Matroid Designs of Prime Power Index*

BARBU C. KESTENBAND† AND H. PEYTON YOUNG

Graduate School of The City University of New York, 33 West 42 Street, New York, New York 10036

Communicated by the Managing Editors

Received August 19, 1975

A class of BIBD's is constructed with parameters generalizing those of the finite projective geometries. These designs are used to construct matroids in which the hyperplanes are equicardinal and the complement of every hyperplane has prime power cardinality. These so-called matroid designs of prime power index "almost" have the property that the flats of any given rank are equicardinal.

1. Introduction

A matroid \( M = [E, \mathcal{S}] \) is a finite set \( E \) together with a nonempty family \( \mathcal{S} \) 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 [6].

Evidently, matroids generalize the notion of linear independence in vector spaces [15]. They also have proved particularly useful in generalizing certain theorems about graphs [14] and theorems in combinatorial optimization [7]. On the other hand, one may view matroids as primarily geometric structures, by studying the relations among the closed sets [4]. Thus, matroids provide a unifying theme for many areas of combinatorics.

In this paper we shall explore certain connections between matroids and yet another area of combinatorics, the theory of block designs. In particular, we shall investigate certain matroids that generalize in a natural way the finite projective geometries—which are the foundation of so much in combinatorial design theory. These connections arise from the notion of a matroid design, which we now proceed to define.

* This work was supported in part by the Army Research Office under Contract DA-31-124-ARO(D)-366.
† Present address: New York Institute of Technology, Wheatley Road, P.O. Box 170, Old Westbury, L.I., N.Y. 11568.
Given a matroid \([E, \mathcal{F}]\), 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 a \((r(E) - 1)\)-flat, i.e., a maximal subset of \(E\) containing no basis of \(E\).

\(M = [E, \mathcal{F}]\) is a matroid design (MD) if all hyperplanes have the same cardinality, \(k(M)\). Using the well-known hyperplane axiomatization of matroids, we have the following alternate characterization of matroid designs: \(\mathcal{H}\) is the family of hyperplanes of a matroid design on a finite set \(E\) if and only if

1. The members of \(\mathcal{H}\) are equicardinal subsets of \(E\),

2. For any \(H_1, H_2 \in \mathcal{H}\), \(H_1 \neq H_2\), and \(x \in E\) there exists \(H \in \mathcal{H}\) satisfying \(\{x\} \cup H_1 \cap H_2 \subseteq H\).

We say that a matroid \(M\) is a perfect matroid design (PMD) if for every \(h\), all \(h\)-flats of \(M\) are equicardinal. The archetypical PMD's are the finite projective and affine geometries. Other known classes of PMD's are the \(t\)-designs with \(\lambda = 1\), and the affine triple systems [18]. PMD's are highly complex and beautiful structures, but difficult to find. In particular, they are very special cases of balanced incomplete block designs (BIBD's) and they must satisfy stringent numerical conditions, although these are far from sufficient for their existence [19]. On the face of it, matroid designs appear to be much more general than PMD's, but in fact they are almost as hard to construct. Indeed, all known examples of matroid designs are "almost" perfect matroid designs. This general observation will be made precise in Section 3 for a certain class of matroid designs that are closely related to the finite projective geometries.

Murty [12] posed the problem of characterizing all MD's on a set of cardinality \(v\), having rank \(r\) and hyperplane cardinality \(k\). In [17] Young developed methods for solving this problem, and the solution turns out to depend on the prime factorization of \(v - k\). \(v - k = \gamma(M)\) is called the index of the matroid design. A complete solution is known for all ranks \(r\) when the index is a prime, a prime squared, or is the product of distinct primes \(p\) and \(q\), where \(p < (2q/3) + 1\) and \(pq \neq 6, pq \neq 15\).

A finite projective geometry \(PG(n, q)\) of dimension \(n\) and order \(q\), \(q\) a prime power, is a matroid design on \(v = (q^{n+1} - 1)/(q - 1)\) elements with hyperplane size \(k = (q^n - 1)/(q - 1)\), so the index is \(v - k = q^n\), a prime power. The class of matroid designs of prime power index turns out to be a particularly interesting class of designs about which much can be said, and by the above, they constitute a natural generalization of finite projective geometries. In this paper we shall extend the methods of [17] to completely characterize all rank 3 matroid designs of prime power index. All such designs will be shown to be closely related to certain classes of block designs—and, in particular, to unitals. We are therefore led to construct a general
class of BIBD's from which these rank 3 matroid designs are derived. Moreover, for any rank \( r \), we will show that all matroid designs of prime power index and rank \( r \) are "almost" perfect matroid designs—which provides an important tool for analyzing the structure of matroid designs.

Let \( \mathcal{H} \) be the hyperplane family of the matroid \( M \) on a set \( E \); we will denote this situation by \( M = (E, \mathcal{H}) \). For any \( E' \subseteq E \), the contraction of \( M \) to \( E' \) is the matroid \( M \cdot E' = (E', \mathcal{H}') \) where \( \mathcal{H}' = \{ H \cap E' : H \in \mathcal{H} \text{ and } E-E' \subseteq H \} \). Evidently, \( r(M \cdot E') = r(M) - r(E - E') \). Moreover, if \( M \) is a matroid design, then so is any contraction of \( M \). A separator of \( M \) is a nonempty subset \( S \) of \( E \) such that either \( S \subseteq H \) or \( E - S \subseteq H \) for all \( H \in \mathcal{H} \). \( M \cdot S \) is a component of \( M \), and \( M \) is connected if it has but one component. If \( M \) is a matroid design then each of its components is a matroid design; hence it suffices to consider only connected matroid designs. The class of all connected matroid designs of rank \( n \) and index \( \gamma \) we denote by \( M_n(\gamma) \).

We make the following general remarks about matroids. Any element that is dependent is called a loop, and the set of all loops constitute the 0-flat. As the 0-flat is contained in every flat, we may exclude all loops without altering the essential relations among the various flats. We therefore always assume in the sequel that matroids have no loops. The 1-flats will be called points; for any flat \( F \) the points meeting \( F \) partition \( F \). It should be noted that a point may contain more than one element; we say that a point having cardinality \( m \) is an \( m \)-point. In the case of a graphic matroid, a multiple-cardinality point just corresponds to a set of parallel edges. A 2-flat is called a line. Clearly, every two distinct points are contained in a unique line. More generally, we have [19]:

**Theorem 1.** If \( M \) is a rank \( n \) matroid and \( F^i \subseteq F^k \) are an \( i \)-flat and \( k \)-flat of \( M \), then \( F^k - F^i \) is partitioned by the sets of form \( F^{i+1} - F^i \), where \( F^{i+1} \) ranges over the \((i+1)\)-flats containing \( F^i \) and contained in \( F^k \).

A point of \( M \) is simple if it is a singleton, and \( M \) is simple if all of its points are simple. Simple matroids have been called combinatorial geometries by Crapo and Rota [4], while matroids are designated as mere "pre-geometries." On the face of it, there appears to be no reason for considering anything other than simple matroids, for we can always just replace all points by singletons. However, this replacement may alter the cardinality of the flats, and therefore will not do if our interest is matroid designs. Moreover, even if we wished to restrict our attention to simple matroid designs, we should find that this cannot conveniently be done, because the class of simple matroids is not closed under contraction, and contraction turns out to be one of the most useful tools for analyzing matroid designs. It is for this reason that we study matroid designs—simple and nonsimple.

If \( M = (E, \mathcal{H}) \) is a matroid and \( \alpha \) a positive integer, define a new matroid
\( \alpha M \) by replacing each element \( x \in E \) by an \( \alpha \)-set \( S_x \), where \( S_x \cap S_{x'} = \emptyset \) for \( x \neq x' \), and making corresponding replacements in the hyperplanes. \( \alpha M \) is called an \( \alpha \)-inflation of \( M \); likewise \( M \) is an \( \alpha \)-deflation of \( \alpha M \). Where \( E \) is a \( r \)-set, \( \mathcal{H} \) the set of all \( k \)-subsets of \( E \), \( k < v \), and \( \alpha \) is a positive integer, we say that \( \alpha M = \alpha(E, \mathcal{H}) \) is an \( (\alpha, k, v) \)-trivioid, abbreviated by \( \sigma(\alpha, k, v) \). Every rank 1 or rank 2 matroid design is a trivioid. As trivioids are not particularly interesting we define \( \tilde{M}_n(\gamma) \) to be the set of all rank \( n \) nontrivial connected matroid designs of index \( \gamma \).

Then the following is true [17].

**Theorem 2.** \( \tilde{M}_n(\gamma) = \emptyset \) for some \( n \geq 3 \) implies \( \tilde{M}_m(\gamma) = \emptyset \) for all \( m \geq n \). In particular, all connected MD’s of index \( \gamma \) are trivial if and only if all connected rank 3 MD’s of index \( \gamma \) are trivial.

2. **Transversal Designs and Matroid Designs**

A species that occurs frequently in the literature on block designs is a close relative of the Balanced Incomplete Block Designs—the so-called transversal designs.

It turns out that they play an essential role in characterizing rank 3 matroid designs of prime power index. Let \( \mathcal{S} \) be a family of nonempty subsets partitioning a finite set \( E \). A subset \( T \) of \( E \) such that \(| T \cap S | \leq 1 \) for all \( S \in \mathcal{S} \) is said to be a partial transversal of \( \mathcal{S} \), and \(| T | \) is its length. The triple \( (E, \mathcal{S}, \mathcal{T}) \) is a transversal design (TD) with parameters \( t, v, s, k, \lambda \), where \( v \geq k \geq t \geq 2 \), \( s \geq 1 \), \( \lambda \geq 1 \), if:

(i) \( | \mathcal{S} | = v \) and \( | S | = s \) for all \( S \in \mathcal{S} \);

(ii) \( \mathcal{T} \) is a family of partial transversals of \( \mathcal{S} \) all having length \( k \);

(iii) Every length-\( t \) partial transversal of \( \mathcal{S} \) is contained in exactly \( \lambda \) members of \( \mathcal{T} \).

The members of \( \mathcal{S} \) are called **groups**, and the members of \( \mathcal{T} \) are called **blocks**. For short we denote a transversal design as above by \( \text{TD}_i(v, s, k, \lambda) \). A TD with \( s = 1 \) is the same as a \( t - (v, k, \lambda) \) design and if also \( t = 2 \), we have a Balanced Incomplete Block Design, denoted \((v, k, \lambda)\)-BIBD. The number of blocks containing any given length-\( i \) transversal is

\[
\lambda_i = \lambda s^{t-i} \binom{v-i}{t-i} / \binom{k-i}{t-i}, \quad 0 \leq i \leq t,
\]

which must be integer for the design to exist.

It should be noted that TD’s crop up in the literature under a variety of guises and names. Hanani [9] used certain TD’s with \( v = k \), \( t = 2 \), \( \lambda = 1 \)
to construct BIBD’s with \( k = 3, 4, \) and \( 5, \) and called them \( T \)-systems. Bose [3] uses the term *group divisible design* for a TD with \( t = 2 \) and is motivated by applications to the design of experiments. Wilson [16] uses the term group divisible design to mean incidence structures \((E, \mathcal{S}, \mathcal{T})\) as above with \( t = 2 \) but not necessarily equicardinal groups or blocks. Having noted these differences, we will stay with the term “transversal design” in the sequel.

The connection between transversal designs and matroid designs arises in the following way. Let \((E, \mathcal{S}, \mathcal{T})\) be a \( TD_2(v, s, k, 1) \), \( s \leq k \), and let \( P \) be a set of \( k - s \) elements disjoint from \( E \). If \( \mathcal{H} = \mathcal{T} \cup \{S \cup P : S \in \mathcal{S}\} \), then \((E, \mathcal{H}) = M\) is a rank \( 3 \) matroid design. Any MD obtained in this manner will be denoted by \( MD(v, s, k) \). Examples of such structures will be discussed in Sections 4 and 5.

3. MATROID DESIGNS OF PRIME POWER INDEX

We will now show that every rank \( 3 \) matroid design of prime power index is a \( MD(v, s, k) \) for suitable \( v, s, \) and \( k \). Moreover, we shall show that the cardinality of all points, lines, and the space \( E \) must be of a particular form. First, for any matroid \( M \) we define \( \alpha_i = \alpha_i(M) \) to be the cardinality of the smallest \( i \)-flat in \( M \), \( 1 \leq i \leq r(M) = n \). A *small* \( i \)-flat is an \( i \)-flat having cardinality \( \alpha_i \), any \( i \)-flat having larger cardinality will be called a *large* \( i \)-flat.

**Theorem 3.** Let \( M = (E, \mathcal{H}) \) be a rank \( 3 \) matroid design with index \( p^m \), \( p \) a prime.

(i) Then there exist integers \( 0 \leq a_1 \leq a_2 \leq a_3 = m \) such that

\[
\alpha_1(M) = p^{a_1},
\]
\[
\alpha_2(M) = p^{a_2} + p^{a_1},
\]
\[
\alpha_3(M) = p^{a_3} + p^{a_2} + p^{a_1}.
\]

(ii) There is at most one large point, \( y \), and \( |y| = p^{a_2} - p^{b} + p^{a_1} \), where \( b \) satisfies (and is uniquely determined by)

\[
a_2 > b \geq a_1
\]
\[
a_3 = (2t + 1)(a_2 - a_1) + b, \quad t \text{ integer}, t \geq 1.
\]

**Proof.** Let \( L \) be any line of \( M \), and let \( x_0, x_1, \ldots, x_s \) be all the points contained in \( L \), \( s \geq 1 \). For each \( i, |L - x_i| \) divides \( p^m \) (by Theorem 1),
hence $|L - x_i| = p^{r_i}$ for integer $r_i \geq 0$. Summing over $i$ we obtain

$$(s + 1) |L| - |L| = \sum_{i=0}^{s} |L - x_i| = \sum_{i=0}^{s} p^{r_i},$$

and

$$|L| = \left(\sum_{i=0}^{s} p^{r_i}\right)/s. \quad (2)$$

Without loss of generality, let $r_0 \leq r_1 \leq \cdots \leq r_s$, and let $t$ be the first integer for which $r_t = r_s$. Then

$$0 < |x_s| = \frac{\sum_{i=0}^{s} p^{r_i}}{s} - p^{r_s} \leq \frac{tp^{r_{t-1}} + (s - t + 1)p^{r_s} - sp^{r_s}}{s} = \frac{tp^{r_{t-1}} + (1 - t)p^{r_s}}{s} = \frac{p^{r_{t-1}}(t + (1 - t)p)}{s}.$$

Hence $t + (1 - t)p > 0$ and $p > t(p - 1)$, which implies $t = 0$ or $t = 1$. In either case we have, by (2),

$$|L| = \frac{p^{r_0}}{s} + p^{r_s}, \quad \text{and} \quad |x_1| = |x_2| = \cdots = |x_s| = \frac{p^{r_0}}{s}.$$

Notice that, by choice, $p^{r_0}/s \leq p^{r_s}$. Since all lines are equicardinal, $p^{r_0}/s$ and $p^{r_s}$ are therefore invariants of $M$. Let $p^{a_1} = p^{r_0}/s$, $p^{a_2} = p^{r_s}$. Then $\alpha_1(M) = p^{a_1}$, $\alpha_2(M) = p^{a_1} + p^{a_2}$, and $\alpha_3(M) = |E| = p^{a_1} + p^{a_2} + p^{a_3}$, proving (i).

The above argument also shows that for any line $L$ of $M$, all points, except at most one, have cardinality $p^{a_1}$. Since any two points are contained in a line there can exist at most one large point. If $y$ is such a point, $y \subseteq L$, then as above $|L| - |y| = p^{r_0}$, whence

$$|y| = p^{a_2} - p^{r_0} + p^{a_1}, \quad \text{and} \quad a_2 > r_0 \geq a_1. \quad (3)$$

Letting $b = r_0$ we have established the first part of (ii). Now deflate $M$ by $p^{a_1}$ (we can do this because $p^{a_1}$ divides $|y|$), to obtain $M'$ with large point $y'$. There are

$$\frac{p^{a_3-a_1} + p^{b-a_1}}{p^{b-a_1}} = p^{a_3-b} + 1$$

lines containing $y'$, and exclusive of $y'$ they form the groups (each of size
MATROID DESIGNS

217

$p^{b-a_1}$ of a TD$_2$, with $\lambda = 1$, whose blocks are all other lines. The blocks have size $p^{a_2-a_1} + 1$. Thus, by (1),

$$\frac{p^{2(b-a_2)}(p^{a_2-b} + 1)p^{a_2-b}}{(p^{a_2-a_1} + 1)p^{a_2-a_1}} \text{ must be integer.} \quad (4)$$

Since $|y| > p^{a_2}, a_2 > a_1$, whence it follows from (4) that $a_2 - b$ must be an odd multiple of $(a_2 - a_1)$. Finally if $a_2 - b = a_2 - a_1$, then the transversals are full (i.e., meet every group) and in this case for $\lambda = 1, t = 2, s \geq 2$ the transversal size $k$ and group size $s$ must satisfy $k \leq s + 1$. Thus $p^{a_2-b} + 1 \leq p^{b-a_1} + 1$ so $a_2 - b = a_2 - a_1 \leq b - a_1$, whence $b \geq a_2$, a contradiction. Hence $a_2 - b = (2t + 1)(a_2 - a_1)$ for some $t \geq 1$. This, together with $a_2 > b \geq a_1$ determines $b$ uniquely,

Q.E.D.

An algebraic consequence of Theorem 3 is as follows. Let $M = (E, \mathcal{H})$ be a rank 3 matroid with $v$ points and $b$ hyperplanes ($b \geq v$), and let $A$ be the $b \times v$ incidence matrix of $M$, i.e., of hyperplanes versus points. Then every hyperplane contains at least two points and every two points are contained in exactly one hyperplane, i.e., $(AA^T)_{ii} \geq 2, 1 \leq i \leq b$ and $(A^TA)_{ij} = 1$ for all $i \neq j, 1 \leq i \leq b, 1 \leq j \leq v$. Conversely, any $b \times v$ matrix $A, b, v \geq 2$, satisfying the above two conditions is the incidence matrix of some rank 3 matroid $M$. For $M$ to be a matroid design, the points must have multiplicities such that all hyperplanes are equicardinal, i.e., there must be a solution $z$ in positive integers to a system of form: $Az = k \cdot 1$, where $1$ is a $b \times 1$ vector of 1's, $k$ is a positive integer. The index of the matroid is then $\sum_{i=1}^v z_i - k = \gamma$, so that equivalently $(E - A)z = \gamma \cdot 1$, where $E$ is the $b \times v$ matrix of all 1's. Thus we have the following corollary of Theorem 3.

**Corollary 3.1.** If $A$ is a $b \times v$ 0, 1-matrix satisfying $(AA^T)_{ii} \geq 2$ and $(A^TA)_{ij} = 1$ for all $i \neq j$ and $p$ is a prime, then any positive integer solution $z$ to the system

$$(E - A)z = p^m \cdot 1$$

is of form (subject to relabelling of columns)

$$z_1 = p^{a_2} - p^b + p^{a_1}, \quad z_2 = \cdots = z_v = p^{a_1}$$

for some integers $0 \leq a_1 \leq b \leq a_2$, where either $b = a_2$ or $b < a_2$ and is determined by $m = (2t + 1)(a_2 - a_1) + b, t \geq 1$.

Using Theorem 3 we may now easily describe the structure of any rank 3 matroid design of index $p^m$ in terms of transversal designs (and BIBD's). Let $M$ be as in Theorem 3. Then $M$ is a trivioid if and only if $a_2 = a_1$, and it must be a $(p^{a_1}, 2, p^{m-a_1} + 2)$-trivioid. If $M$ is not a trivioid, let $M'$ be a
$p^{a_2}$-deflation of $M$. If $M'$ has a large point, then the proof of Theorem 3 shows that $M'$ is a TD$_2(v, s, k, 1)$ with the large point attached to each group, i.e., it is an MD$(v, s, k)$ with
\[ v = p^{a_2-b} + 1, \]
\[ s = p^{b-a_1}, \]
\[ k = p^{a_2-a_1} + 1, \]
and $a_2 - b$ is an odd multiple of $a_2 - a_1$. That is, $M'$ is of form MD $(p^{(2r+1)s} + 1, p^r, p^s + 1)$ where $r, s$ are integers such that $0 \leq r < s$.

If $M'$ has all points equicardinal, then $M'$ is evidently a BIBD with parameters
\[ v = p^{a_2-a_1} + p^{a_2-a_1} + 1, \]
\[ k = p^{a_2-a_1} + 1, \]
\[ \lambda = 1. \]
The integer conditions (1) and $a_2 > a_1$ imply that $a_2 - a_1$ must be an odd multiple of $a_2 - a_1$.

An alternate way of characterizing any BIBD with $\lambda = 1$ is to fix one element and regard the blocks containing it, exclusive of that element, as the groups of a TD on the remaining blocks. Looked at in this way the above BIBD $M'$ may be represented as a TD$(v', s', k', 1)$ with a singleton point attached to all the groups, i.e., as an MD$(v', s', k')$ where
\[ v' = p^{a_2-a_2} + 1, \]
\[ s' = p^{a_2-a_2}, \]
\[ k' = p^{a_2-a_1} + 1. \]
and $a_2 - a_2$ is an odd multiple of $a_2 - a_1$. That is, $M'$ is of form MD $(p^{(2r+1)s} + 1, p^r, p^s + 1)$. Combined with the above, we have proved the following corollary of Theorem 3.

**Corollary 3.2.** Every nontrivial rank 3 MD of index $p^m$ is a $p^{m-(2t+1)s-1}$-MD$(p^{(2r+1)s} + 1, p^r, p^s + 1)$ for some integers $t, r, s$ such that $0 \leq t, 0 \leq r < s$, and $(2t + 1)s + r \leq m$.

The case $r = s$ above corresponds to an inflation of a BIBD. Consider now the case $r = 0$. If $M'$ is a MD$(p^{(2r+1)s} + 1, 1, p^s + 1)$, then $M'$ is a BIBD $M''$ together with an additional point of cardinality $p^s$ attached to every element of $M''$. In general, if $M'' = (E'', \mathscr{X}'')$ is any rank 3 matroid,
and $F$ is a set of cardinality $h$, where $F \cap E'' = \emptyset$, then we may define a new rank 3 matroid $M'$ on the set $E'' \cup F$ whose hyperplane family is $\mathcal{H}''$ together with all sets of form $P'' \cup F$, where $P''$ ranges over all points of $M''$. $M'$ is called a one-point extension of $M''$, and denoted by $M'' \oplus h$.

Later, in Sections 4 and 5, we shall establish the existence of all matroid designs in Corollary 3.2 corresponding to the cases $r = 0$ and $r = s$ by showing that the appropriate infinite classes of BIBD's exist. These BIBD's turn out to be based on the so-called unitals. However, our present object is to explore some further consequences of Theorem 3.

Theorem 3 says that every rank 3 matroid design of prime power index is "almost" a transversal design, hence "almost" a BIBD. We will now show that for any rank, any matroid design of prime power index is "almost" a perfect matroid design (PMD).

First we need the following definitions. If $M$ is a matroid and $F$ a $k$-flat of $M$, $k \geq 1$, then the reduction of $M$ to $F$, $M \times F$, is the matroid on set $F$ whose hyperplanes are the $(k - 1)$-flats of $M$ that are contained in $F$.

For any rank $n$ matroid $M$ the sequence $\alpha_n(M), \alpha_{n-1}(M), ..., \alpha_1(M)$ where $\alpha_i(M)$ is the cardinality of the smallest $i$-flat in $M$ will be called the $\alpha$-sequence of $M$. If $M$ is a PMD, all $i$-flats have cardinality $\alpha_i = \alpha_i(M)$. In this case, it is convenient to define the numbers $d_1 = 1$ and $d_i = (\alpha_i - \alpha_{i-1})/\alpha_1$, $2 \leq i \leq n$. The sequence $d_1, d_2, ..., d_n$ is called the $d$-sequence of $M$. For any rank $n$ PMD the $d$-sequence must satisfy the conditions [19]:

\begin{equation}
\frac{d_{i+1}}{d_i} \geq \frac{d_{i}}{d_{i-1}} \quad 2 \leq i \leq n,
\end{equation}

\begin{equation}
d_{i-1} \mid d_i, \quad 2 \leq i \leq n,
\end{equation}

and

\begin{equation}
\prod_{l=i}^{j} \sum_{m=1}^{k} d_m / \prod_{l=i+1}^{j} \sum_{m=1}^{k} d_m \quad \text{is integer for } 0 \leq i \leq j \leq k \leq n.
\end{equation}

These conditions mean that nontrivial PMD's, particularly those of higher ranks, are very rare. We now prove the following generalization of Theorem 3, which shows that matroid designs of prime power index are quite rare also.

**Theorem 4.** Let $M$ be a connected matroid design of prime power index $p^n$ and rank $n \geq 1$. Then

(i) there exist integers $a_1, a_2, ..., a_n = m$ such that

\[ \alpha_k(M) = \sum_{i=1}^{k} p^{a_i} \quad \text{for } 1 \leq k \leq n; \]
(ii) there is at most one large point, and if it exists its cardinality is of form

\[ \sum_{i=1}^{n-1} p^{a_i} - \sum_{i=1}^{n-2} p^{b_i} \]

for suitable integers \( b_i \);

(iii) for any small \((n - 2)\)-flat \( F \) of \( M \), \( M \times F \) is a PMD with \( d \)-sequence \( p^{a_2-a_1}, p^{a_3-a_1}, \ldots, 1 \).

Proof. The theorem has been established for \( n = 3 \) and is obviously true for \( n = 1 \) and \( n = 2 \). We next prove it for \( n = 4 \).

Given \( M = (E, \mathcal{H}) \), for any flat \( F \) of \( M \) abbreviate \( M \cdot (E - F) \) by \( M_F \).
Also for any \( S \subseteq E \) let \( \text{cl}(S) \), the closure of \( S \), denote the smallest flat containing \( S \).

Now let \( L \) be a small line of \( M \), \( r(M) = 4 \). Then for any point \( x \) in \( L \), \( L - x \) is a small point of \( M_x \), hence by induction, \( L - x \) is a power of \( p \).
It follows just as in the proof of Theorem 3 that \( \alpha_x(M) = | L | = p^{a_2(L)} + p^{a_1(L)} \)
for some integers \( a_2(L) \geq a_1(L) \geq 0 \), all points in \( L \) (except possibly one) have cardinality \( p^{a_2(L)} \), and the remaining point has cardinality \( p^{a_2(L)} - p^{b(L)} + p^{a_1(L)} \), where \( a_2(L) \geq b(L) \geq a_1(L) \). Let \( x \) be any \( p^{a_1(L)} \)-cardinality point in \( L \), and consider \( M_x \). By Theorem 3, \( M_x \) has at most one large point, hence, in \( M \), \( x \) is contained in at most one large line; call it \( L' \). Thus, any point \( y \) not in \( L' \) lies in a small line. Then as above any such \( y \) is contained in at most one large line \( L'' \); hence all points, except possibly \( L' \cap L'' \), are contained in some small line, and therefore in at most one large line.

If every point is contained in a small line, let \( x_0 \) be an arbitrary fixed point; otherwise let \( x_0 \) be the unique point contained in no small line.

For any \( x_1 \neq x_0 \), let \( L_1 \) be a small line containing \( x_1 \). Then, as above, all points in \( L_1 \) have cardinality \( p^{a_1(L_1)} \) (except possibly \( x_0 \)), and \( | L_1 | = p^{a_2(L_1)} + p^{a_1(L_1)} \), \( a_2(L_1) \geq a_1(L_1) \). But \( | L_1 | = | L | = p^{a_2(L)} + p^{a_1(L)} \), hence \( a_2(L) = a_2(L_1) \) and \( a_1(L) = a_1(L_1) \) do not depend on the particular small line chosen. Thus \( \alpha_x(M) = p^{a_2} + p^{a_1}, a_2 \geq a_1 \). Now \( p^{a_1} \) divides \( | L_1 - x_1 | \), which is a small point in \( M_{x_1} \). Since \( | L_1 - x_1 | \) divides the cardinality of every point in \( M_{x_1} \), \( p^{a_1} \mid | L - x_1 | \), where \( L = \text{cl}(x_0, x_1) \). But \( p^{a_1} \) also divides the cardinality of every point in a small line, hence \( p^{a_1} \mid y \) for all \( y \subseteq L, y \neq x_0 \), hence also \( p^{a_1} \mid x_0 \). Thus \( x_0 \geq p^{a_1} \) and \( \alpha_x(M) = p^{a_1} \). Also, by Theorem 1, the sets \( H - L \) (where \( L \) is a fixed small line and \( H \) ranges over the hyperplanes containing \( L \)) partition \( E - L \), hence \( | H - L | \) divides \( p^{a_1} \), so \( | H - L | = p^{a_1} \) for some integer \( a_1 \). Here \( a_2 \geq a_1 \), else \( H \) would contain lines smaller than \( p^{a_2} + p^{a_1} \). Setting \( m = a_4 \) we then have \( a_4 \geq a_3 \geq a_2 \geq a_1 \), \( a_3 = \sum_{i=1}^{3} p_i, a_4 = \sum_{i=1}^{4} p_i \).

This proves statement (i) for \( n = 4 \). In the sequel we shall assume (by deflating) that \( a_1 = 0 \).

Let \( x_1, x_2, x_3 \) be distinct large points, and say \( x_1 \neq x_0 \). Then \( \text{cl}(x_1, x_2) \)
and \( \text{cl}\{x_1, x_3\} \) are not small lines (because each contains two large points), but \( x_1 \) is contained in at most one large line. Hence \( \text{cl}\{x_1, x_2\} = \text{cl}\{x_1, x_3\} \) and it follows that all large points lie on one line; call this line \( L_0 \).

Next we show that every point other than \( x_0 \) is simple. If \( a_2 = 0 \) this follows at once, since every point other than \( x_0 \) is in some small line. Hence assume \( a_2 > 0 \). Suppose that there exists a point \( x_1 \neq x_0 \) with \( |x_1| > 1 \). Then \( x_1 \subseteq L_0 \). We will obtain a contradiction by proving that there exist distinct 3-flats \( F \) and \( F' \), each containing only small lines, such that \( F' \) contains no large points and \( F \) contains \( x_1 \) and no other large points.

Suppose that we have established (8). Since \( x_1 \) lies in a small line,

\[
|x_1| = p^{a_2} - p^{d_1} + 1 \quad \text{for some} \ d_1, \ a_2 > d_1 \geq 0.
\]

(9)

Given, \( F, F' \) as in (8), the small lines in \( F \) not containing \( x_1 \) form a \( \text{TD}_2 \) on the groups \( S_k = L_k - \{x_1\} \), where \( L_k \) ranges over the lines in \( F \) containing \( x_1 \). The number of groups is

\[
\frac{a_3 - |x_1|}{|S_k|} = \frac{p^{a_3} + p^{d_1}}{p^{a_2}} = p^{a_3 - d_1} + 1.
\]

Hence the number of lines in \( F \) not containing \( x_1 \) is

\[
\frac{p^{a_2}(p^{a_3 - d_1} + 1) p^{a_3 - d_1}}{(p^{a_2} + 1) p^{a_2}},
\]

whence \( a_3 - d_1 \) is an odd multiple of \( a_2 \).

But the lines in \( F' \) form a 2-design, hence their number is

\[
\frac{(p^{a_2} + p^{a_2} + 1)(p^{a_2} + p^{a_2})}{(p^{a_2} + 1) p^{a_2}} = p^{a_3 - a_2} + 1 + \frac{p^{a_3}}{p^{a_2} + 1} \left( p^{a_3 - a_2} + 1 \right),
\]

whence \( a_3 - a_2 \) must also be an odd multiple of \( a_2 \). Since \( a_2 > d_1 \), this is impossible.

To prove (8) we argue as follows. Suppose there exists a large line \( L_1 \) containing only simple points. For any \( z \subseteq L_1 \), \( z \neq x_0 \), \( M_z \) has \( \alpha_4(M_z) = p^{a_2}, \alpha_4(M_z) = p^{a_3} + p^{a_2} \). Hence \( |L_1 - z| = p^{a_3} - p^b + p^{a_2} \) for some \( b, a_3 > b \geq a_2 \) (because \( L_1 \) is large). Thus

\[
|L_1| = p^{a_3} - p^b + p^{a_2} + 1.
\]

If \( L_0 \cup L_1 = E \), then either \( M \) is disconnected, or has rank less than or equal to 3, contrary to hypothesis. Hence, choose \( y \not\subseteq L_0 \cup L_1 \), \( |y| = 1 \), and consider the \( |L_1| = t \) lines \( N_1, N_2, \ldots, N_t \) meeting both \( y \) and \( L_1 \).
Each $N_i \subseteq \text{cl}(L_1 \cup \{y\}) = H$ and $|N_i| \geq p^{a_3} + 1$, so

$$tp^{a_2} + 1 \leq t \sum_{i=1}^{t} (|N_i| - |y|) + |y| \leq |H| = p^{a_3} + p^{a_2} + 1,$$

or

$$(p^{a_3} - p^b + p^{a_2} + 1)p^{a_2} + 1 \leq p^{a_3} + p^{a_2} + 1,$$

or

$$p^{a_3} - p^b + p^{a_2} \leq p^{a_3 - a_2}.$$

Since $b < a_3$, 

$$p^{a_3} - p^b + p^{a_2} > p^b(p^{a_3 - b} - 1) \geq p^b(p - 1)p^{a_3 - b - 1} \geq p^{a_3 - 1},$$

the last because $p \geq 2$. Thus $p^{a_3 - 1} < p^{a_3 - a_2}$, which contradicts the assumption that $a_2 > 0$. In summary, under the hypothesis $a_2 > 0$,

\begin{equation}
\text{every large line must contain a large point, hence meets } L_0. \tag{10}
\end{equation}

If $L_0$ is small, then $x_1$ is the unique large point in $L_0$, hence also the unique large point in $M$. $x_1$ is contained in at most one large line, but by the above every large line of $M$ meets $x_1$. Therefore one can certainly find $F, F'$ as in (8) to obtain a contradiction.

Suppose on the other hand that $L_0$ is large. Since $M_{x_1}$ has $\alpha$-sequence $p^{a_3}, p^{a_2}, p^{d_1}$, and $L_0 - x_1$ is the large point, we have by (9)

$$|L_0| = p^{a_3} - p^e + p^{d_1} + |x_1| = p^{a_3} - p^e + p^{a_2} + 1$$

for some $e, a_3 > e \geq d_1$. Moreover, by Theorem 3,

$$a_4 = (2t + 1)(a_3 - d_1) + e, \quad \text{where} \quad t \geq 1,$$

so

$$a_4 - d_1 \geq 3(a_3 - d_1) + e - d_1 \geq 3(a_3 - d_1)$$

and

$$a_4 - a_3 \geq 2(a_3 - d_1) > 2(a_3 - a_2) > a_3 - a_2. \tag{11}$$

Choose any simple point $y \notin L_0$ and let $F^* = \text{cl}(L_0 \cup y)$. If $M_x$ contains a large point, $z$, then this comes from a large line, which by (10) lies in $F^*$.

Since $M_y$ has $\alpha$-sequence $p^{a_3}, p^{a_2}, p^{d_1}$, we have $z = p^{a_3} - p^f + p^{a_2}$ for some $f, a_3 \geq f \geq a_2$. In $M_y$ there are $p^{a_3 - f} + 1$ lines containing $z$ and $F^* - \{y\} = L^*$ is among them. However, if every line in $M_y$ meets $L^*$ then a simple calculation shows that $p^{a_3 - a_2} + 1 = p^{a_3 - f} + 1$ or $a_4 - f = a_3 - a_2$; but by (11) $a_4 - f \geq a_4 - a_3 > a_3 - a_2$, a contradiction. Thus there is a line $L'$ of $M_y$ disjoint from $L^*$, hence $L' \cup \{y\} = F'$ does not meet $L_0$. By (10), $F'$ contains
no large lines. The same construction works if $z$ is small. On the other hand, there is also clearly a 3-flat $F$ in $M$ such that $F \cap L_0 = \{x_i\}$. Since $x_1$ is contained in a small line, it is contained in at most one large line, namely $L_0$; thus $F$ contains no large lines. This leads to a contradiction as in (8), hence there is no large point $x_1 \neq x_0$.

If $x_0$ itself is large, and contained in a small line then by Theorem 3 it is contained in at most one large line. Further, we must have $a_2 > 0$, so (10) implies every large line meets $x_0$, i.e., there is at most large line altogether in $M$. But then we may construct $F, F'$ as in (8), a contradiction.

In summary, we have established that either

(i) $M$ contains one large point, $x_0$, and $x_0$ is contained in no small line,

or

(ii) $M$ contains only small points. (12)

In case (12)(i), $M_{x_0}$ has $\alpha$-sequence $p^{a_2}, p^{d}, p^e$ for some integers $d, e$, hence $|x_0| = p^{a_2} + p^{a_3} + p^{a_4} - p^d - p^e$, proving statement (ii). Statement (iii) follows from (12) when $n = 4$.

Now we prove the theorem by induction for any rank $n$. Assume the theorem holds for all $n' < n$, where $n \geq 5$. Note that the induction hypothesis for statement (ii) implies, by contraction, that for all $r$,

any $r$-flat contained in some small $(r + 1)$-flat is contained in at most one large $(r + 1)$-flat. (13)

We shall actually show inductively the following somewhat stronger version of (iii) in the Theorem.

For any $1 \leq r, s \leq n - 2$ no small $s$-flat contains a large $r$-flat. (14)

We know (14) holds for all $n \leq 4$; assume it holds for all $n' < n$, where $n \geq 5$. By applying contraction to $M$ we deduce that

for any $r, s$ such that $2 \leq r \leq s \leq n - 2$, no small $s$-flat contains a large $r$-flat. (15)

If $L$ is any small line in $M$, then by induction (statement (i)) $|L - x|$ is a $p$-power for any point $x$ in $L$, hence, as in the proof of Theorem 3, $\alpha_2(M) = |L| = p^{a_2} + p^{a_3}$ for integers $a_2 \geq a_4$, every point on $L$ has cardinality divisible by $p^{a_2}$, and there is at most one point on $L$ with cardinality bigger than $p^{a_2}$.

Let $F$ be a small 3-flat, $\{x_1, x_2, x_3\}$ a basis of $F$. By (13), each of the lines $L_1 = \text{cl}(x_1, x_2)$, $L_2 = \text{cl}(x_2, x_3)$, $L_3 = \text{cl}(x_1, x_3)$ is in at most one large
3-flat. If some \( L_i \) is in no large 3-flat then every point in \( M \) is in some small 3-flat.

If, on the other hand, \( F_1, F_2, F_3 \) are large 3-flats containing \( L_1, L_2, L_3 \) respectively, then they meet in at most one point. Hence in any case

\[
\text{there is at most one point } x_0 \text{ not contained in a small 3-flat.} \quad (16)
\]

Now by (15), no small 3-flat contains a large line, so

\[
\text{every point except } x_0 \text{ is contained in a small line.} \quad (17)
\]

If \( L \) is any line containing \( x_0 \), then for any point \( x \) in \( L, x \neq x_0, p_{a_1} \mid |x| \) and \( M_x \) has small point cardinality \( p^d \) for some \( d, a_0 \geq d \geq a_1 \), hence \( p^d \mid |L - x_0| \), hence \( p_{a_1} \mid |x_0| \) and \( \alpha_1(M) = p_{a_1} \). Let \( K \) be any small \((n - 2)\)-flat of \( M \). By (15), \( K \) contains a small line of \( M \), hence a small point \( x \subset K \). By induction, every \( r \)-flat in \( K \) containing \( x, n - 2 \geq r \geq 2 \), is small in \( M \), hence every smallest \( r \)-flat containing \( x \) is a small \( r \)-flat of \( M \).

Since \( M_x \) is a connected matroid design of prime power index and rank \( n - 1 \), there are, by induction, numbers \( m = a'_{n-1} \geq a'_{n-2} \geq \cdots \geq a'_{1} \) such that every small \( r \)-flat of \( M_x \) has cardinality \( \sum_{i=1}^{r} p_{a_i} \). Then \( a'_{i} = a_{2} \), and setting \( a_i = a'_{i-1} \) for \( 2 \leq i \leq n - 1 \), we see that \( a_n \geq a_{n-1} \geq \cdots \geq a_1 \) and every small \( r \)-flat of \( M \) has cardinality \( \sum_{i=1}^{r} p_{a_i} \), proving (i).

We may deflate by \( p_{a_1} \), i.e., assume \( a_1 = 0 \) in what follows.

Now all large points lie on a common line \( L_0 \) because no small line contains two distinct large points and at most one point \( (x_0) \) is contained in two large lines.

Consider any small 3-flat in \( M \). Clearly, (13) implies that there is a small 3-flat \( F_0 \) not containing \( L_0 \). Hence there is a line \( L_1 \) in \( F_0 \) such that \( L_1 \cap L_0 = \emptyset \), and by (14) there is at most one large 3-flat containing \( L_1 \). Since \( r(L_0 \cup L_1) \leq 4 < n \) and \( M \) is connected, there are at least two 3-flats containing \( L_1 \) and not contained in \( \text{cl}(L_0 \cup L_1) = K \), hence at least one small 3-flat \( F_1 \) containing \( L_1 \) and not meeting \( L_0 \). By (15), \( F_1 \) contains no large lines, and since \( F_1 \cap L_0 = \emptyset \), (18) implies it contains no large points. Therefore \( F_1 \) is a simple, rank 3 MD with \( \alpha \)-sequence \( p_{a_3}, p_{a_2}, 1 \). The integer condition (1) then implies that \( a_3 \) is an even multiple of \( a_2 \).

If \( x \) is any large point contained in a small 3-flat, say \( F_2 \), then \( F_2 \) and \( F_1 \) are rank 3 MD's with the same \( \alpha \)-sequence \( p_{a_3}, p_{a_2}, 1 \) but one has a large point and the other does not. Then \( F_2 \) must satisfy Theorem 3(ii), which implies \( a_3 = (2t + 1)a_2 + b \) for some \( t \geq 1, b < a_2 \), which is impossible. Hence by (16), \( x_0 \) is the only possible large point. This proves statement (ii) for \( n \).

Suppose \( x_0 \) is contained in a small line. We will show that \( |x_0| = 1 \).
MATROID DESIGNS

If \( a_0 = 0 \) this is immediate. Hence suppose \( a_0 > 0 \), \( M_{a_0} \) has rank \( n - 1 \) and its \( \alpha \)-sequence is of form \( p^{a_n}, p^{a_{n-1}}, ..., p^{a_2} \) where \( a_n = a_n' \geq a_{n-1}' \geq \cdots \geq a_0' \). We have \( p^{a_2} + |x_0| = p^{a_2} + 1 \) and \( |x_0| = p^{a_2} - p^{a_2} + 1 \). Every hyperplane in \( M_{a_0} \) has cardinality \( \sum_{i=2}^{n-1} p^{a_i} \), hence

\[
\sum_{i=2}^{n-1} p^{a_i'} + |x_0| = \sum_{i=1}^{n-1} p^{a_i} = \alpha_{n-1}(M),
\]

so

\[
\sum_{i=3}^{n-1} p^{a_i'} + p^{a_2} + 1 = \sum_{i=3}^{n-1} p^{a_i} + p^{a_2} + 1,
\]

which implies

\[
\sum_{i=3}^{n-1} p^{a_i'} = \sum_{i=3}^{n-1} p^{a_i}
\]

and

\[
\left( \sum_{i=3}^{n-1} p^{a_i' - a_3'} + 1 \right) p^{a_3'} = \sum_{i=4}^{n-1} \left( p^{a_i' - a_3} + 1 \right) p^{a_3}.
\] (19)

Now, for all \( i \geq 4 \), \( a_i - a_3 \geq a_4 - a_3 \). If \( a_4 - a_3 = 0 \), then every small 4-flat \( K \) is just the union of two small 3-flats \( F_1, F_2 \) which intersect in a line. But then \( K \) contains simple lines and \( a_3 = 0 \), contrary to assumption. Likewise we have \( a_4' - a_3' \geq a_4' - a_3' \) for all \( i \), and \( a_4' - a_3' > 0 \), for if \( a_4' = a_3' \) then there is a 3-flat \( F \) containing \( x_0 \), \( F = L_1 \cup L_2 \), where \( L_1, L_2 \) are two small lines containing \( x_0 \). This implies again \( a_2 = 0 \), contrary to hypothesis.

Hence in (19) the two terms in brackets are prime to \( p \) (this uses the fact that \( n \geq 5 \)), hence by the unique factorization theorem \( a_3' = a_3 \). But then \( x_0 \) is contained in a 3-flat in \( M \) of cardinality \( p^{a_2} + p^{a_2} + |x_0| = p^{a_2} + p^{a_2} + 1 = \alpha_3(M) \), i.e., a small 3-flat of \( M \). This leads to a contradiction just as before. Therefore no small line contains a large point.

To prove (14), let \( F \) be a small \( s \)-flat and suppose \( F \) contains a large \( r \)-flat \( F' \) for some \( r, s \), where \( 1 \leq r \leq s \leq n - 2 \). If \( r > 1 \) then contracting at any point \( x \in F' \) yields a contradiction to the inductive hypothesis (15). Hence \( F' \) is a large point. But then \( F' \) is contained in a small line (namely, any line in \( F \)), contradicting (19). Statement (iii) follows at once.

Q.E.D.

For any given index \( p^m \) and rank \( n \), Theorem 4 may be used to determine the structural relations among the flats of any matroid design having the given index and rank, much as Theorem 3 was used to describe the rank 3 MD's in Corollary 3.2. In ranks greater than 3 the flats form "design-like" structures that are generalizations of transversal designs, and these structures must satisfy certain divisibility conditions similar to (1). However, an exhaustive description of these structures for arbitrary \( p^m \) and \( n \) is too
involved to pursue here, and the further question of their existence is, in
general, an unsolved problem. In the next sections we shall show the existence
of a new class of transversal designs and BIBD’s based on unitals, which in
particular can be used to construct certain classes of rank 3 MD’s of prime
power index.

4. Unitals

According to Corollary 3.2 all nontrivial rank 3 matroid designs of prime
power index \( p^m \) are of form \( p^{m-(2t+1)s-r} \) MD\( (p^{(2t+1)s}+1, p^r, p^s+1) \) where
\( 0 \leq r \leq s \). If \( r = 0 \) this is just an inflation of \( M \oplus p^s \) where \( M \) is a BIBD
with parameters \( (p^{(2t+1)s}+1, p^s+1, 1) = (q^{2t+1}+1, q+1, 1) \) where \( q = p^s \).
If \( 2t+1 = 3 \) (the simplest nontrivial case) such a BIBD is called a unital.
Unitals appear in a natural way in the study of the unitary polarities of
projective geometries. Given a unitary polarity of a Desarguesian projective
plane \( PG(2, q^2) \) (\( q \) a prime power) there are \( q^3+1 \) isotropic points and each
nonisotropic line contains \( q+1 \) such points, thereby giving rise to a unital,
[5], [1]. Bose [2] gives the following explicit construction of a unital for
any prime power \( q \).

Let the points of \( PG(2, q^2) \) be denoted by equivalence classes of triples
\( (a_1, a_2, a_3), a_i \in GF(q^2), \) not all \( a_i = 0 \). Bose defines the unitary polarity \( \pi \)
which takes any projective point \( A = (a_1, a_2, a_3) \) to the line \( L_A = \{(x_1, x_2, x_3): a_1q x_1 + a_2 q x_2 + a_3 q x_3 = 0\} \), called the polar of \( A \), and \( \pi \) maps
each line \( L = \{(x_1, x_2, x_3): b_1 x_1 + b_2 x_2 + b_3 x_3 = 0\} \) to the point
\( (b_1^{1/q}, b_2^{1/q}, b_3^{1/q}) \). The isotropic points \( (x_1, x_2, x_3) \) of \( \pi \) are those lying on
their own polars, i.e., those satisfying

\[
x_1^{q+1} + x_2^{q+1} + x_3^{q+1} = 0. \tag{20}
\]

It may then be shown [2] first, the set \( C \) of all isotropic points has cardinality
\( q^3 + 1 \); second, if \( A \in C \) then \( L_A \) intersects \( C \) at exactly one point (thus \( L_A \)
is tangent to \( C \)); finally, any secant to \( C \) (i.e., any line meeting \( C \) in at least
two distinct points) meets \( C \) in exactly \( q+1 \) points. Thus \( C \) together with
the secant lines form a unital with parameters \( v = q^3 + 1, k = q + 1, \lambda = 1 \). Any unital obtainable in this way we call a Bose unital. A BIBD
\( (E, B) \) is said to be resolvable if the block family \( B \) can be partitioned into
classes \( C_1, C_2, \ldots, C_n \) such that each class \( C_i \) partitions \( E \). Then we have [2]:

every Bose unital is resolvable. \( \tag{21} \)

The fundamental axiom of projective geometry is Pasch’s axiom, which
states that if distinct lines \( L_1 \) and \( L_2 \) meet at point \( x \), and distinct lines \( L_3 \)
and $L_4$ each meet both $L_1$ and $L_3$ at points different than $x$, then $L_3$ meets $L_4$. In a BIBD with $\lambda = 1$, a *Pasch configuration* is defined to be a set of four distinct lines (i.e., blocks) such that each of the lines intersects the other three in distinct points. (See Fig. 1.)

![Fig. 1. The Pasch configuration.](image)

It may then be shown [13, 10] that no Bose unital contains a Pasch configuration. This distinguishes the Bose unitals from the other known unitals, all of which do contain Pasch configurations. One such class is obtained from Ree groups [11] but only applies to the case where $q$ is an odd power of 3. Another class is due to Ganley [8] but again it does not include all prime powers $q$. The only other known unital is a specific construction for $q = 5$ due to Hanani. This unital is constructed by considering the 126 element set $G \cup \{\infty\}$, where $G = GF(5) \times GF(25)$, and the base blocks:

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

$$
\{(0, t^{6\alpha+5}), (0, t^{6\alpha+14}), (1, t^{6\alpha+4}), (1, t^{6\alpha+16}), (3, t^{6\alpha+11}), (3, t^{6\alpha+23})\},
$$

where $\alpha = 0, 1$, $t$ is a primitive root of $GF(25)$, namely $t^2 + 3t + 3 = 0$, and the blocks are developed cyclically over the additive group $GF(5) \times GF(25)$. The blocks containing $\infty$ are

$$
\{(0, \beta), (1, \beta), (2, \beta), (3, \beta), (4, \beta), \infty\}, \quad \beta \in GF(25).
$$

It may be verified [10] that the Hanani unital contains Pasch configurations, and is therefore not a Bose unital.

Kestenband [10] discusses a general approach to obtaining new unitals for any odd prime power $q$, but does not succeed in constructing them except for $q = 5$, which gives a result isomorphic to Hanani’s.

In the next section we shall show how unitals may be used to construct all BIBD’s with parameters $(q^{2t+1} + 1, q + 1, 1)$, $q$ a prime power, and in fact much more general classes of BIBD’s.
5. CONSTRUCTION OF MATROID DESIGNS AND A NEW FAMILY OF TRANSVERSAL DESIGNS

In this section we will show the existence of a general family of transversal designs, and as particular corollaries derive the existence of certain classes of rank 3 matroid designs of prime power index. The principal theorem is the following.

**Theorem 5.** For any prime power \( q \), and integers \( h' \geq 0, 0 \leq n_0 < n_1 < \cdots < n_r \), where \( n_i \equiv i (\text{mod } 2) \), \( h = 0 \) implies \( n_0 = 0 \) and \( n_0 = 0 \) implies \( r \geq 1 \), TD\(_2\)(\( q^{n_0} + q^{n_1} + \cdots + q^{n_r} \), \( q^h \), \( q + 1, 1 \)) exists.

We begin by proving the following:

**Lemma 5.1.** 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 the projective geometry PG\((n, q)\) over the finite field GF\((q)\), with hyperplane family \( \mathcal{H} \) and line family \( \mathcal{L} \), consider a point \( a \) and let:

\[
\begin{align*}
E &= \text{PG}(n, q) - \{a\}, \\
\mathcal{L} &= \{L - \{a\}: L \in \mathcal{L}, a \in L\}, \\
\mathcal{T} &= \{H: H \in \mathcal{H}, a \notin H\}. 
\end{align*}
\]

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

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

\[
v = |\mathcal{L}| = (q^n - 1)/(q - 1).
\]

Then no line containing \( a \) meets any hyperplane not containing \( a \) in more than one point; hence no two points \( b, c \in S \in \mathcal{L} \) 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 \(\mathcal{T}\).

Hence

\[
\lambda = \frac{q^{n-1} - 1}{q - 1} - \frac{q^{n-2} - 1}{q - 1} = q^{n-2}.
\]

This completes the proof. Q.E.D.

Lemma 5.1 generalizes a construction in [3, p. 183].
At this point, a further definition is needed. 

\( A(v, k, \lambda) \)-BIBD on a set \( E \) is called centrally resolvable if there exists an element \( a \in E \) such that

\[
E - \{a\} = \bigcup_{i=1}^{(v-1)/(k-1)} E_i, \quad \text{where} \quad |E_i| = k - 1 \text{ for all } i,
\]

the \( E_i \)'s are mutually disjoint and the sets \( \{a\} \cup E_i \) appear as blocks in the design, each \( \lambda \) times, for all \( i \).

**Lemma 5.2.** The existence of a centrally resolvable \( (v, k, \lambda) \)-BIBD is equivalent to the existence of a \( TD_2((v - 1)/(k - 1), k - 1, k, \lambda) \).

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

The converse is now obvious. \( \blacksquare \)

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

**Lemma 5.3.** The existence of a \( (v, k, 1) \)-BIBD is equivalent to the existence of a \( TD_2((v - 1)/(k - 1), k - 1, k, 1) \).

The next four lemmas enable us to construct new designs by composing known ones.

**Lemma 5.4.** If there exist a \( TD_4(w, s', v, \lambda') \) and a \( TD_4(v, s, k, \lambda) \), then there exists a \( TD_4(w, ss', k, \lambda \lambda') \). Furthermore, resolvability of the first two designs implies resolvability of the last.

**Proof.** The first statement is a slight modification of [17, (133)]. As for the second statement, that is a straightforward consequence of the method of construction. \( \blacksquare \)

**Lemma 5.5.** If there exists a \( (w, u, 1) \)-BIBD and a \( (nu + 1, n + 1, 1) \)-BIBD, then there exists a \( (nw + 1, n + 1, 1) \)-BIBD. Moreover, if the first two BIBD's are resolvable, so is the last.

**Proof.** Aside from resolvability, this has been proved in [9, Proposition 3.10]. Proving resolvability:

Let \( A = \{z\} \cup (\bigcup_{i=1}^{n} E_i) \), where \( |E_i| = w, i = 1, 2, \ldots, n \), and \( E_i \cap E_j = \emptyset \) for \( i \neq j \) and \( \emptyset \notin E_i \) for any \( i \), so that \( |A| = nw + 1 \).

We introduce the following notation:

\[
\frac{w - 1}{u - 1} = r; \quad \frac{w}{u} = s; \quad \frac{nu + 1}{n + 1} = t.
\]
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,

\[ \mathcal{B}_{ij} = \{B_{ij}^1, B_{ij}^2, \ldots, B_{ij}^s\} \]

and

\[ |B_{ij}^k| = u \quad \text{for all } i, j, k. \quad (22) \]

Also

\[ \bigcup_{k=1}^{s} B_{ij}^k = E_i \quad \text{for all } j. \quad (23) \]

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

\[ |F_j^k| = nu + 1, \quad \text{by (22)}. \]

We construct now on each \(F_j^k\) a resolvable \((nu + 1, n + 1, 1)\)-BIBD with block family \(\mathcal{C}_j^k\), in such a way that for any \(i, j, k\):

\[ |C \cap B_{ij}^k| = 1 \quad \text{for any } C \in \mathcal{C}_j^k \text{ such that } z \in C. \quad (24) \]

If \(T_j^k\) is the subfamily of \(\mathcal{C}_j^k\) consisting of all blocks containing \(z\), then \(\bigcup_{k=1}^{s} T_j^k\) can be made to be the same collection of blocks, regardless of \(j\). This can be achieved by virtue of (23).

By resolvability, \(\mathcal{C}_j^k = \bigcup_{h=1}^{u} \mathcal{C}_{jh}^k\), where \(\mathcal{C}_{jh}^k\) 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 \(C \in \mathcal{C}_j^k\) and since for any fixed \(j, k\) and any \(C \in \mathcal{C}_j^k\) there exists a unique \(h\) such that \(C \in \mathcal{C}_{jh}^k\), we see that:

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

\[ C \in \mathcal{C}_{jh}^k. \quad (25) \]

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 (25) holds and consider

\[ \mathcal{D}_C = \bigcup_{j=1}^{r} \mathcal{C}_{jh}^k \]

**Claim:** \(\mathcal{D}_C\) is a parallel class of blocks of the BIBD on \(A\).
To prove this, we observe that for any fixed $j$, the blocks in $\mathcal{C}_j^k \subset \mathcal{D}_C$ contain all points of $F_j^k$, each once. For a different $j$, say $j'$, the blocks in $\mathcal{C}_{j'}^k \subset \mathcal{D}_C$ 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 $\mathcal{D}_C$ account for the following number of different points of $A$.

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

i.e., all the points of $A$. Q.E.D.

**Lemma 5.6.** If there exists a $\text{TD}_2(w + 1, s, k, \lambda)$ and a $\text{TD}_2(v, sw, k, \lambda)$, then there exists a $\text{TD}_2(sw + 1, s, k, \lambda)$.

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

To obtain the required $\text{TD}_2$, we first construct for $i = 1, 2, \ldots, v$, a design $(E_i, \mathcal{S}_i, \mathcal{T}_i) \equiv \text{TD}_2(w + 1, s, k, \lambda)$, where:

$$\mathcal{S}_i = \{S_{(i-1)w+1} : j = 1, 2, \ldots, w\} \cup \{S_{sw+1}\}$$

and $E_i = \bigcup_{S_h \in \mathcal{S}_i} S_h$.

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

We construct an $(E - S_{sw+1}, \mathcal{F}, \mathcal{T}_i) \equiv \text{TD}_2(v, sw, k, \lambda)$, where $\mathcal{F} = \{F_1, F_2, \ldots, F_v\}$.

Now, $(E, \mathcal{F}, \bigcup_{i=1}^v \mathcal{T}_i \cup \mathcal{F})$ is the desired $\text{TD}_2(sw + 1, s, k, \lambda)$. Q.E.D.

**Lemma 5.7.** If there exists a $\text{TD}_2(w, ss', k, \lambda)$ and a $\text{TD}_2(s', s, k, \lambda)$, then there exists a $\text{TD}_2(ws', s, k, \lambda)$.

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

We construct an $(E, \mathcal{S}', \mathcal{F}) \equiv \text{TD}_2(w, ss', k, \lambda)$ where

$$\mathcal{S}' = \bigcup_{i=0}^{s'-1} S_{i+fw} : i = 1, 2, \ldots, w \bigcup_{S_h \in \mathcal{S}} S_h.$$

Next, for each $i = 1, 2, \ldots, w$, we construct an $(E_i, \mathcal{S}_i, \mathcal{T}_i) \equiv \text{TD}_2(s', s, k, \lambda)$ where $\mathcal{S}_i = \{S_i, S_{i+sw}, \ldots, S_{i+(s'-1)w}\}$ and $E_i = \bigcup_{S_h \in \mathcal{S}_i} S_h$.

Then $(E, \mathcal{F}, \bigcup_{i=1}^w \mathcal{T}_i \cup \mathcal{F})$ is the required $\text{TD}_2(ws', s, k, \lambda)$. Q.E.D.

We note next the following

**Lemma 5.8.** Where $q$ is any prime power, there exist resolvable $(1 + q^{2t+1}, 1 + q, 1)$-BIBD's for any $t \geq 0$. 
Proof. There exist resolvable \((1 + q^9, 1 + q, 1)\)-BIBD's, by (21). Also, there exist resolvable \((q^{2t}, q^2, 1)\)-BIBD's, the affine geometry \(AG(t, q^2)\) being such a design.

Apply now Lemma 5.5 with \(w = q^{2t}, u = q^2, n = q\), to obtain the desired BIBD. Q.E.D.

Lemma 5.8 solves the problem of constructing rank 3 matroid designs corresponding to the case \(r = 0\) in Corollary 3.2.

We are prepared now to prove Theorem 5.

Proof of Theorem 5. In a \(TD_2(v, s, k, \lambda)\), the replication number \(r\) represents the number of blocks containing any given element and is given [17] by:

\[
r = \lambda(v - 1)s/(k - 1).
\]

In the case of the \(TD_2\) required by Theorem 5, we obtain:

\[
r = (q^{n_0} + \cdots + q^{n_r} - 1) q^h.
\]

Thus, \(h = 0\) implies \(n_0 = 0\).

If \(n_0 = 0 = r\), we get a \(TD_2(1, q^h, q + 1, 1)\) which cannot exist and hence \(n_0 = 0\) implies \(r \geq 1\).

Let first \(n_0 = 0\); we then have to construct a

\[TD_2(1 + q^{n_1} + \cdots + q^{n_r}, q^h, q + 1, 1),\]

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 Lemma 5.8, if and only if \(n_1 \equiv 1 \text{ mod } 2\).

\(TD_2(q + 1, q^h, q + 1, 1)\) exists also: if \(h = 0\) it is a trivial BIBD and if \(h > 0\), we substitute \(q^h\) for \(q\) in Lemma 5.1, then let \(n = 2\) and \(v = q + 1\).

We apply now Lemma 5.4 with \(t = 2\) and

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

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

Hence the theorem holds for \(n_0 = 0, h \geq 0\) and \(r = 1\).

Assume that it holds for \(n_0 = 0, h \geq 0\) and some fixed \(r \geq 1\), i.e., \(TD_2(1 + q^{n_1} + \cdots + q^{n_r}, q^h, q + 1, 1)\) exists where \(n_1 < n_2 < \cdots < n_r\).

Let us use Lemma 5.6 with:

\[
w = q^{n_1}, \ v = 1 + q^{n_2-n_1} + \cdots + q^{n_{r+1} - n_1}, \ s = q^k, \ k = q + 1, \ \lambda = 1,
\]

where \(n_1 < n_2 < \cdots < n_{r+1}\).
MATROID DESIGNS

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

$TD_2(v, sw, k, \lambda)$ is $TD_2(1 + q^{n_2-n_1} + \cdots + q^{n_{r+1}-n_1}, q^{h+n_1}, q + 1, 1)$

and exists by the inductive hypothesis, since $0 < n_2 - n_1 < \cdots < n_{r+1} - n_1$ and $n_i - n_i \equiv i - 1 \mod 2$ for $i = 2, 3, \ldots, r + 1$.

Hence $TD_2(vw + 1, s, k, \lambda)$ exists; but this is $TD_2(1 + q^{n_1} + q^{n_2} + \cdots + q^{n_{r+1}}, q^h, q + 1, 1)$ and hence the theorem is valid for $r + 1$, which completes the induction for the case $n_0 = 0$.

We now turn to the case $n_0 \neq 0$. If $n_0 \neq 0, h \neq 0$ either, for $h = 0$ implies $n_0 = 0$. If now $r = 0$, we have $TD_2(q^{n_0}, q^h, q + 1, 1)$ with $n_0 \geq 2$. A $(q^{n_0+1}, q + 1, 1)$-BIBD exists by Lemma 5.8. By Lemma 5.3, this is equivalent to $TD_2(q^{n_0}, q, q + 1, 1)$. Hence $TD_2(q^{n_0}, q^h, q + 1, 1)$ exists for $h = 1$.

Assume now that $TD_2(q^{n_0}, q^h, q + 1, 1)$ exists for some $h$. Lemma 5.1, for $n = 2$, supplies a $TD_2(q + 1, q, q + 1, 1)$. We apply now Lemma 5.4 with $t = 2$ and $w = q^{n_0}$, $s' = q^h$, $v = k = q + 1$, $\lambda = \lambda' = 1$, $s = q$, to obtain $TD_2(q^{n_0}, q^{h+1}, q + 1, 1)$ and this completes the induction, showing that $TD_2(q^{n_0}, q^h, q + 1, 1)$ exists.

Having disposed of the case $r = 0$, we now let $r \geq 1$ and apply Lemma 5.7 with:

$w = 1 + q^{n_1-n_0} + \cdots + q^{n_r-n_0}$, $s = q^h$, $s' = q^{n_0}$, $k = q + 1$, $\lambda = 1$.

The hypotheses of Lemma 5.7 are satisfied: $TD_2(w, ss', k, \lambda)$ is $TD_2(1 + q^{n_1-n_0} + \cdots + q^{n_r-n_0}, q^{h+n_0}, q + 1, 1)$, which has already been shown to exist, since $n_i - n_0 \equiv i \mod 2$ for $i = 1, 2, \ldots, r$. $TD_2(s', s, k, \lambda)$ is $TD_2(q^{n_0}, q^h, q + 1, 1)$ which has been obtained above.

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

Q.E.D.

**Corollary 5.1.** $(1 + q + q^{2t+2}, 1 + q, 1)$-BIBD's exist for any prime power $q$ and any $t \geq 0$.

**Proof.** Apply Theorem 5 with $h = n_0 = 0$, $n_1 = 1$, $n_2 = 2t + 2$ Q.E.D.

This corollary solves the problem of constructing the rank 3 matroid designs corresponding to the case $r = s$ in Corollary 3.2.

Another immediate consequence of Theorem 5 which is worth mentioning is the following:

**Corollary 5.2.** For any prime power $q$, there exists a $(1 + q^{n_1} + q^{n_2} + \cdots + q^{n_r}, 1 + q, 1)$-BIBD, where $r \geq 1$, $n_i \equiv i \mod 2$ ($i = 1, 2, \ldots, r$) and $n_1 < n_2 < \cdots < n_r$.

The projective geometry $PG(r, q)$ is clearly a particular case of these designs, namely when $n_i = i$, $i = 1, 2, \ldots, r$. 


In conclusion, we have shown that the rank 3 matroid designs
\[ p^{m-(2^{r-1})s-r} \text{MD}(p^{(2^{r-1})s+1}, p^r, p^s+1), \quad 0 \leq r \leq s, \]
of Corollary 3.2 exist if \( r = 0 \) or \( r = s \). We conjecture that all such matroid designs exist, though we do not know of a construction at this time. Equivalently, we would like to show that all transversal designs of type \( TD_3(1 + p^{(2^{r-1})s}, p^r, p^s+1, 1) \) with \( 0 < r < s \) exist (\( p \) a prime). This would completely solve the existence problem for rank 3 matroid designs of prime power index.

REFERENCES


Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.