nw+v+1}\}$, where $|S_h| = s$ for $h = 1, 2, \ldots, nw + v + 1$.

First, for each $r = 1, 2, \ldots, n$, we let $(E_r, \mathcal{S}_r, \mathcal{J}_r)$ be a $TD_2(w + 1, s, k, \lambda\lambda')$, where:

$$\mathcal{S}_r = \{S_{(r-1)w+j} : j = 1, 2, \ldots, w\} \cup \{S_{nw+v+1}\} \quad \text{and}$$

$$E_r = \bigcup_{S_h \in \mathcal{S}_r} S_h .$$

Let now $F_r = \{S_{(r-1)w+j} : j = 1, 2, \ldots, w\}$, $r = 1, 2, \ldots, n$ and $F = \bigcup_{r=1}^{n} F_r$. Let also $\mathcal{F} = \{F_1, F_2, \ldots, F_n\}$.

We let $(F, \mathcal{F}, \mathcal{J})$ be a resolvable $TD_2(n , w, k', \lambda)$.

Then $b = |\mathcal{J}| = \frac{\lambda n(n - 1)w^2}{k'(k' - 1)}$, by (1.25).

Each parallel class of blocks consists of nw/k' blocks, so that there are $bk'/nw = \frac{\lambda(n - 1)w}{k' - 1} = \lambda v$ parallel classes:

$$\mathcal{J} = \bigcup_{m=1}^{\lambda v} \mathcal{J}'_m \quad , \quad \mathcal{J}'_m \text{ being the parallel classes.}$$

$$\mathcal{J}'_m = \{T_{m1}, T_{m2}, \ldots, T_{m,nw/k'}\}.$$

Now for each $i = 1, 2, \ldots, \lambda$; $j = 1, 2, \ldots, nw/k'$; $h = 1, 2, \ldots, v$, let us construct a $(G_{ijh}, \mathcal{G}_{ijh}, \mathcal{J}_{ijh}) \equiv TD_2(k' + 1, s, k, \lambda')$, where:

$$\mathcal{G}_{ijh} = T_{i+(h-1)\lambda, j} \cup \{S_{nw+h}\} \quad \text{and} \quad G_{ijh} = \bigcup_{S_u \in \mathcal{G}_{ijh}} S_u .$$

Lastly, we construct a $(U, \mathcal{S}', \mathcal{U}) \equiv TD_2(v + 1, s, k, \lambda\lambda')$, where:

$\mathcal{S}' = \{S_{nw+1}, S_{nw+2}, \ldots, S_{nw+v+1}\}$ and $U = \bigcup_{S_h \in \mathcal{S}'} S_h$.

Then $(E, \mathcal{S}, \bigcup_{r=1}^{n} \mathcal{T}_r \cup (\bigcup_{i=1}^{\lambda} \bigcup_{j=1}^{nw/k'} \bigcup_{h=1}^{v} \mathcal{T}_{ijh}) \cup U)$ is the required $TD_2(nw + v + 1, s, k, \lambda\lambda')$, QED.

We proceed now to the construction of the class of $(1 + q + q^{2t+2}, 1 + q, 1)$ - BIBD's. It turns out that these BIBD's are particular instances of a large class of TD_2's. More precisely, we shall prove that the following theorem holds:

Theorem 3.6 For any prime power q,

$TD_2(q^{n_o} + q^{n_1} + \ldots + q^{n_r}, q^h, 1 + q, 1)$ exists, where:

(a) $n_i \equiv i \bmod 2$, $i = 0, 1, \ldots, r$;

(b) $n_o < n_1 < \ldots < n_r$;

(c) $h = 0$ implies $n_o = 0$ and $n_o = 0$ implies $r \geq 1$.

For the proof we need several lemmas.

Lemma 3.1 Where q is a prime power, $TD_2(v, q, v, q^{n-2})$ exists for any $n \geq 2$ and any $v \leq (q^n-1)/(q-1)$.

Proof It suffices to prove the lemma for $v = (q^n-1)/(q-1)$, for then, for any smaller v we simply delete the superfluous elements from all blocks.

In $PG(n, q)$ over $GF(q)$ with hyperplane family $\mathcal{H}$ and line family $\mathcal{L}$, consider a point α and let:

$E = PG(n, q) - \{\alpha\}$

$\mathcal{S} = \{L - \{\alpha\} : L \in \mathcal{L}, \alpha \in L\}$

$\mathcal{T} = \{H : H \in \mathcal{H}, \alpha \notin H\}$

The triple $(E, \mathcal{S}, \mathcal{T})$ is the desired design.

To prove this, we note that α is on $(q^n-1)/(q-1)$ lines, whence:

$$v = |\mathcal{S}| = (q^n-1)/(q-1) .$$

Then no line containing a meets any hyperplane not containing a in more than one point; hence no two points $b, c \in S \in \mathcal{S}$ occur in the same block.

Now let b, c be two points not collinear with a. b and c occur together in $(q^{n-1} - 1)/(q - 1)$ hyperplanes. Of these, the $(q^{n-2} - 1)/(q - 1)$ hyperplanes containing the two - dimensional subspace generated by the triangle $\{a, b, c\}$ are not members of $\mathcal{I}$.

Hence $$\lambda = \frac{q^{n-1} - 1}{q - 1} - \frac{q^{n-2} - 1}{q - 1} = q^{n-2}$$

This completes the proof, QED.

Lemma 3.1 generalizes a construction in [4], p. 183.

At this point, a further definition is needed.

Definition 3.3 A (v, k, λ) - BIBD on a set E is called Centrally resolvable if there is an element $a \in E$ such that:

$E - \{a\} = \bigcup_{i=1}^{\frac{v-1}{k-1}} E_i$, where $|E_i| = k - 1$ for all i, the E_i's are mutually disjoint and the sets $E_i \cup \{a\}$ appear as blocks in the design, each λ times, for all i.

Lemma 3.2 The existence of a centrally resolvable (v, k, λ) - BIBD is equivalent to the existence of a $TD_2(\frac{v - 1}{k - 1}, k - 1, k, \lambda)$.

Proof Given the centrally resolvable BIBD on E, delete the element a which meets the condition of definition 3.3, and all blocks containing it. The remaining blocks are the block family of the desired TD_2.

The converse is now obvious, QED.

Since any BIBD with $\lambda = 1$ is centrally resolvable, we have the following:

Corollary 3.1 The existence of a $(v, k, 1)$ - BIBD is equivalent to the existence of a $TD_2(\frac{v - 1}{k - 1}, k - 1, k, 1)$.

Lemma 3.3 Where q is a prime power, $TD_2(q^m, q^n, q + 1, 1)$ exists for any $n \geq 1$ iff $m \geq 2$ and m is even.

Proof

$$b = \frac{q^m(q^m - 1)q^{2n}}{(q + 1)q} \quad , \text{ which is integral iff } m \text{ is even.}$$

Let $m = 2h$, $h \geq 1$.

The proof is by induction on $n \geq 1$.

A $(q^{2h+1} + 1, q + 1, 1)$ - BIBD exists by corollary 2.2. By corollary 3.1, this is equivalent to a $TD_2(q^{2h}, q , q + 1 , 1)$.

Hence the lemma holds for $n = 1$.

Assume that $TD_2(q^{2h}, q^n, q + 1, 1)$ exists for some n.

Lemma 3.1, for $n = 2$, supplies a $TD_2(q + 1, q, q +1, 1)$. We apply now theorem 3.2 with:

$w = q^{2h}$, $s' = q^n$, $v = k = q + 1$, $\lambda = \lambda' = 1$, $s = q$,

to obtain $TD_2(q^{2h}, q^{n+1}, q + 1, 1)$. This completes the induction, QED.

We are prepared now to prove theorem 3.6.

Proof of Theorem 3.6 The replication number of the desired TD_2 is, by (1.26):

$$r = \frac{q^{n_o} + \ldots + q^{n_r} - 1)q^h}{q}$$

Thus, $h = 0$ implies $n_o = 0$.

If $n_o = 0 = r$, we get a $TD_2(1, q^h, q + 1, 1)$ which cannot exist. Hence $n_o = 0$ implies $r \geq 1$.

Let first $n_o = 0$; we then have to construct a $TD_2(1 + q^{n_1} + \ldots q^{n_r}, q^h, q + 1, 1)$, where $h \geq 0$ and $r \geq 1$.

$TD_2(1 + q^{n_1}, 1, q + 1, 1)$ is a $(1 + q^{n_1}, q + 1, 1)$ - BIBD and therefore exists by corollary 2.2, iff $n_1 \equiv 1 \bmod 2$.

$TD_2(q + 1, q^h, q + 1, 1)$ exists also: if $h = 0$ it is a trivial BIBD and if $h > 0$, we substitute q^h for q in lemma 3.1,

then let $n = 2$ and $v = q + 1$.

We apply now theorem 3.2 with:

$w = 1 + q^{n_1}$, $v = k = q + 1$, $s' = \lambda = \lambda' = 1$, $s = q^h$,

to get a $TD_2(1 + q^{n_1}, q^h, q + 1, 1)$ for $h \geq 0$.

Hence the theorem holds for $n_o = 0$, $h \geq 0$ and $r = 1$.

Assume that it holds for $n_o = 0$, $h \geq 0$ and some fixed $r \geq 1$, i.e. $TD_2(1 + q^{n_1} + \ldots + q^{n_r}, q^h, q + 1, 1)$ exists , where $n_1 < n_2 < \ldots < n_r$.

Let us use theorem 3.3 with:

$w = q^{n_1}$, $v = 1 + q^{n_2 - n_1} + \ldots + q^{n_{r+1} - n_1}$, $s = q^h$, $k = q + 1$,

$\lambda = 1$, where $n_1 < n_2 < \ldots < n_{r+1}$.

$TD_2(w + 1, s, k, \lambda)$ is $TD_2(q^{n_1} + 1, q^h, q + 1, 1)$ and has been obtained before.

$TD_2(v, sw, k, \lambda)$ is $TD_2(1 + q^{n_2 - n_1} + \ldots + q^{n_{r+1} - n_1}, q^{h+n_1}, q + 1, 1)$ and exists by assumption, since $0 < n_2 - n_1 < \ldots < n_{r+1} - n_1$ and $n_i - n_1 \equiv i - 1 \bmod 2$ for $i = 2, 3, \ldots, r + 1$.

Hence $TD_2(vw + 1, s, k, \lambda)$ exists; but this is:

$TD_2(1 + q^{n_1} + \ldots + q^{n_{r+1}}, q^h, q + 1, 1)$, hence the theorem is valid for $r + 1$, which completes the induction.

Therefore we have disposed of the case $n_o = 0$, $h \geq 0$, $r \geq 1$.

We now turn to the case $n_o \neq 0$.

If $n_o \neq 0$, $h \neq 0$ either, for $h = 0$ implies $n_o = 0$.

If now $r = 0$, the theorem reduces to lemma 3.3, so we can assume $r \geq 1$.

We apply now theorem 3.4 with:

$w = 1 + q^{n_1 - n_o} + \ldots + q^{n_r - n_o}$, $s = q^h$, $s' = q^{n_o}$, $k = q + 1$, $\lambda = 1$.

The hypotheses of theorem 3.4 are satisfied:

$TD_2(w, ss', k, \lambda)$ is $TD_2(1 + q^{n_1-n_o} + \ldots + q^{n_r-n_o}, q^{h+n_o}, q + 1, 1)$, which has already been shown to exist since $n_i - n_o \equiv i \bmod 2$ for $i = 1, 2, \ldots, r$.

$TD_2(s', s, k, \lambda)$ is $TD_2(q^{n_o}, q^h, q + 1, 1)$, which exists by lemma 3.3.

Therefore $TD_2(ws', s, k, \lambda)$ exists. But this is precisely the required design, QED.

Corollary 3.2 $(1 + q + q^{2t+2}, 1 + q, 1)$ - BIBD exists for any prime power q and any $t \geq 0$.

Proof Apply theorem 3.6 with $h = n_o = 0$, $n_1 = 1$, $n_2 = 2t + 2$, QED.

This solves the problem of the type III matroids in $\mathfrak{M}_3(p^n)$.

Another immediate consequence of theorem 3.6 which is worth mentioning, is the following:

Corollary 3.3 For any prime power q there exists a $(1 + q^{n_1} + q^{n_2} + \ldots + q^{n_r}, q + 1, 1)$ - BIBD, where $r \geq 1$, $n_i \equiv i \bmod 2$ $(i = 1, 2, \ldots, r)$ and $n_1 < n_2 < \ldots < n_r$.

PG(r, q) is clearly obtained as a particular case of the last BIBD's, when $n_i = i$, $i = 1, 2, \ldots, r$.

*

We shall conclude by considering several other classes of TD_2's of general interest which, however, do not appear to be connected with the construction of matroid designs.

We first note the following:

Theorem 3.7 $TD_2(q + 1, q - 1, q, 1)$ exists for any prime power q.

Proof Let E be a $(q^2 - 1)$ - set partitioned by the family $\mathcal{S} = \{S_1, S_2, \ldots, S_{q+1}\}$, where $|S_h| = q - 1$ for $h = 1, 2, \ldots, q + 1$.

Let $z \notin E$ and construct an AG(2, q) on $E \cup \{z\}$ in such a

way that the lines containing z are $S_h \cup \{z\}$, $h = 1, 2, \ldots, q + 1$. The remaining lines are the blocks of the desired TD_2, QED.

This result is due to Hanani ([12], lemma 11).

We also note that $TD_2(q + 1, q - 1, q, 1)$ is symmetrical for any q, in the sense that the number of blocks is the same as the number of elements. Indeed, by (1.25) we have:

$$b = \frac{(q + 1)q(q - 1)^2}{q(q - 1)} = q^2 - 1$$

The replication number is, by (1.26):

$$r = \frac{q(q - 1)}{q - 1} = q \tag{3.1}$$

A $TD_2(v, s, k, \lambda)$ is said to be <u>regular</u> if $rk - vs\lambda > 0$.

In the case of $TD_2(q + 1, q - 1, q, 1)$ we get by (3.1):

$$rk - vs\lambda = q \cdot q - (q + 1)(q - 1) = 1 > 0 ,$$

hence it is regular.

Since the TD_2 in question is regular and symmetrical, a theorem of Connor ([5], p. 607, thm. 6.2) implies that the blocks fall into $v = q + 1$ groups of $s = q - 1$ blocks each, which are such that any two blocks in the same group are disjoint and any two blocks from different groups meet on $\lambda = 1$ element.

In other words, we may obtain a new $TD_2(q + 1, q - 1, q, 1)$ by calling the blocks "points" and the points, "blocks".

As an application, we mention:

<u>Theorem 3.8</u> If $q - 1$ and q are both prime powers, $TD_2(q^n, q - 1, q, 1)$ and $TD_2(q^n + 1, q - 1, q, 1)$ exist for any $n \geq 1$.

<u>Proof</u> $AG(n, q)$ is a $TD_2(q^n, 1, q, 1)$.

$TD_2(q, q - 1, q, 1)$ exists too: substitute $q - 1$ for q in lemma 3.1, then let $n = 2$.

Now combine these two TD_2's by theorem 3.2 , where:

$w = q^n$, $v = k = q$, $s = q - 1$, $s' = \lambda = \lambda' = 1$,

to get a $TD_2(q^n, q - 1, q, 1)$.

As for $TD_2(q^n + 1, q - 1, q, 1)$, if n is odd, combining $TD_2(q^{2t+1} + 1, 1, q + 1, 1)$ with $TD_2(q + 1, q - 1, q, 1)$, according to theorem 3.2, yields a $TD_2(q^{2t+1} + 1, q - 1, q, 1)$.

In this case, $q - 1$ need not be a prime power.

If n is even, however, we cannot relax the hypotheses of the theorem, because we do not know whether $TD_2(q^2, q - 1, q, 1)$ exists for all prime powers q , which is needed in what follows.

We have to prove that $TD_2(q^{2m} + 1, q - 1, q, 1)$ exists for any $m \geq 1$.

Let $m = 1$ and let us apply theorem 3.5 with:

$w = k = q$, $s = n = k' = q - 1$, $\lambda = \lambda' = 1$.

Then $TD_2(w + 1, s, k, \lambda\lambda')$ is $TD_2(q + 1, q - 1, q, 1)$, which exists by theorem 3.7.

$TD_2(n, w, k', \lambda)$ is $TD_2(q - 1, q, q - 1, 1)$. The latter is resolvable: it is obtained from $AG(2, q)$ by designating one parallel class of lines as the groups, then deleting all the points from one of the groups. Hence all remaining lines will contain $q - 1$ points and can be divided into q parallel classes of q lines each.

$TD_2(k' + 1, s, k, \lambda')$ is $TD_2(q, q - 1, q, 1)$, which has already been shown to exist.

Moreover, $v = \frac{(n - 1)w}{k' - 1} = w = q$ and so:

$TD_2(v + 1, s, k, \lambda\lambda')$ is $TD_2(q + 1, q - 1, q, 1)$ and exists.

So all the hypotheses of theorem 3.5 are satisfied and hence $TD_2(nw + v + 1, s, k, \lambda\lambda') \equiv TD_2(q^2 + 1, q - 1, q, 1)$ exists.

Therefore the design exists for $m = 1$.

Assume now that $TD_2(q^{2m} + 1, q - 1, q, 1)$ exists for some m. We again make use of theorem 3.5, by letting:

$$n = k' = q^2 - 1 \quad , \quad w = q^{2m} \quad , \quad s = q - 1 \quad , \quad k = q \quad , \quad \lambda = \lambda' = 1.$$

$TD_2(w + 1, s, k, \lambda\lambda')$ is $TD_2(q^{2m} + 1, q - 1, q, 1)$ and exists by the inductive hypothesis.

$TD_2(n, w, k', \lambda)$ is $TD_2(q^2 - 1, q^{2m}, q^2 - 1, 1)$ and it is resolvable: it is obtained from $AG(2, q^{2m})$ by designating one parallel class of lines as the groups and by removing all points belonging to $q^{2m} - q^2 + 1$ groups. Hence all remaining lines will contain $q^2 - 1$ points and can be divided into q^{2m} parallel classes of q^{2m} lines each.

$TD_2(k' + 1, s, k, \lambda') \equiv TD_2(q^2, q - 1, q, 1)$ exists (see the first part of the theorem).

$$v = \frac{(n - 1)w}{k' - 1} = w = q^{2m}$$

$TD_2(v + 1, s, k, \lambda\lambda') \equiv TD_2(q^{2m} + 1, q - 1, q, 1)$ exists by the inductive hypothesis.

Therefore $TD_2(nw + v + 1, s, k, \lambda\lambda') \equiv TD_2(q^{2m+2} + 1, q - 1, q, 1)$ exists. Thus we have proved by induction that $TD_2(q^{2m} + 1, q - 1, q, 1)$ exists for all $m \geq 1$, QED.

We conclude with two more theorems concerning TD_2's.

Theorem 3.9 Where q is a prime power, there exists a resolvable $TD_2(q^n, q^m, q, 1)$ for any $n \geq 1$, $m \geq 0$.

Proof For $m = 0$ this is $AG(n, q)$.

If the theorem holds for some m we apply theorem 3.2 to $TD_2(q^n, q^m, q, 1)$ and $TD_2(q, q, q, 1)$, the latter being clearly $AG(2, q)$ with one parallel class of lines as groups and thereby resolvable.

We obtain a $TD_2(q^n, q^{m+1}, q, 1)$, which is resolvable, QED.

Theorem 3.10 For any odd prime power q and $m|n$, $TD_2(\frac{q^n - 1}{q^m - 1}, 2^k(q^m - 1), 3, 2)$ exists for any $k \geq -1$.

Proof Let x be a primitive root of $GF(q^n)$.

Let us denote $\frac{q^n - 1}{q^m - 1} = u$ and let $E = \{x^i : i = 1, 2, \ldots, \frac{q^n - 1}{2}\}$ be partitioned by the collection $\mathcal{S} = \{S_1, S_2, \ldots, S_u\}$, where $S_h = \{x^{ju+h} : j = 0, 1, \ldots, \frac{q^m - 3}{2}\}$.

We will first construct an $(E, \mathcal{S}, \mathcal{J}) \equiv TD_2(u, \frac{q^m - 1}{2}, 3, 2)$.

For any a, b $(a, b \leq \frac{q^n - 1}{2})$ such that $a \not\equiv b \bmod u$, consider the triples (x^a, x^b, x^c) and (x^a, x^b, x^d) , where $x^c = \pm(x^a + x^b)$ and $x^d = \pm(x^a - x^b)$, the signs being chosen so as to have $c, d \leq \frac{q^n - 1}{2}$.

These triples are the blocks of the required TD_2. This is so because:

Firstly, $a \not\equiv b \bmod u$ implies $c, d \not\equiv a, b \bmod u$, because $\{x^{ku} : k = 1, 2, \ldots, q^{m-1}\}$ are the nonzero elements of a field.

Secondly, each pair appears exactly twice in the blocks of the TD_2, for if (x^a, x^b, x^c) is a block with $x^c = \pm x^a \pm x^b$, then the pair $\{x^a, x^c\}$, say, gives rise to two blocks, one of which is precisely (x^a, x^b, x^c): if $x^c = x^a + x^b$, then $-(x^a - x^c) = x^b$ and if $x^c = -x^a - x^b$, then $-(x^a + x^c) = x^b$.

Similarly for the pair $\{x^a, x^d\}$.

Therefore $TD_2(u, \frac{q^m - 1}{2}, 3, 2)$ exists.

Now assume $TD_2(u, 2^k(q^m - 1), 3, 2)$ exists for some k.

$TD_2(3, 2, 3, 2)$ exists, too, by lemma 3.1 with $q = 2$, $n = 3 = v$.

We combine these two designs according to theorem 3.2 to get a $TD_2(u, 2^{k+1}(q^m - 1), 3, 2)$ and this concludes the inductive argument, QED.

* * *

Concerning the matroid design problem, we have not succeeded in solving it completely: matroid designs of type IV consist essentially of designs of form $TD_2(1 + p^{(2t+1)m}, p^h, p^m + 1, 1)$ (see theorem 1.2), with $0 < h < m$.

As we have mentioned above, we do not yet know how to construct TD_2's with these parameters.

REFERENCES

1. R. C. Bose, On the application of finite projective geometry for deriving a certain series of balanced Kirkman arrangements, Calcutta Math. Soc. Golden Jubilee Vol., 1959, p. 341 - 354.

2. R. C. Bose and K. R. Nair, Partially Balanced Incomplete Block Designs, Sankhyā, vol. 4 (1939), p. 337 - 372.

3. R. C. Bose and W. S. Connor, Combinatorial Properties of Group Divisible Incomplete Block Designs, The Annals of Math. Statist. 23 (1952), p. 367 - 383.

4. R. C. Bose, S. S. Shrikhande and K. N. Bhattacharya, On the Construction of Group Divisible Incomplete Block Designs, The Annals of Math. Statist. 24 (1953), p. 167 - 195.

5. W. S. Connor, Some relations among the blocks of symmetrical group divisible designs, The Annals of Math. Statist. 23 (1952), p. 602 - 609.

6. H. Crapo and G. C. Rota, On the foundations of combinatorial theory: Combinatorial geometries, M. I. T., Cambridge, Mass., 1970.

7. P. Dembowski, Finite Geometries, Springer-Verlag New York Inc., 1968.

8. J. Edmonds, Matroids and the greedy algorithm, Math. Programming 1 (1971), p. 127 - 136.

9. J. Edmonds, Submodular functions, matroids and certain polyhedra, in Combinatorial Structures and Their Applications (Proceedings of the Calgary International Symposium on Combinatorial Structures, 1969), (Gordon and Breach, New York, 1970).

10. M. Hall, Jr., Combinatorial Theory, Blaisdell 1967.

11. H. Hanani, The Existence and Construction of Balanced Incomplete Block Designs, The Annals of Math. Statist. 32 (1961), p. 361 - 386.

12. H. Hanani, On BIBD with blocks having five elements, Journal of Combin. Theory (A) 12 (1972), p. 184 - 201.

13. H. Luneburg, Some Remarks concerning the Ree Groups of type (G_2), Journal of Algebra 3 (1966), p. 256 - 259.

14. H. B. Mann, Addition Theorems, Interscience 1965.

15. U. S. R. Murty, Equicardinal matroids and finite geometries, in Combinatorial Structures and Their Applications (Gordon and Breach, New York, 1970).

16. M. E. O'Nan, Automorphisms of Unitary Block Designs, Journal of Algebra 20 (1972), p. 495 - 511.

17. Th. Storer, Cyclotomy and Difference Sets, Markham 1967.

18. W. T. Tutte, Lectures on Matroids, J. Res. Nat. Bureau of Standards, Sec. B 69B (1965), p. 1 - 47.

19. H. Whitney, On the abstract properties of linear dependence, Amer. Journal Math. 57 (1935), p. 509 - 533.

20. Richard M. Wilson, An Existence Theory for Pairwise Balanced Designs, Journal of Combin. Theory (A) 13 (1972), p. 220 - 245.

21. H. Peyton Young, Existence Theorems for Matroid Designs, Trans. Amer. Math. Soc., vol. 183 (1973), p. 1 - 35.

22. H. Peyton Young, Affine Triple Systems, Centro Internazionale Matematico Estivo (C. I. M. E.), 1972.

23. H. Peyton Young and J. Edmonds, Matroid Designs, J. Res. Nat. Bureau of Standards, B, Vol. 77B, p. 15 - 44.