JOURNAL OF RESEARCH of the National Bureau of Standards — B. Mathematical Sciences
Vol. 77B, Nos. 1 & 2, January–June 1973

Matroid Designs*

Peyton Young and Jack Edmonds*****

(November 22, 1972)

Matroids are investigated in which equicardinality conditions are imposed on the flats. Such matroids are shown to be closely related to certain types of BIBD's. Existence and uniqueness theorems for these structures are derived, together with a boundedness criterion on their rank. Several classes are exhibited, including finite projective and affine geometries, certain t-designs (Steiner systems) and so-called trivioids. By viewing certain t-designs as matroids, new ways of constructing BIBD's are derived. Three new series of 3-designs and two new 4-designs are obtained by these methods. A matroid analysis of the 5-(24,8,1) design of Witt is presented, and examples are obtained from it of matroids having equicardinal hyperplanes but not equicardinal flats in lower ranks. Several general conjectures and existence problems for these types of matroids are suggested.

Key words: Balanced incomplete block designs; matroid designs; matroids.

1. Introduction

In this paper we shall investigate mathematical structures that bring together matroid theory and the theory of balanced incomplete block designs (BIBD's). From this unification we shall derive a number of new results in both of these fields. We shall be interested in two special types of matroids: those in which the hyperplanes are equicardinal, (called matroid designs), and those in which the flats of any given rank are equicardinal, (called perfect matroid designs). Matroid designs were first introduced under the name "equicardinal matroids" by U.S.R. Murty [10].[1]

Perfect matroid designs exhibit the high degree of regularity found in the classical finite projective and affine geometries; however, they comprise a variety of other structures, including t-designs (Steiner-systems) and so-called trivioids. They also represent a highly specialized class of BIBD's. Indeed, their complexity is indicated by the fact that the families of flats of any two different ranks form a BIBD. We shall develop a useful parametric description of perfect matroid designs that provides a classification of known examples and systematic framework for the search for new ones. Consistency conditions on the parameters are derived as well as additional types of existence conditions arising from the matroid structure. These conditions are used to tabulate all perfect matroid designs with less than forty-five points. We also explore the structure of perfect matroid designs, and show how certain known t-designs, when regarded as matroids, yield constructions of new t-designs.

Matroid designs in general may be viewed as variants of BIBD's. Frequently they consist of BIBD's that have been modified by the addition of certain objects and blocks. In this paper we show that matroid designs do indeed encompass a wider class of structures than perfect matroid designs, and we shall present a number of examples that will be derived from a matroid analysis of the famous 5-(24, 8, 1) design of Witt [13].

AMS subject classification: Primary 05, Secondary 20.
* An invited paper.
** Present address: City University of New York, Graduate School and University Center, New York, N.Y.
*** Present address: University of Waterloo, Waterloo, Ontario.
[1] Figures in brackets indicate the literature references at the end of this paper.

We begin with a development of the necessary theory, and then present the theory of perfect matroid designs. In the last section, we shall analyze the Witt design and give constructions of other types of matroid designs.

2. Matroids

A *matroid* $M = (E, \mathscr{I})$ is defined to be a finite set E together with a nonempty set $\mathscr{I}$ of subsets of E, called *independent* sets, such that:
(I 1) $\emptyset$ is independent and every subset of an independent set is independent;
(I 2) for every $A \subseteq E$, all maximal independent subsets of A have the same cardinality, called the *rank* of A, $r(A)$.

A maximal independent subset of A is called a *basis of* A, or M*-basis of* A, if we wish to specify the matroid under consideration. *A basis of* M is just an M-basis of E, and $r(M)$, the *rank of* M, is equal to $r(E)$. For convenience, it will always be assumed in the sequel that the function designated by r is the rank function of the matroid designated by M.

A subset of E that is not independent is said to be *dependent*, and the minimal dependent sets are called *circuits*.

A fundamental relation between independent sets and circuits is the following:
(1) THEOREM: *For any independent subset* J *of a matroid* (E, $\mathscr{I}$), *and any* $x \in E - J$, $J \cup \{x\}$ *contains at most one circuit.*
PROOF: Suppose to the contrary that x is contained in two distinct circuits C_1 and C_2. Let J' be any basis of $J \cup \{x\}$ containing $C_1 \cap C_2$. Then $|C_1 - J'| \geq 1$ and $|C_2 - J'| \geq 1$, so

$$|J'| \leq |J \cup \{x\}| - 2 < |J|.$$

But then J' and J are two bases of $J \cup \{x\}$ of different cardinalities, contradicting (I 2).
(2) THEOREM: *Let* $\mathscr{C}$ *be a family of subsets of a finite set* E. $\mathscr{C}$ *is the circuit-family of a matroid on* E *if and only if*

(C1) $\emptyset \notin \mathscr{C}$ *and no member of* $\mathscr{C}$ *is a proper subset of another.*

(C2) *For any two distinct members* C_1 *and* C_2 *of* $\mathscr{C}$ *and* $x \in C_1 \cap C_2$, $C_1 \cup C_2 - \{x\}$, *contains a member of* $\mathscr{C}$.

PROOF: Let $(E, \mathscr{I})$ be a matroid with circuit family $\mathscr{C}$. $\emptyset$ is independent, so $\emptyset \notin \mathscr{C}$. Then (C1) follows from the definition of circuit, and (C2) is an immediate consequence of (1). Conversely, let $\mathscr{C}$ satisfy (C1) and (C2), and let $\mathscr{I}$ be the family of subsets of E containing no members of $\mathscr{C}$. Then $\emptyset \in \mathscr{J}$ and (I1) clearly holds. Suppose that (I2) does not hold for some subset A. Let $\mathscr{J}$ be the family of *maximum cardinality* members of $\mathscr{I}$ in A, *and* $\mathscr{J}'$ the family of all other *maximal* members of $\mathscr{I}$ in A. Let $|J_1 \cap J_2|$ be maximum among all $J_1 \in \mathscr{J}$, $J_2 \in \mathscr{J}'$. Then for $x \in J_2 - J_1$, $J_1 \cup \{x\}$ contains a member C of $\mathscr{C}$ containing x. If C' were another such member of $\mathscr{C}$, then by (C2), J_1 would contain a member of $\mathscr{C}$, contradicting $J_1 \in \mathscr{I}$. Hence C is unique. Further, $C \not\subseteq J_2$, so let $y \in C \cap (J_1 - J_2)$. By the uniqueness of C, $J_1' = (J_1 - \{y\}) \cup \{x\} \in \mathscr{I}$. Then $|J_1'| = |J_1|$, so $J_1' \in \mathscr{J}'$, but $|J' \cap J_2| > |J_1 \cap J_2|$, a contradiction. Hence $\mathscr{J}' = \emptyset$, and (I2) is proved.

Let $M = (E, \mathscr{I})$ be a matroid. For any $x \in E$ and $A \subseteq E$, x is said to *depend* on A if $x \in A$ or $\{x\} \cup A$ contains a circuit containing x. The *closure* of A, $cl\,(A)$, is the set of all elements that depend on A, and A is said to be a *closed set*, or *flat*, if $cl\,(A) = A$. We write $cl_M(A)$ if we wish to emphasize that closure is taken with respect to M.
(3) It follows easily from the above definition that the intersection of a family of closed sets is closed. We may characterize the closure of a set as follows.
(4) THEOREM: *For any* $A \subseteq E$, *cl* (A) *is the unique maximal set* S *such that* $A \subseteq S \subseteq E$ *and* $r(A) = r(S)$.

PROOF: Let S be some maximal set such that $A \subseteq S \subseteq E$ and $r(A)=r(S)$. Let $x \in cl(A)-A$, C a circuit such that $x \in C \subseteq A \cup \{x\}$. By definition of circuit, $C-\{x\}$ is independent in A, hence it is contained in a basis J of A. Since $r(A)=r(S)$ and $A \subseteq S$, J is also a basis of S. However $J \cup \{x\}$ is dependent, hence J is a basis of $S \cup \{x\}$ and $r(S \cup \{x\})=r(S)$. By the maximality of S, it follows that $x \in S$. Hence $cl(A) \subseteq S$. On the other hand, let $x \in S-A$ and let J be any basis of A. Then $J \cup \{x\}$ is dependent, so $J \cup \{x\}$ contains a circuit C containing x; hence $x \in cl(A)$. Therefore $S \subseteq cl(A) \subseteq S$, so $S=cl(A)$, and S is unique.

(5) COROLLARY: $cl(cl(A) \cup B)=cl(A \cup B)$ *for any subsets* A,B *of* E.

(6) A *k-flat* of a matroid $M=(E, \mathscr{I})$ is defined to be a closed subset of E having rank k, or (by (4)) a maximal subset of E having rank k. The *hyperplanes* of M are its $(r(M)-1)$ − flats. The following relationship between the hyperplanes and bases of M is immediate.

(7) The hyperplanes of a matroid M are the maximal subsets containing no basis, and the bases of M are the minimal subsets contained in no hyperplane.

(8) THEOREM: *If* $\mathscr{B}$ *is the basis family of a matroid* $M=(E, \mathscr{I})$, *then* $\mathscr{B}^*=\{E-B\colon B \in \mathscr{B}\}$ *is the basis family of a matroid* M^*, *called the dual of* M. *The circuits of* M^* *are precisely the set-complements of the hyperplanes of* M.

PROOF. Let $\mathscr{C}^*=\{E-H\colon H$ is a hyperplane of $M\}$. Clearly, $\mathscr{C}^*$ satisfies (C1).

Applying (7), we also see that the members of $\mathscr{B}^*$ are precisely the maximal subsets of E containing no member of $\mathscr{C}^*$. For any distinct $C_1^*, C_2^* \in \mathscr{C}^*$ and $x \in C_1^* \cap C_2^*$, suppose $S=C_1^* \cup C_2^*-\{x\}$ contains no member of $\mathscr{C}^*$. Then $S \subseteq B^*$ for some $B^* \in \mathscr{B}^*$, and $x \notin B^*$. Letting $H_1=E-C_1^*$, $H_2=E-C_2^*$, and $B=E-B^*$, we have that $B-\{x\} \subseteq H_1 \cap H_2$. Since $r(B-\{x\})=r(H_1)=r(H_2)$, it follows from (4) that $H_1=H_2$ and $C_1^*=C_2^*$, a contradiction. Thus $\mathscr{C}^*$ also satisfies (C2), so it is the circuit family of a matroid M^*. By the first sentence above, it follows that $\mathscr{B}^*$ is the basis-family of M^*.

We note that $M^{**}=M$. The complements of the hyperplanes of M (i.e., the circuits of M^*) are also called the *co-circuits* of M. Using (2) and (8), we may characterize the hyperplane-family of a matroid as follows.

(9) THEOREM: *Let* $\mathscr{H}$ *be a family of subsets of a finite set* E, $E \notin \mathscr{H}$. $\mathscr{H}$ *is the hyperplane family of a matroid on the set* E *if and only if*

(H1) *No member of* $\mathscr{H}$ *is a proper subset of another.*

(H2) *For any two distinct members* H_1 *and* H_2 *of* $\mathscr{H}$, *and any* $x \in E$, $\{x\} \cup (H_1 \cap H_2)$ *is contained in some member of* $\mathscr{H}$.

Although a matroid may be equally well characterized by its independent sets, its circuits, or its hyperplanes, we shall find it most useful to present it "geometrically" in terms of its hyperplanes, or more generally, its flats. We shall henceforth denote a matroid on the set E with hyperplane-family $\mathscr{H}$ by $(E, \mathscr{H})$.

Let $M=(E, \mathscr{H})$ be any matroid.

(10) The 0-flat of M, F^0, is unique and consists of all elements not contained in any basis of M. Such elements are called *loops.* By the definition of closure, F^0 is a subset of every flat. Hence we may exclude all loops from M without essentially altering the set relationships among the various flats.

(11) To simplify the presentation of later results, we shall therefore always assume in the sequel that M has no loops.

(12) The 1-flats or *points*, of M are analogous to geometric points in the sense that every flat F is partitioned by the points that meet it. This follows immediately from (3), (4), and the assumption that the 0-flat of M is null.

(13) A 2-flat of M is called a *line.* For any two distinct points a and b of M, $r(a \cup b)=2$, because $\{x, y\}$ is a basis of $a \cup b$ for any $x \in a$ and $y \in b$. Hence a and b are contained in a unique line of M, namely $cl(a \cup b)$.

The following theorem expresses a basic fact about the structure of flats in a matroid.

(14) THEOREM: *Let* M *be a rank* n *matroid. For any* i-*flat* F^i *and* k-*flat* F^k *of* M *such that* $F^i \subset F^k$,

493-033 OL - 73 - 2

$0 \leqslant i < k \leqslant n$, $F^k - F^i$ *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.

PROOF: Let F^i and F^k be given as above, and let J be a basis of F^i. For any $x \in F^k - F^i$ and basis J of F^i, $J \cup \{x\}$ is independent, and, by (5), $cl(J \cup \{x\}) = cl(F^i \cup \{x\})$. Hence $F_x^{i+1} = cl(F^i \cup \{x\})$ is an $(i+1)$-flat containing F^i and x. If $F_x^{i+1} \not\subseteq F^k$, then $F_x^{i+1} \cap F^k$ would be a flat properly containing the i-flat F^i, and properly contained in the $(i+1)$-flat F_x^{i+1}, which is absurd. Hence every element $x \in F^k - F^i$ is contained in an $(i+1)$-flat F_x^{i+1} such that $F^i \subseteq F_x^{i+1} \subseteq F^k$. Finally, if A and B are any two distinct $(i+1)$-flats that contain F^i and are contained in F^k, then $A \cap B$ is a flat containing the i-flat F^i and properly contained in the $(i+1)$-flat A. Hence $A \cap B = F^i$, and $(A - F^i) \cap (B - F^i) = \emptyset$. Thus 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, partition $F^k - F^i$.

3. Perfect Matroid Designs

3.1. The Geometry of Flats in a Perfect Matroid Design

The geometric structure imposed on the flats of a matroid by (14) is not nearly as restrictive as the structure of the classical finite affine and projective geometries. We propose to investigate matroids that bear a closer resemblance to the classical geometries, in that equicardinality conditions are imposed on their flats. We shall find that these structures constitute a very special and intriguing class of block designs.

(15) A matroid M is said to be a *matroid design* if all of its hyperplanes have the same cardinality, which we denote by $k(M)$. If, for every integer j, $0 \leqslant j \leqslant r(M)$, all of the j-flats of M have the same cardinality $\alpha(j)$, then M is called a *perfect matroid design*, abbreviated by *PMD*. Like the finite geometries whose properties it generalizes, PMD's exhibit strong regularities of structure in addition to the equicardinality of the flats of a given rank.

(16) THEOREM: *Let* M *be a rank* n *PMD. For any integers* i, j, k, *such that* $0 \leqslant i \leqslant j \leqslant k \leqslant n$, *and any* i*-flat* F^i *and* k*-flat* F^k *such that* $F^i \subseteq F^k$, *the number* $t_M(i, j, k)$ *of* j*-flats* F^j *such that* $F^i \subseteq F^j \subseteq F^k$ *is independent of the choice of* F^i *and* F^k. *Moreover, the function* $t_M(i, j, k)$ *so defined satisfies the following relations.*

(T0) $$t_M(i, i, k) = 1, \quad 0 \leqslant i \leqslant k \leqslant n,$$

and

$$t_M(0, 1, i+1) > t_M(0, 1, i), \quad 1 \leqslant i \leqslant n-1.$$

(T1) $$t_M(i, i+1, k) = \frac{t_M(0, 1, k) - t_M(0, 1, i)}{t_M(0, 1, i+1) - t_M(0, 1, i)}, \quad 0 \leqslant i < k \leqslant n.$$

(T2) $$t_M(i, j, k) = \frac{t_M(i, l, k)\, t_M(l, j, k)}{t_M(i, l, j)}, \quad 0 \leqslant i \leqslant l \leqslant j \leqslant k \leqslant n.$$

PROOF: For given i and k, $0 \leqslant i \leqslant k \leqslant n$, and any given i-flat F^i and k-flat F^k such that $F^i \subseteq F^k$, F^i is clearly the only i-flat containing F^i and contained in F^k. Hence $t_M(i, i, k) = 1$ for every choice of F^i and F^k. Moreover, where F^{i+1} is any $(i+1)$-flat containing F^i, we have $F^i \underset{\neq}{\subset} F^{i+1}$, and hence, by (12), F^{i+1} contains more points than does F^i.

(17) Where $\alpha(k)$ is the number of elements in any k-flat of M, the number of points in any k-flat of M is clearly $\alpha(k)/\alpha(1)$, and hence $t_M(0, 1, k)$ is well-defined for every k, $1 \leqslant k \leqslant n$. For any i and

k, $1 \leq i < k \leq n$, and for any i-flat F^i and k-flat F^k such that $F^i \subseteq F^k$, it follows from (14) that the number of $(i+1)$-flats F^{i+1} such that $F^i \subseteq F^{i+1} \subseteq F^k$ is

$$\frac{\alpha(k)-\alpha(i)}{\alpha(i+1)-\alpha(i)} = \frac{t_M(0,1,k)-t_M(0,1,i)}{t_M(0,1,i+1)-t_M(0,1,i)},$$

which is independent of the particular F^i and F^k chosen. Thus we have shown that $t_M(i, i+1, k)$ is well-defined for every i and k, $0 \leq i < k \leq n$, and that (T1) holds.

Now let i be fixed, $0 \leq i \leq n$. We shall prove by induction on j, $i \leq j \leq n$, that for every k, $j \leq k \leq n$, $t_M(i, j, k)$ is well-defined. We have already shown this for $j = i$ and $j = i+1$. Suppose we have shown that $t_M(i, j, k)$ is well-defined for every j, $i \leq j \leq j_0$. If $j_0 = n$, we are done. Otherwise, choose $k \geq j_0 + 1$ and let F^i be an i-flat, F^k a k-flat such that $F^i \subseteq F^k$. Let V^{j_0} denote the set of j_0-flats F^{j_0} such that $F^i \subseteq F^{j_0} \subseteq F^k$, and let V^{j_0+1} denote the set of (j_0+1) — flats F^{j_0+1} such that $F^i \subseteq F^{j_0+1} \subseteq F^k$.

(18) Every member of V^{j_0} is contained in $t_M(j_0, j_0+1, k)$ members of V^{j_0+1}, by (17), and every member of V^{j_0+1} contains $t_M(i, j_0, j_0+1)$ members of V^{j_0}, by the inductive hypothesis on j. Since $|V^{j_0}| = t_M(i, j_0, k)$, also by the hypothesis on j, we have

$$|V^{j_0+1}| = \frac{t_M(i, j_0, k)\, t_M(j_0, j_0+1, k)}{t_M(i, j_0, j_0+1)},$$

and hence $t_M(i, j_0+1, k) = |V^{j_0+1}|$ is well-defined. This proves by induction that $t_M(i, j, k)$ is well-defined whenever $0 \leq i \leq j \leq k \leq n$.

Finally, (T2) follows from a counting argument similar to that used in (18).

(19) The function $t_M(i, j, k)$ of (16) is called the *t-function of M*.

3.2. *t*-Designs

Perfect matroid designs form a special class of structures called t-designs, which are a generalization of balance incomplete block designs (BIBD's). (They have also been called tactical configurations by Hanani [6]. See also [4] and [7].)

(20) For $t \geq 2$ let t be an integer greater than 1. A *t-design*, or more specifically, a $t-(v, k, \lambda)$ *design*, $(V, \mathscr{W})$, is a v-set V and a system $\mathscr{W}$ of k-subsets of V, $k < v$, called *blocks*, such that every t-subset of V is contained in exactly λ blocks.

Repeated blocks are admissible in the system $\mathscr{W}$. We shall sometimes refer to any such pair $(V, \mathscr{W})$ as a $D_t(v, k, \lambda)$. A BIBD is precisely a 2-design.

(21) For any $t-(v, k, \lambda)$ design $(V, \mathscr{W})$ and integer i, $0 \leq i \leq t$, we let λ_i denote the number of blocks containing any fixed i-subset of V. λ_t is identical with λ, and, in general (see, for example, [7]),

(22)
$$\lambda_i = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} \text{ for } 0 \leq i \leq t.$$

In particular, $(V, \mathscr{W})$ is also an $i-(v, k, \lambda_i)$ design for $2 \leq i \leq t$. Moreover, it follows that, for a given set of parameters t, v, k, λ, the numbers λ_i given by (22) must be integers for a $t-(v, k, \lambda)$ design to exist.

(23) A particularly useful result is the well-known *Fisher Inequality*, which states that, if a $t-(v,k,\lambda)$ design exists, then the number of blocks, λ_0, is greater than or equal to the number of elements, v. Using (22), we may then state this condition as

(24) $$\frac{\lambda\binom{v}{t}}{\binom{k}{t}} \geqslant v.$$

3.3. Consequences of Fisher's Inequality for PMD's

Let M be a rank n PMD. For any i-flat F^i and k-flat F^k of M such that $F^i \subseteq F^k$, let $I_j(F^i, F^k)$ denote the set of all j-flats F^j of M such that $F^i \subseteq F^j \subseteq F^k$.

(25) THEOREM: *For any PMD* M *and integers,* i, j, k, *such that* $2 \leqslant \mathrm{i}+2 \leqslant \mathrm{j} < \mathrm{k} \leqslant \mathrm{r(M)}$, *and any* i-*flat* $\mathrm{F^i}$ *and* k-*flat* $\mathrm{F^k}$ *of* M *such that* $\mathrm{F^i} \subseteq \mathrm{F^k}$, *the set* $\mathscr{W} = \{\mathrm{I}_{i+1}(\mathrm{F^i}, \mathrm{F^j})\colon \mathrm{F^i} \subseteq \mathrm{F^j} \subseteq \mathrm{F^k}$ *and* $\mathrm{F^j}$ *is a* j-*flat of* M$\}$ *is the system of blocks of a BIBD on the set* $\mathrm{V} = \mathrm{I}_{i+1}(\mathrm{F^i}, \mathrm{F^k})$ *with* $\lambda = \mathrm{t_M(i+2, j, k)}$.

PROOF: For any member $I_{i+1}(F^i, F^j)$ of $\mathscr{W}$, $F^i \subseteq F^j \underset{\neq}{\subset} F^k$ because $j<k$. Hence, for $x \in F^k - F^j$, the $(i+1)$-flat $A = cl(F^i \cup \{x\})$ is contained in V, but is not contained in $I_{i+1}(F^i, F^j)$. Thus the members of $\mathscr{W}$ are proper subsets of V.

For any two distinct $(i+1)$-flats F_1 and F_2 in V, $F_1 \cap F_2 = F^i$, by (14). Let J be a basis of F^i, and let $x \in F_1 - F^i$, $y \in F_2 - F^i$. Then $J \cup \{x\}$ is a basis of F_1, and $J \cup \{y\}$ is a basis of F_2. Since $x \notin F_2 = cl(J \cup \{y\})$, $J \cup \{x, y\}$ is an independent set of rank $i+2$ in $F_1 \cup F_2$, and in fact it must be a basis of $F_1 \cup F_2$, because every element of $F_1 \cup F_2$ depends on either $J \cup \{x\}$ or on $J \cup \{y\}$. Hence $cl(F_1 \cup F_2)$ is the unique $(i+2)$-flat containing $F_1 \cup F_2$, and $cl(F_1 \cup F_2) \subseteq F^k$. Further, every $(i+2)$-flat is contained in exactly $t_M(i+2, j, k)$ j-flats contained in F^k. Hence every two $(i+1)$-flats in V are contained together in exactly $t_M(i+2, j, k)$ j-flats contained in F^k, which proves that $(V, \mathscr{W})$ is a BIBD with $\lambda = t_M(i+2, j, k)$.

(26) In (25), the members of $\mathscr{W}$ are in one-to-one correspondence with the j-flats F^j such that $F^i \subseteq F^j \subseteq F^k$. Hence $|\mathscr{W}| = t_M(i, j, k)$. Likewise, $|V| = t_M(i, i+1, k)$. Applying Fisher's Inequality to the results of (25) and (26), we obtain, for any perfect matroid design M

(T3) $\quad t_M(i, i+1, k) \leqslant t_M(i, j, k)$ for $2 \leqslant i+2 \leqslant j < k \leqslant n$.

(27) A function $t(i, j, k)$ of integers i, j, k such that $0 \leqslant i \leqslant j \leqslant k \leqslant n$ for some integer n is said to be *T-consistent* if it is positive integer-valued and satisfies the relations (T0), (T1), (T2) of (15) and (T3) above. In particular, the t-function of a PMD is T-consistent.

(28) Any T-consistent function that is actually the t-function of some PMD will be called a *realizable T*-consistent function.

3.4. Further Properties of Matroids and Perfect Matroid Designs: Reduction, Contraction, Truncation

Let $M = (E, \mathscr{I})$ be a fixed matroid of rank n.

(29) For any subset E' of E, let $\mathscr{I}' = \{J \in \mathscr{I} : J \subseteq E'\}$. $M' = (E', \mathscr{I}')$ clearly satisfies (I1) and (I2), hence it is a matroid, called the *submatroid of M on E'*, or the *reduction of M to E'*, and denoted by $M \times E'$. Clearly, the rank function, r', of M' is just the rank function of M restricted to the subsets of E'. The following result is immediate.

(30) THEOREM: *The flats of* $\mathrm{M} \times \mathrm{E'}$ *are precisely the intersections of the flats of* M *with* E'.

(31) Let E' be a subset of E, and let $\mathscr{I}' = \{J' \subseteq E' : J' \cup J \in \mathscr{I}$ for some M-basis J of $E - E'\}$. It is easily verified that $(E', \mathscr{I}')$ satisfies (I1) and (I2), hence it is a matroid, called the *contraction of M to E'*, and denoted by $M \cdot E'$.

(32) For any $A \subseteq E'$, the rank of A in $M \cdot E'$ is given by $r'(A) = r(A \cup (E - E')) - r(E - E')$, where r is the rank function of M. In particular, $r(M \cdot E') = r(M) - r(E - E')$.

The flats of $M \cdot E'$ are characterized in terms of the flats of M as follows.

(33) THEOREM: *For* $E' \subseteq E$ *and* $0 \leq j \leq r(M) - r(E-E')$, $F \subseteq E'$ *is a* j*-flat of* $M \cdot E'$ *if and only if* $F \cup (E-E')$ *is a* $(j+r(E-E'))$*-flat of* M.

PROOF: A set $F \subseteq E'$ is closed in $M \cdot E'$ if and only if $r'(F \cup \{x\}) > r'(F)$ for every $x \in E'-F$, by (4). This occurs if and only if $r(F \cup (E-E') \cup \{x\}) > r(F \cup (E-E'))$ for every $x \in E-(F \cup (E-E'))$ that is, if and only if $F \cup (E-E')$ is closed in M. Further, by (32), $r'(F)=j$ if and only if $r(F \cup (E-E')) = j + r(E-E')$. Thus F is a j-flat of $M \cdot E'$ if and only if $F \cup (E-E')$ is a $(j+r(E-E'))$-flat of M.

(34) Let $F^i \subseteq F^k$ be an i-flat and k-flat respectively. *The interval of M between* F^i *and* F^k, $M(F^i, F^k)$, is the matroid $(M \times F^k) \cdot (F^k - F^i)$.

Since the set $\mathfrak{F}$ of flats of a matroid M includes E and is closed under intersections, $\mathfrak{F}$ may be viewed as a lattice, ordered by inclusion. Such a lattice is called a *matroid lattice*, or *geometric lattice* [1].

(35) By (30) and (33), the flats of an interval $M(F^i, F^k)$ of M correspond $1-1$ with the flats A of M such that $F^i \subseteq A \subseteq F^k$, and the corresponding lattices ordered by inclusion are isomorphic. This fact is sometimes useful in picturing the structure of a matroid interval $M(F^i, F^k)$. In particular, this observation yields a proof of the following.

(36) THEOREM: *If* M *is a rank* n *PMD with* t*-function* $t_M(i, j, k)$, *and* $F^h \subseteq F^l$ *are an* h*-flat and* l*-flat of* M *respectively, then* $M(F^h, F^l)$ *is a rank* l-h *PMD with* t*-function*

$$t(i,j,k) = t_M(i+h, j+h, k+h), 0 \leq i \leq j \leq k \leq l\text{-h}.$$

(37) For any integer l, $0 \leq l \leq r(M)$, let $\mathscr{I}' = \{J \subseteq E: J \in \mathscr{I} \text{ and } |J| \leq l\}$. Clearly, $M' = (E, \mathscr{I}')$ is a matroid having rank function $r'(A) = \min\{l, r(A)\}$. M' is called the *l-truncation of* M, and denoted by $M^{(l)}$. The flats of $M^{(l)}$ are the flats of M having rank at most $l-1$, and E. If M is a PMD having t-function $t_M(i,j,k)$, then $M^{(l)}$ is a rank l PMD having t-function

$$t(i,j,k) = t_M(i,j,k) \text{ for } 0 \leq i \leq j \leq k < l,$$

$$t(i,j,l) = t_M(i,j,n) \text{ for } 0 \leq i \leq j < l,$$

and

$$t(i,l,l) = 1 \text{ for } 0 \leq i \leq l.$$

(38) A point (1-flat) of a matroid M is said to be an *m-point* if it has cardinality m, and it is a *simple point* if $m=1$. In general, a *simple flat* of M is a flat that is an independent set, i.e., a flat whose rank equals its cardinality. The matroid M is said to be *simple* if all of its points are simple.

(39) Let $M = (E, \mathscr{H})$ be any matroid, and α a positive integer. For each element $x \in E$ choose a set S_x of α elements in such a way that for distinct elements $x, x' \in E$, $S_x \cap S_{x'} = \emptyset$. Let $E' = \bigcup_{x \in E} S_x$, and let $\mathscr{H}' = \{\bigcup_{x \in H} S_x : H \in \mathscr{H}\}$. Clearly, $M' = (E', \mathscr{H}')$ satisfies (H1) and (H2), hence M' is a matroid. M' is said to be an *α-inflation* of M, and M is an *α-deflation* of M'. Now F' is a flat of M' if and only if $F' = \bigcup_{x \in F} S_x$ for some flat F of M. This relation establishes a one-to-one correspondence between the flats of M and M' that preserves inclusion. It follows that if M is a PMD whose points have cardinality α, then there exists an α-deflation M' of M such that M' is simple, and the lattices of M and M' are isomorphic. In particular, M is a PMD if and only if M' is, and their t-functions are the same. Hence there is no loss of generality in proving certain results for simple PMD's.

3.5. *d*-Sequences and *D*-Consistency

The relations (T0)–(T3) impose strong restrictions on the possible parameters for a PMD. However, it is often quite awkward to verify directly whether a given function $t(i,j,k)$ satisfies these relations. We shall define an auxiliary set of parameters for a PMD that is considerably easier to handle, and contains all the information of the associated t-function.

Let M be a rank n PMD with t-function $t_M(i, j, k)$, $0 \leq i \leq j \leq k \leq n$, and define the sequence $d(M) = (d_n, d_{n-1}, \ldots, d_1)$ by the relation

$$d_i = t_M(0, 1, i) - t_M(0, 1, i-1), \qquad 1 \leq i \leq n, \tag{40}$$

where we take $t_M(0, 1, 0) = 0$. In case $r(M) = 0$, that is, if $M = \{\emptyset, \emptyset\}$, we let $d(M)$ be the empty sequence. $d(M)$ is called the *d-sequence* of M.

(41) THEOREM: *Let* t(i, j, k) *be a positive, integer-valued,* T-*consistent function on integers* i, j, k *where* $0 \leq i \leq j \leq k \leq n$. *Let* $d_i = t(0, 1, i) - t(0, 1, i-1)$ *for each* i, $1 \leq i \leq n$. *Then*

$$t(i, j, k) = \frac{\prod_{l=i+1}^{j} \sum_{m=l}^{k} d_m}{\prod_{l=i+1}^{j} \sum_{m=l}^{k} d_m}, \text{ for } 0 \leq i \leq j \leq k \leq n. \tag{42}$$

where an empty product is assumed to take the value 1 .

PROOF: For given i, $0 \leq i \leq n$, the proof of (41) is by induction on the set $S = \{(k, j) : i \leq j \leq k \leq n\}$, ordered lexicographically. For $k = j = i$, both sides of (42) are equal to "1".

Assume then that (42) holds for all pairs $(k, j) \in S$ such that $(k, j) \leq (w, u)$ for some $(w, u) \in S$. We may assume that $(w, u) \neq (n, n)$; otherwise, we are done. Suppose first that $w = u$. The successor of (u, u) in S is $(u+1, i)$, hence we must show that (42) holds for $j = i$, $k = u+1$. This follows immediately from (T0) and the fact that empty products have value "1". Hence we may assume that $u < w$, and we must prove (42) for $(k, j) = (w, u+1)$. By (T2) and (T1),

$$t(i, u+1, w) = \frac{t(i, u, w)t(u, u+1, w)}{t(i, u, u+1)} = \frac{t(i, u, w)}{t(i, u, u+1)} \cdot \frac{t(0, 1, w) - t(0, 1, u)}{t(0, 1, u+1) - t(0, 1, u)},$$

$$= \frac{t(i, u, w)}{t(i, u, u+1)} \cdot \frac{\sum_{m=u+1}^{w} d_m}{d_{u+1}},$$

by definition of the d_i's.

Applying the induction hypothesis to $t(i, u, w)$ and $t(i, u, u+1)$ in the above expression and simplifying, we have finally

$$t(i, u+1, w) = \frac{\sum_{m=u+1}^{w} d_m \prod_{l=i+1}^{u} \sum_{m=l}^{w} d_m}{d_{u+1} \prod_{l=i+1}^{u} \sum_{m=l}^{u+1} d_m} = \frac{\prod_{l=i+1}^{u+1} \sum_{m=l}^{w} d_m}{\prod_{l=i+1}^{u+1} \sum_{m=l}^{u+1} d_m},$$

which is (42) with $(k, j) = (w, u+1)$. The theorem follows now by induction.

A sequence $(d_n, d_{n-1}, \ldots, d_1)$ of positive integers is said to be *D-consistent* if $d_1 = 1$ and the associated function $t(i, j, k)$ given by (42) is T-consistent. The relations (T0)–(T3) for the function $t(i, j, k)$ then translate into the following conditions on $(d_n, d_{n-1}, \ldots, d_1)$.

(43) THEOREM: *A sequence* $D = (d_n, d_{n-1}, \ldots, d_1)$ *is* D-*consistent if and only if*

$$d_1 = 1 \textit{ and } d_i \geq 1,\ 1 \leq i \leq n. \tag{D0}$$

$$\frac{\prod_{l=i+1}^{j} \sum_{m=l}^{k} d_m}{\prod_{l=i+1}^{j} \sum_{m=l}^{j} d_m} \textit{ is integral for } 0 \leq i \leq j \leq k \leq n. \tag{D1}$$

(D2) $$\mathrm{d}_{i-1}|\mathrm{d}_i,\ 2 \leqslant i \leqslant n,\ \textit{and}\ \frac{\mathrm{d}_{i+1}}{\mathrm{d}_i} \geqslant \frac{\mathrm{d}_i}{\mathrm{d}_{i-1}},\ 2 \leqslant i \leqslant n-1.$$

PROOF: Let $t(i, j, k)$ be given from D by (42). In particular,

(44) $$t(0, 1, i) = \sum_{m=1}^{i} d_m/d_1 = \sum_{m=1}^{i} d_m,$$

hence

(45) $$d_i = t(0, 1, i) - t(0, 1, i-1) \text{ for } 1 \leqslant i \leqslant n,$$

where we take $t(0, 1, 0) = 0$.

It follows from (45) that $d_i \geqslant 1$ if and only if $t(0, 1, i) > t(0, 1, i-1)$. Further, $t(i, i, k) = 1$, by our convention that empty products take the value '1'. Hence (D0) is equivalent to (T0). (D1) is equivalent to the requirement that $t(i, j, k)$ be integer valued.

To prove (D2), given that $t(i, j, k)$ is T-consistent, we use (45) to write

(46) $$\frac{d_{i+1}}{d_i} = \frac{[t(0, 1, i+1) - t(0, 1, i-1)] - [t(0, 1, i) - t(0, 1, i-1)]}{t(0, 1, i) - t(0, 1, i-1)}$$

$$= t(i-1, i, i+1) - 1, \text{ for } 1 \leqslant i \leqslant n-1, \text{ by (T1).}$$

Likewise,

(47) $$\frac{d_i}{d_{i-1}} = t(i-2, i-1, i) - 1 \text{ for } 2 \leqslant i \leqslant n.$$

In particular,

(48) $$d_{i-1}|d_i \text{ for } 2 \leqslant i \leqslant n.$$

By (T2), $t(i-2, i, i+1) = \dfrac{t(i-2, i-1, i+1)t(i-1, i, i+1)}{t(i-2, i-1, i)}$ and by (T3) $t(i-2, i, i+1) \geqslant t(i-2, i-1, i+1)$. Hence, using the fact that $t(i, j, k)$ is positive,

(49) $$t(i-1, i, i+1) \geqslant t(i-2, i-1, i).$$

Substituting (46) and (47) in (49), we find that $\dfrac{d_{i+1}}{d_i} \geqslant \dfrac{d_i}{d_{i-1}}$, $2 \leqslant i \leqslant n-1$. Combined with (48), this establishes (D2).

It remains to show that (T1), (T2), and (T3) hold for $t(i, j, k)$ given that D satisfies (D0)–(D2). From (42) and (44) it follows that

$$\frac{t(0,1,k) - t(0,1,i)}{t(0,1,i+1) - t(0,1,i)} = \frac{\sum_{m=i+1}^{k} d_m}{d_{i+1}} = t(i, i+1, k),$$

which establishes (T1). (T2) also follows immediately from (42) by substitution.

To prove (T3), we write, for integers $2 \leqslant i+2 \leqslant j < k \leqslant n$,

(50) $$t(i,j,k)=\frac{\prod_{l=i+1}^{j}\sum_{m=l}^{k} d_m}{\prod_{l=i+1}^{j}\sum_{m=l}^{j} d_m}=\frac{\sum_{m=i+1}^{k} d_m}{d_j}\cdot\prod_{l=i+2}^{j}\left(\frac{\sum_{m=l}^{k} d_m}{\sum_{m=l-1}^{j} d_m}\right)$$

By (D2), $d_m \geqslant d_{m-1}\dfrac{d_l}{d_{l-1}}$ for $m \geqslant l$. Hence (50) implies

(51) $$t(i,j,k)\geqslant\frac{\sum_{m=i+1}^{k} d_m}{d_j}\left(\prod_{l=i+2}^{j}\frac{d_l}{d_{l-1}}\right)\left(\prod_{l=i+2}^{j}\frac{\sum_{m=l}^{k} d_{m-1}}{\sum_{m=l-1}^{j} d_m}\right)$$

The first iterated product is equal to $\dfrac{d_j}{d_{i+1}}$, and the second is greater than or equal to "1" (using the positivity of the d_m's and the fact that $j<k$). Hence

(52) $$t(i,j,k)\geqslant\frac{\sum_{m=i+1}^{k} d_m}{d_{i+1}}=t(i,i+1,k).$$

COROLLARY: *For any PMD* M, *the* d-*sequence of* M, d(M), *satisfies (D0), (D1), (D2), and* $t_M(i, j, k)$ *is given in terms of* d(M) *by* (42).

3.6. Classes of Perfect Matroid Designs and Their d-Sequences

We shall first describe the operations on d-sequences that correspond to the operations introduced in Section 3.4.

Let M be a rank n PMD with d-sequence $d(M)=(d_n, d_{n-1}, \ldots, d_1)$.

(53) From paragraph (39) it follows that an α-inflation or α-deflation of M has the same d-sequence as M.

(54) If F^p is a p-flat and F^q a q-flat of M such that $F^p \subseteq F^q$, then the interval of M, $M(F^p, F^q)$ has t-function $t(i,j,k)=t_M(i+p, j+p, k+p)$, $0\leqslant i\leqslant j\leqslant k\leqslant q-p$, by (36). Hence, for $1\leqslant k\leqslant q-p$, $1\leqslant k\leqslant q-p$,

$$t(0,1,k)-t(0,1,k-1)=t_M(p,p+1,k+p)-t_M(p,p+1,k+p-1)$$

$$=\frac{\sum_{m=p+1}^{k+p} d_m}{d_{p+1}}-\frac{\sum_{m=p+1}^{k+p-1} d_m}{d_{p+1}}=\frac{d_{k+p}}{d_{p+1}}, \text{ by (42).}$$

Hence, M (F^p, F^q) has d-sequence $\left(\dfrac{d_q}{d_{p+1}}, \dfrac{d_{q-1}}{d_{p+1}}, \ldots, \dfrac{d_{p+1}}{d_{p+1}}\right)$.

(55) For any integer h, $1\leqslant h\leqslant n$, the d-sequence of $M^{(h)}$ (the h-truncation of M) is clearly

$$\left(\sum_{j=h}^{n} d_j, d_{h-1}, \ldots, d_1\right).$$

(56) A matroid M on the set E is said to be *disconnected* if for some nonempty proper subset S of E, every circuit of M is contained in S or in $E-S$. Such a subset is called a *proper separator* of M. If M contains no circuits, it is said to be *totally disconnected.*

(57) THEOREM: *If a simple PMD is disconnected, then it is totally disconnected.*

PROOF: Let M be a disconnected, simple PMD and let S be a proper separator of M. Let C be a circuit of M having minimum cardinality, say $|C|=\gamma$. $\gamma \geqslant 3$ because M is simple and contains no loops. We may also suppose without loss of generality that $C \subseteq S$. $r(C)=\gamma-1$, so $cl(C)$ is a $(\gamma-1)$-flat and $|cl(C)| \geqslant \gamma \geqslant 3$.

Let $x, y \in C$, $x \neq y$. Then $C-\{x, y\}$ is independent, and $I=(C-\{x, y\}) \cup \{z\}$ is independent for any $z \in E-S$, since no circuit of M meets both S and $E-S$ and M contains no loops. Let w be an element of $E-I$ that depends on I. Then w depends either on $\{z\}$ or on $C-\{x, y\}$. The former is impossible because M is simple. If the latter were the case, then $(C-\{x, y\}) \cup \{w\}$ would contain a circuit smaller than C, which is contrary to the choice of C. Thus no element of $E-I$ depends on I, so $cl(I)=I$. I is therefore a $(\gamma-1)$-flat having cardinality $\gamma-1$. But then I and $cl(C)$ are two $(\gamma-1)$-flats having distinct cardinalities, contrary to the definition of a PMD. Hence M contains no circuits; that is, M is totally disconnected.

We shall now introduce three general classes of PMD's.

(58) For any integers v and k such that $v>k \geqslant 0$, there exists a PMD M on v elements with hyperplane size k. Namely, let M_E denote the totally disconnected matroid on a v-set E, and let $M = M_E^{(k+1)}$ (the $(k+1)$-truncation of M_E). Where α is a positive integer, any α-inflation $M(\alpha)$ of such an M is called an (α, k, v)-*trivioid*, denoted by $\sigma(\alpha, k, v)$, and $M(\alpha)$ is said to be a *trivial* matroid design. The hyperplanes of $M(\alpha)$ are precisely the subsets of E that are unions of any k distinct points.

The d-sequences of trivioids are characterized as follows.

(59) Theorem: *Every sequence of form* $(d_n, 1, 1, \ldots, 1)$ *having length* n *is the* d-*sequence of an* $(\alpha, n-1, d_n+n-1)$-*trivioid, and conversely.*

PROOF: Let $d(M)=(d_n, 1, \ldots, 1)$ for some rank n PMD $M=(E, \mathscr{H})$. By (42), $t_M(0,1,j)=j$ for $0 \leqslant j \leqslant n-1$, and $t_M(0,1,n)=d_n+n-1$.

Let α be the common cardinality of the points of M, and let M' be an α-deflation of M. M' is simple and has the same t-function as M. Thus, every j-flat of M' has cardinality j, for $0 \leqslant j \leqslant n-1$. Since every j-subset of E is certainly contained in some j-flat, it follows that every j-subset of E is a j-flat for $0 \leqslant j \leqslant n-1$. Thus M' is a $(1, n-1, d_n+n-1)$-trivioid, and M is an $(\alpha, n-1, d_n+n-1)$-trivioid.

Conversely, for any positive integers n, d_n, and α, an $(\alpha, n-1, d_n+n-1)$-trivioid certainly exists, and it is straightforward to verify that its d-sequence is $(d_n, 1, \ldots, 1)$.

(60) Any sequence of form $(d_n, 1, 1, \ldots, 1)$ is said to be a *trivial* sequence. By (59), every trivial sequence is D-consistent.

(61) Let us also note here a general property of D-consistent sequences: if $D=(d_n, d_{n-1}, \ldots, d_1)$ is D-consistent and $d_j=1$ for some j, then $d_j=d_{j-1}=\ldots=d_1=1$. Indeed, for $1 \leqslant i \leqslant j$, (D0) implies that $d_i \geqslant 1$, and (D2) implies that $d_i \mid d_j$. Hence $d_j=1$ implies that $d_i=1$ for $1 \leqslant i \leqslant j$.

(62) We recall that for any matroid $M=(E, \mathscr{H})$, the co-circuits of M are the complements in E of the hyperplanes of M. Since any hyperplane of M is partitioned by the points that meet it, the same holds for any co-circuit of M. Let $c^*(M)$ denote the minimum cardinality of the co-circuits of M. If M is a matroid design, then $c^*(M)$ is the size of every co-circuit of M. In particular, if M is a *simple* PMD, then the leading term of $d(M)$, the d-sequence of M, is $c^*(M)$.

(63) THEOREM: *Every PMD* M *with prime co-circuit cardinality* $c^*(M)$ *is a trivioid.*

PROOF: Let $c^*(M)=p$ be a prime. Where α is the cardinality of the points of M, $\alpha \mid c^*(M)$ because every co-circuit is partitioned by the points that meet it. If $\alpha=p$, then the complement of any point is a hyperplane, so M is a $\left(p, \frac{k(M)}{p}, \frac{k(M)}{p}+1\right)$-trivioid. Otherwise, $\alpha=1$ *and* M is simple. Therefore $d(M)=(p, d_{n-1}, \ldots, d_1)$. Let j be the greatest integer such that $d_j=1$. By (D2), $d_{n-1} \mid p$ and $\frac{p}{d_{n-1}} \geqslant \frac{d_{j+1}}{d_j} > 1$. Hence $d_{n-1}=1$, so $d_i=1$ for $1 \leqslant i \leqslant n-1$. Thus, $d(M)$ is trivial, so, by (59), M is a trivioid.

In another paper [14] we show that Theorem (63) applies to matroid designs in general.

A second class of PMD's comes from the t-designs with $\lambda = 1$.

(64) THEOREM: *For any integer* $t \geqslant 2$, M *is a* $t-(v, k, 1)$ *design such that* $k < v$ *if and only if* M *is a simple rank* $t+1$ *PMD with* d-*sequence* $(v-k, k-t+1, 1, \ldots, 1)$.

PROOF: Let $t \geqslant 2$, and let $M=(E, \mathscr{H})$ be a $t-(v, k, 1)$ design such that $k < v$. First we shall show that $(E, \mathscr{H})$ satisfies (H1) and (H2). Since $k < v$, the members of $\mathscr{H}$ are proper subsets of E. Further, no member of $\mathscr{H}$ is properly contained in another. Thus, (H1) is satisfied.

Suppose that H_1 and H_2 are two distinct blocks. Then $|H_1 \cap H_2| < t$, because any t-set is contained in exactly one block, and for any $x \in E$, $\{x\} \cup (H_1 \cap H_2)$ is contained in at least one t-set, hence in at least one block. Thus M is a matroid with hyperplane family $\mathscr{H}$. By (7), the bases of M are just the minimal subsets of E contained in no hyperplane, that is, the $(t+1)$-subsets of E contained in no hyperplane. Thus $r(M) = t+1$.

For any t-subset T of E, $H = cl\ (T)$ is the unique hyperplane containing T. Since $H \subsetneqq E$, there exists $x \in E-H$, and $\{x\} \cup T$ is contained in no hyperplane of M, hence $\{x\} \cup T$ is a basis, and T is independent in M. Thus every t-subset of E is independent. It follows that every j-flat of M, $1 \leqslant j \leqslant t-1$, is simple. In particular, since $t \geqslant 2$, M is simple. Hence $t_M\ (0, 1, j) = j$, for $1 \leqslant j \leqslant t-1$, $t_M\ (0, 1, t) = k$, and $t_M\ (0, 1, t+1) = v$. Therefore, by definition of the d-sequence $d(M) = (v-k, k-t+1, 1, \ldots, 1)$.

Suppose, conversely, that $t \geqslant 2$ and M is a simple, rank $t+1$ PMD with d-sequence $(v-k, k-t+1, 1, \ldots, 1)$. Then, by (42), $t_M\ (0, 1, j) = j$ for $1 \leqslant j \leqslant t-1$; that is, every j-flat of M is simple for $1 \leqslant j \leqslant t-1$. Hence every t-subset T of E must be independent in M, and is therefore contained in a unique member of $\mathscr{H}$, namely $cl\ (T)$. Again using (42) and the fact that M is simple, we find that the hyperplanes of M have cardinality k, and $|E| = v$. Thus, $M = (E, \mathscr{H})$ is a $t-(v, k, 1)$ design.

(65) As a special case of (64), it follows that every BIBD with $\lambda = 1$ is a rank 3 PMD.

(66) In analogy with matroid designs, we say that a $t-(v, k, \lambda)$ design $(E, \mathscr{H})$ is *trivial* if $\mathscr{H}$ consists of all k-subsets of E.

For $t \geqslant 3$, relatively few nontrivial t-designs have been found, and for $T \geqslant 6$ no nontrivial t-designs are known. We shall briefly mention here all known examples of nontrivial $t-(v, k, 1)$ designs, where $t \geqslant 3$.

(67) For any prime power q and integer $f \geqslant 1$, choose the finite Galois fields $GF(q)$ and $GF(q^f)$ such that $GF(q) \subseteq GF(q^f)$. Then the images of $GF(q) \cup \{\infty\}$ under the group of transformations

$$\mathscr{G} = \left\{ \frac{ax^{q^i}+b}{cx^{q^i}+d} : a, b, c, d \in GF(q^f), ad-bc \neq 0, 0 \leqslant i \leqslant f \right\}$$

are the blocks of a $3-(q^f+1, q+1, 1)$ design on the set $GF(q^f) \cup \{\infty\}$. In the case $f=2$, the $3-(q^2+1, q+1, 1)$ design of this type is called an *inversive plane of order* q, abbreviated by $IP(q)$. (For a more detailed treatment, see [6] and [7].)

(68) A second infinite class of 3-designs consists of the $3-(v, 4, 1)$ designs, which are known as quadruple systems. As shown in [6], necessary and sufficient conditions for the existence of a quadruple system $3-(v, 4, 1)$ are that $v \equiv 2$ or $4 \pmod 6$.

(69) The only other $t-(v, k, 1)$ designs known for $t \geqslant 3$ are due to Witt [13]. They have parameters $4-(11, 5, 1)$, $4-(23, 7, 1)$, $5-(12, 6, 1)$, and $5-(24, 8, 1)$, and are related to the Mathieu groups M_{12} and M_{24}.

(70) We point out that for a sequence of form $(v-k, k-t+1, 1, \ldots, 1)$, the condition (D1) for D-consistency simply reduces to the requirement that the numbers λ_i associated (22) with the corresponding $t-(v, k, 1)$ design be integers. Likewise, (D2) is simply a consequence of Fisher's inequality for this t-design. However, it is well-known from BIBD theory that for given parameters t, v, k, λ the integrality of the expressions for λ_i and Fisher's inequality are not sufficient to assure the existence of a $t-(v, k, \lambda)$ design. Hence, in particular, the D-consistency of a sequence does not imply that it is actually the d-sequence of some PMD.

A D-consistent sequence that is the d-sequence of some PMD will be called a *realizable D-consistent sequence*. We shall presently develop several additional criteria for D-consistent sequences to be realizable.

A third class of PMD's consists of the classical finite projective and affine geometries of arbitrary dimension. This class is the prototype on which PMD's are modeled.

A finite projective geometry $(E, \mathscr{L})$ is a set E of points and a set $\mathscr{L}$ of lines satisfying certain well-known incidence axioms [12]. A finite projective geometry of *dimension* n and *order* s will be abbreviated by $PG(n, s)$, where $n \geqslant 2$ and $s+1 \geqslant 3$ is the number of points on every line, and $s^{n+1}-1/s-1$ is the total number of points. The *subspaces* of a $PG(n, s)$ are those subsets $S \subseteq E$ such that for every $x, y \in S$, the unique line containing x and y is a subset of S. The *hyperspaces* are just the maximal proper subspaces.

(71) The points and lines of a $PG(2, s)$ form a BIBD with $\lambda = 1$, namely, a $2-(s^2+s+1, s+1, 1)$ design. That is, any $PG(2, s)$ is a rank 3 PMD with d-sequence $(s^2, s, 1)$. Conversely, it may be shown by a simple counting argument that in any PMD with d-sequence $(s^2, s, 1)$, every two lines meet [5]; and hence every such PMD is a $PG(2, s)$.

(72) For $n \geqslant 3$, a $PG(n, s)$ exists if and only if s is a prime power [12] and in this case it is isomorphic to the $PG(n, s)$ constructed as follows. Let $s = q$, where q is a prime power, and let E be the set of all nonzero $(n+1)$-tuples over the Galois field $GF(q)$. Let $\mathscr{I}$ be the family of all subsets of E that are linearly independent over $GF(q)$. Clearly, $M = (E, \mathscr{I})$ is a rank $n+1$ matroid. Moreover, for $0 \leqslant j \leqslant n+1$, every j-flat of M contains $q^j - 1$ elements. In particular, the points of M each contain $q-1$ elements. Where M' is any $(q-1)$-deflation of M, it follows that M' is a simple, rank $n+1$ PMD with t-function given by $t_{M'}(0, 1, j) = q^j - 1/q - 1$ and d-sequence $(q^n, q^{n-1}, \ldots, q, 1)$. For any 3-flat F of M', $M' \times F$ has d-sequence $(q^2, q, 1)$ and is therefore a $PG(2, q)$. It follows easily that the point-family E' and line-family $\mathscr{L}'$ of M' together satisfy the projective axioms. Since every line has cardinality $q+1$, and $|E'| = q^{n+1} - 1/q - 1$, $(E', \mathscr{L}')$ is a $PG(n, q)$. The subspaces of $(E', \mathfrak{L}')$ are precisely the spans of independent sets of M'; i.e., they are precisely the flats of M'.

(73) It follows from (71) and (72) that the family E of points and the family $\mathscr{H}$ of hyperspaces of any $PG(n, s)$ $(E, \mathscr{L})$ are the points and hyperplanes of a rank $n+1$ PMD whose flats are the subspaces of $(E, \mathscr{L})$. In this sense, every $PG(n, s)$ is a rank $n+1$ PMD with d-sequence $(s^n, s^{n-1}, \ldots, s, 1)$.

(74) Suppose that $M = (E, \mathscr{H})$ is any simple PMD with d-sequence of form $(\ldots, s^2, s, 1)$. Then just as above we may conclude that every 3-flat of M is a $PG(2, s)$, and hence that the line-family $\mathscr{L}$ of M satisfies the projective axioms. Thus, $(E, \mathscr{L})$ is a $PG(h, s)$ for some integer h. However, this does not necessarily imply that M is a $PG(h, s)$ in the sense described above. Conceivably, M might be constructed so that its flats constituted a proper subcollection of the subspaces of the $PG(h, s)$ defined by the lines. On the other hand, we may observe that the total number of points of M must be $s^h - 1/s - 1$. This leads to the following useful criterion, which was pointed out to the authors by Richard Wilson.

(75) If $D = (d_n, d_{n-1}, \ldots, 1)$ is a realizable D-consistent sequence such that $n \geqslant 3$ and $d_3 = s^2$, $d_2 = s$ for some $s \geqslant 2$, then

$$\sum_{i=1}^{n} d_i = \frac{s^h - 1}{s - 1}$$

for some positive integer h.

However, if we know that $d(M) = (s^n, s^{n-1}, \ldots, s, 1)$ then we may conclude that M is a $PG(n, s)$.

(76) THEOREM: *For any integers* $n \geqslant 2$ *and* $s \geqslant 2$, *every simple rank* $n+1$ *PMD with* d*-sequence of form* $(s^n, s^{n-1}, \ldots, s, 1)$ *is a* $PG(n, s)$, *and conversely.*

PROOF: For a simple PMD $M=(E, \mathscr{H})$ with $d(M)=(s^n, s^{n-1}, \ldots, s, 1)$ and line-family $\mathscr{L}$, $(E, \mathscr{L})$ is a finite projective geometry of order s, by (74). Since M is simple,

$$|E|=t_M(0, 1, n+1)=\sum_{i=0}^{n} s^i=\frac{s^{n+1}-1}{s-1};$$

hence $(E, \mathscr{L})$ is a $PG(n, s)$.

Let $\mathscr{H}'$ be the family of hyperspaces of $(E, \mathscr{L})$. To show that M is a $PG(n, s)$, we will show that $\mathscr{H}=\mathscr{H}'$. By (73), $M'=(E, \mathscr{H}')$ is a PMD with the same d-sequence as M. Hence their t-functions are the same, so they contain the same number of flats. But for any flat F of M and distinct $x, y \in F$, $cl_M(\{x, y\}) \in \mathscr{L}$ and $cl_M(\{x, y\}) \subseteq F$; hence F is a subspace of $(E, \mathscr{L})$. Therefore, every flat of M is a flat of M'. Hence they have the same flats, and in particular $\mathscr{H}=\mathscr{H}'$. Thus M is a $PG(n, s)$. The converse has already been noted in (73).

The criterion of (75) may be applied to show that certain D-consistent sequences are not realizable. For example, the sequence (36, 4, 2, 1) satisfies (D0), (D1), and (D2) (as may be verified directly), but $36+4+2+1=43 \neq 2^h-1$ for any integer h.

(77) For any $PG(n, s)$ $M=(E, \mathscr{H})$ and hyperplane H_0 of M, a matroid of form $M'=M \times (E-H_0)$, is called *an affine geometry of dimension* n *and order* s, abbreviated by $EG(n, s)$. If F' is any j-flat of M', $0 \leqslant j \leqslant n+1$, then $F=cl_M(F')$ is a j-flat of M not contained in H_0. By the modular law for projective geometries ([12], Chapter 7, Theorem 10), $r(F \cap H_0)=r(F)-1$. Hence we have $|F'| = |F|-|F \cap H|=s^{j-1}$. Conversely, for any j-flat F of M not contained in H_0, $F'=F-H_0$ is a flat of M' and $|F'|=s^{j-1}$, so, by the above, F' must be a j-flat of M'. Thus, M' is a rank $n+1$ PMD whose j-flats are precisely the sets of form $F-H_0$ for j-flats F of M not contained in H_0, and the d-sequence of M' is $(s^{n-1}(s-1), s^{n-2}(s-1), \ldots, s-1, 1)$.

As in the case of projective geometries, we may also characterize affine geometries by their d-sequences. For this purpose we use the well-known axiomatization of affine geometries due to Lenz [8]. Let $M=(E, \mathscr{H})$ be a simple PMD with d-sequence

$$d(M)=(s^{n-1}(s-1), s^{n-2}(s-1), \ldots, s-1, 1)$$

for some integers $n \geqslant 2$ and $s \geqslant 2$. Where F is any 3-flat of M, $d(M \times F)=(s^2-s, s-1, 1)$ and $t_{M \times F}(1, 2, 3)=s+1$. Thus every point is contained in $s+1$ lines, and since for every line L of $M \times F$ and $x \in F-L$ there are exactly s lines meeting both x and L, there is a unique line containing x and disjoint from L. Thus the lines of $M \times F$ decompose into parallel classes. By adjoining an ideal point for each parallel class and an ideal line we conclude that $M \times F$ is the reduction of a $PG(2, s)$ to the complement of some line; that is, it is an $EG(2, s)$.

(78) Let $\mathscr{L}$ be the family of lines of M, and for any $L_1, L_2 \in \mathscr{L}$ write $L_1 \| L_2$ if either $L_1=L_2$, or $L_1 \cap L_2 = \varnothing$ and $r(L_1 \cup L_2)=3$. For any $L \in \mathscr{L}$ and point x there is a unique line L_x containing x such that $L_x \| L$ — namely, $L_x=L$ if $x \in L$ and otherwise L_x is the unique line containing x and disjoint from L in the 3-flat $cl(L \cup \{x\})$. It remains only to show that $\|$ is a transitive relation on $\mathscr{L}$ to establish Lenz's incidence axioms for the line-family of an affine geometry. Let L_1, L_2, L_3 be distinct lines such that $L_1 \| L_2$ and $L_1 \| L_3$. Then $K=cl(L_1 \cup L_2 \cup L_3)$ is a 4-flat and $d(M \times K)=(s^3-s^2, s^2-s, s-1, 1)$. Pick $x \in L_3$, and let $H=cl(L_2 \cup \{x\})$, $H_{12}=cl(L_1 \cup L_2)$, $H_{13}=cl(L_1 \cup L_3)$. $M'=(M \times K) \cdot (K-\{x\})$ has d-sequence $(s^2, s, 1)$ and $H-\{x\}$, $H_{13}-\{x\}$ are hyperplanes (2-flats) of M'. By (76), M' is an inflation of a $PG(2, s)$, so by the modular law, $(H-\{x\}) \cap (H_{13}-\{x\})$ is a point of M'.

Hence $H \cap H_{13}=L$ is a line of $M \times K$ containing x. If $L \cap L_1=\varnothing$, then $L \| L_1$ and $x \in L$ implies $L=L_3$. Thus $L_2, L_3 \subseteq H$. If $L_2 \cap L_3 \neq \varnothing$, we would have $L_2=L_3$ (since both are parallel to L_1), which is contrary to hypothesis. Hence $L_2 \cap L_3=\varnothing$ and so $L_2 \| L_3$. If $L \cap L_1 \neq \varnothing$, say $L \cap L_1 = \{y\}$, then $L_2 \cup \{y\} \subseteq H_{12} \cap H$ and so $H_{12}=H$. But then $L_1 \cup \{x\} \subseteq H_{13} \cap H$, whence $H=H_{13} = H_{12}$. Thus, $L_2, L_3 \subseteq H$, and since $L_2 \cap L_3=\varnothing$, we have $L_2 \| L_3$, proving the transitivity of $\|$.

It follows that $\mathscr{L}$ is the line-family of an affine geometry of order s on the set E. Since $|E|=s^n$, $(E, \mathscr{L})$ must be an $EG(n, s)$. By (77), the subspaces of $(E, \mathscr{L})$ form a perfect matroid design N

with the same d-sequence as M, and every flat of M is a subspace of N. Thus $M = N$, and we have proved the following.
(79) THEOREM: *For any integers* $n \geq 2$ *and* $s \geq 2$, *every simple rank* $n+1$ *PMD with* d*-sequence* $(s^{n-1}(s-1), s^{n-2}(s-1), \ldots, s-1, 1)$ *is an* $EG(n, s)$, *and conversely.*

3.7. Computation of D-Consistent Sequences

In spite of the insufficiency of the conditions (D0), (D1), and (D2) as existence criteria for PMD's, there are in fact very few sequences that satisfy even these conditions. In this section we will describe how (D0)–(D2) may be applied to determine all possible D-consistent sequences with a given leading term γ.
(80) Let γ be a given positive integer with t prime factors, let $D = (d_n, d_{n-1}, \ldots, d_1)$ be a D-consistent sequence such that $d_n = \gamma$, and let s be the largest index for which $d_s = 1$. The truncated sequence $(d_n, d_{n-1}, \ldots, d_{s+1}) = D'$ is called the *nontrivial part* of D. By (D2), D' can have at most t terms. If t is small, the possibilities for D' will be easy to determine. The possibilities for D are then obtained by extending D' by sequences of "1" 's, subject to the restriction that (D1) is satisfied.
(81) Let $D = (d_n, d_{n-1}, \ldots, d_1)$ be a sequence of positive integers. A *normalized interval of D* having *length i* is a sequence of form

$$\left(\frac{d_{h+i}}{d_{h+1}}, \frac{d_{h+i-1}}{d_{h+1}}, \ldots, \frac{d_{h+1}}{d_{h+1}}\right),$$

where $1 \leq i \leq n$, $0 \leq h \leq n-i$. It is easily verified that the sequence D is D-consistent if and only if every normalized interval of D is D-consistent. This fact is often useful in checking D-consistency of long sequences.
(82) As an application, let us find all D-consistent sequences with leading term 20. From (D2) it follows that the nontrivial part of every D-consistent sequence with leading term 20 is one of the following: (20), (20, 2), (20, 4), or (20, 4, 2). By (59), every sequence of form (20, 1, . . ., 1) is D-consistent. It is easy to check that (20, 2, 1) and (20, 4, 2, 1) are not D-consistent; hence neither of these is the interval of a D-consistent sequence. The sequences (20, 4, 1) and (20, 4, 1, 1) are D-consistent, but (20, 4, 1, 1, 1) is not.

Thus, the only D-consistent sequences with leading term 20 are (20, 4, 1), (20, 4, 1, 1), and trivial sequences. By (79), $EG(2, 5)$ is the unique PMD with d-sequence (20, 4, 1). There is also a PMD with d-sequence (20, 4, 1, 1), namely, the inversive plane $IP(2, 5)$.

In the Appendix we have listed all nontrivial D-consistent sequences with leading terms 1–40 using the methods presented above. PMD's corresponding to the sequences are given, if known. In some cases, existence theorems for BIBD's, the Bruck-Ryser conditions for finite geometries, or Theorem (75) imply that a given D-consistent sequence is not realizable. Together, these conditions and D-consistency are sufficiently powerful that, for all D-consistent sequences with leading term between 1 and 40, the only realizable ones correspond to one of the three classes of PMD's previously discussed: trivioids, t-designs with $\lambda = 1$, and projective and affine geometries (or truncations of these). On the other hand, there is every indication that many more types of PMD's exist, probably an infinite number. For example, the sequence (48, 6, 2, 1) is D-consistent (as may be checked), and satisfies (75) and known BIBD existence criteria, but it does not correspond to a PMD from one of the above four classes. The existence of a PMD with this d-sequence has not yet been established.

3.8. Bounds on the Rank of Nontrivial Perfect Matroid Designs with Given Co-Circuit Cardinality

The Appendix shows that for each N, $1 \leq N \leq 40$ the number of nontrivial D-consistent sequences with leading term N is finite. We shall show presently that this result is true for every positive integer N, and in fact we shall be able to give sharp bounds on the rank of any nontrivial PMD with given co-circuit cardinality. As a preliminary, we shall state and prove an interesting number-theoretic result that appears to be new.

(83) For every pair (n, m) of integers, $n \geqslant m \geqslant 1$, and integer $r \geqslant 1$, let

$$\pi_r(m, n) = \frac{n(n+1)\ldots(n+r-1)}{m(m+1)\ldots(m+r-1)} = \frac{\binom{n+r-1}{r}}{\binom{m+r-1}{r}},$$

and define the *factorial index of* m *in* n, $\beta(m, n)$, to be the maximum integer t such that $\pi_r(m, n)$ is integral for $0 \leqslant r \leqslant t$. We set $\beta(m, n) = 0$ if $m \nmid n$.

(84) **Theorem.** *If* m *and* n *are integers such that* $2 \leqslant m \leqslant \frac{n+1}{2}$, *then* $\beta(m, n) \leqslant n - 2m + 1$.

Proof: We begin with the following identity which is a variant of Van der Monde's formula ([11], p. 9).

(85)
$$\binom{a}{t} = \sum_{r=0}^{t} (-1)^r \binom{b}{r} \binom{a+b-r}{t-r}.$$

Dividing both sides of (85) by $\binom{b}{t}$, and using the relation $\frac{\binom{b}{r}}{\binom{b}{t}} = \frac{\binom{t}{r}}{\binom{b-r}{t-r}}$, $0 \leqslant r \leqslant t$, we can rewrite (85) as follows:

(86)
$$\frac{\binom{a}{t}}{\binom{b}{t}} = \sum_{r=0}^{t} (-1)^r \binom{t}{r} \frac{\binom{a+b-r}{t-r}}{\binom{b-r}{t-r}}.$$

For given integers $n > m \geqslant 2$, let $0 \leqslant t \leqslant n - m$, and substitute $a = n - m$, $b = m + t - 1$ in (86). Then we obtain

(87)
$$\frac{\binom{n-m}{t}}{\binom{m+t-1}{t}} = \sum_{r=0}^{t} (-1)^r \binom{t}{r} \frac{\binom{n+t-1-r}{t-r}}{\binom{m+t-1-r}{t-r}} = \sum_{r=0}^{t} (-1)^r \binom{t}{r} \pi_{t-r}(m, n).$$

Hence, if π_{t-r} is integral for $0 \leqslant t - r \leqslant t$, then $\binom{n-m}{t} \Big/ \binom{m+t-1}{t}$ is integral. If $t > 0$, it follows that $m + t - 1 \leqslant n - m$, so $t \leqslant n - 2m + 1$. If $t = 0$, this inequality also holds, since $m \leqslant \frac{n+1}{2}$. Hence $\beta(m, n) \leqslant n - 2m + 1$.

(88) For any matroid M, let $c(M)$ denote the minimum cardinality of a circuit of M.

(89) **Theorem:** *If* $M = (E, \mathscr{H})$ *is a simple, nontrivial PMD with hyperplane cardinality* $k(M)$, *then*

(i) $k(M) \leqslant |E|/2$.
(ii) $c(M) \leqslant c^*(M)$.
(iii) $r(M) \leqslant c^*(M)$.

PROOF: Let $d(M)=D=(d_n, d_{n-1}, \ldots, d_1)$ and let s be the greatest index such that $d_s=1$. $s \leqslant n-2$ because M, and hence D, is non-trivial. For each k, $1 \leqslant k \leqslant s+1$,

$$\pi_k(d_{s+1}, d_{s+2}+d_{s+1}) = \frac{(d_{s+2}+d_{s+1})(d_{s+2}+d_{s+1}+1)\ldots(d_{s+2}+d_{s+1}+k-1)}{(d_{s+1})(d_{s+1}+1)\ldots(d_{s+1}+k-1)}$$

$$= t_M(s-k-1, s+1, s+2),$$

which is an integer.

Since $\dfrac{d_{s+2}+d_{s+1}+1}{2} \geqslant d_{s+1} \geqslant 2$, (84) implies that

$$s+1 \leqslant (d_{s+1}+d_{s+2}) - 2d_{s+1} + 1$$

that is,

(90) $$s \leqslant d_{s+2} - d_{s+1}.$$

Now

$$\sum_{j=s+1}^{n-1} d_j = \frac{\sum_{j=s+1}^{n-1}(d_{s+2}-d_{s+1})d_j}{d_{s+2}-d_{s+1}} \leqslant \frac{d_{s+1}\sum_{j=s+1}^{n-1}(d_{s+1}-d_j)}{d_{s+2}-d_{s+1}},$$

by (D2), so

(91) $$\sum_{j=s+1}^{n-1} d_j \leqslant \frac{d_{s+1}(d_n-d_{s+1})}{d_{s+2}-d_{s+1}}.$$

Since M is simple, $k(M)=\sum_{j=1}^{n-1} d_j = s + \sum_{j=s+1}^{n-1} d_j$. Hence, by (90) and (91),

$$k(M) \leqslant d_{s+2}-d_{s+1}+\frac{d_{s+1}(d_n-d_{s+1})}{d_{s+2}-d_{s+1}}$$

$$=\frac{(d_{s+2}-d_{s+1})^2-d_{s+1}^2}{d_{s+2}-d_{s+1}}+\frac{d_{s+1}d_n}{d_{s+2}-d_{s+1}}$$

$$=\frac{d_{s+2}(d_{s+2}-2d_{s+1})}{d_{s+2}-d_{s+1}}+\frac{d_{s+1}d_n}{d_{s+2}-d_{s+1}}$$

$$\leqslant\frac{d_n(d_{s+2}-2d_{s+1})}{d_{s+2}-d_{s+1}}+\frac{d_{s+1}d_n}{d_{s+2}-d_{s+1}}$$

$$=d_n,$$

the latter inequality because $d_n \geqslant d_{s+2}$ and $d_{s+2} \geqslant 2d_{s+1}$. Thus, $k(M) \leqslant d_n$. Since M is simple, $k(M)+d_n=|E|$, hence $k(M) \leqslant |E|/2$, and (i) is proved.

Since M is nontrivial, $k(M) > n-1$, every hyperplane is dependent (contains a circuit). Hence $c(M) \leqslant k(M) \leqslant d_n = c^*(M)$, proving (ii). Finally, $r(M)=n \leqslant k(M) \leqslant c^*(M)$, proving (iii).

There are examples of PMD's for which (i), (ii), and (iii) of (89) are all satisfied as equalities: for example, the affine geometry $EG(3, 2)$, and the Witt design 5-(12, 6, 1). Therefore, (89) is, in a certain sense, best possible.

3.9. The t-Designs in a Perfect Matroid Design

We have already observed in (25) that the flats of a given cardinality in a simple PMD M constitute the blocks of a BIBD on the points of M. This result can be sharpened to state that any such collection of flats forms a t-design for some appropriate t. Moreover, we shall show that not only the flats, but also the circuits, and the independent sets, of a given cardinality in a PMD form a t-design for an appropriate t. These results yield a method for deriving new t-designs from known ones in certain cases.

(92) Where $c(M)$ is the minimum cardinality of a circuit of the matroid M, it follows that $c(M)-1$ is the maximum integer m such that every m-subset of E is independent. $c(M)-1$ is called the *independence number of M, $\beta(M)$.*

(93) THEOREM: *Let* $M=(E,\mathscr{I})$ *be a rank* n *PMD with independence number* β, *where* $2\leq\beta\leq n$, *and for each* j, $\beta\leq j\leq n$, let $\mathfrak{F}_j$ *be the set of* j*-flats of* M. *Then* $(E,\mathfrak{F}_j)$ is a $\beta-(|E|, t_M(0,1,j), t_M(\beta,j,n))$ *design.*

PROOF: Let j be given, $\beta\leq j\leq n$. Since every β-subset of E is independent, every β elements are contained in one and only one β-flat, which is contained in precisely $t_M(\beta,j,n)$ j-flats. Since $\beta\geq 2$, M is simple, and hence every j-flat of M contains $t_M(0,1,j)$ elements. Therefore $(E,\mathfrak{F}_j)$ is a $\beta-(|E|, t_M(0,1,j), t_M(\beta,j,n))$ design.

(94) THEOREM: *Let* $M=(E,\mathscr{H})$ *be a rank* n *PMD with independence number* β, $2\leq\beta\leq n$. *For each* j, $\beta\leq j\leq n$, *the family* $\mathscr{I}_j$ *of independent sets of cardinality* j *in* M *are the blocks of a* $\beta-(|E|, j, \mu_j)$ *design on the set* E, *where*

(95)
$$\mu_j=\frac{\prod_{l=\beta}^{j-1}(t_M(0,1,n)-t_M(0,1,l))}{(j-\beta)!}\quad\text{for } j>\beta,$$

and $\mu_j=1$ *for* $j=\beta$.

PROOF: If $j=\beta$, we take $\mu_j=1$ and the theorem obviously holds. Thus we may assume that $j>\beta$.

(96) Let E_β be a fixed β-subset of E, and let $F_0=cl\,(E_\beta)$. E_β is independent, by definition of β. With each independent j-set J containing E_β, we may associate an ordering $J'=(x_1,\ldots,x_{j-\beta})$ of $J-E_\beta$ and a sequence $\mathfrak{F}: F_0\subset F_1\subset\ldots\subset F_{j-\beta}$ of nested flats defined by $F_i=cl\,(F_0\cup\{x_1,\ldots,x_i\})$, The sequence $\mathfrak{F}$ then has the property that $x_{i+1}\in E-F_i$ and $F_{i+1}=cl(F_i\cup\{x_{i+1}\})$ for $0\leq i\leq j-\beta$. For each set J containing E_β, such an association can be made in precisely $(j-\beta)!$ ways.

(97) Conversely, for any sequence of flats $cl\,(E_\beta)=F_0\subset F_1\subset\ldots\subset F_{j-\beta}$, and set $J'=\{x_1,\ldots,x_{j-\beta}\}$ such that $x_{i+1}\in E-F_i$ and $F_{i+1}=cl(F_i\cup\{x_{i+1}\})$ for $0\leq i\leq j-\beta$, the set $J=J'\cup E_\beta$ is an independent set of rank j. If this were not so, let k be the least integer such that $E_\beta\cup\{x_1,\ldots,x_k\}$ were dependent. But by (5), $F_{k-1}=cl(E_\beta\cup\{x_1,\ldots,x_{k-1}\})$, and hence we would have $x_k\in F_{k-1}$, which is contrary to assumption. Therefore J is an independent set of rank j containing E_β.

A sequence of flats and ordered independent set as in (97) can be chosen in precisely

$$\prod_{l=\beta}^{j-1}(t_M(0,1,n)-t_M(0,1,l))$$

distinct ways, and each corresponding independent j-set containing E_β is thereby counted $(j-\beta)!$ times, by (96). Thus E_β is contained in precisely

$$\mu_j=\frac{\prod_{l=\beta}^{j-1}(t_M(0,1,n)-t_M(0,1,l))}{(j-\beta)!}$$

independent j-sets.

(98) THEOREM: *Let* $M=(E,\mathscr{K})$ *be a simple, rank* n *PMD with independent number* β. *For each*

j, $\beta < j \leq n+1$, *the family* $\mathscr{C}_j$ *of cardinality*-j *circuits of* M *are the blocks of a* $\beta-(|E|, j, \eta_j)$ *design on the set* E, *where*

$$(99)\qquad \eta_j = \mu_{j-1}\left[\frac{t_M(0,1,n) + \sum_{i=1}^{j-2}(-1)^{j-i-1}\binom{j-1}{i} t_M(0,1,i)}{j-\beta}\right] - \mu_j,$$

and μ_j *is as defined in (95) for* $\beta < j \leq n$, *and* $\mu_{n+1} = 0$.

PROOF: For each j, $2 \leq j \leq n+1$, let

$$f(j) = t_M(0,1,n) + \sum_{i=1}^{j-2}(-1)^{j-i-1}\binom{j-1}{i} t_M(0,1,i).$$

We shall first establish (98) for the case $j = n+1$.

(100) Let J be a basis of M, and for each i, $1 \leq i \leq n$, let P_i be the set of all pairs (I_i, x) such that I_i is an i-subset of J and $x \in cl(I_i)$, where $cl(I_i)$ is the unique i-flat containing I_i. Since M is simple, $t_M(0,1,i)$ represents the cardinality of any i-flat, $1 \leq i \leq n$. Thus we have $|P_i| = \binom{|J|}{i} t_M(0,1,i) = \binom{n}{i} t_M(0,1,i)$. Let $P = \bigcup_{i=1}^{n} P_i$, and to each pair $(I, x) \in P$ assign the coefficient $(-1)^{n-i}$ if $(I, x) \in P_i$. Thus $f(n+1)$ is the sum of the coefficients of the members of P.

For any $x \in E$, define $F(x)$ to be the sum of the coefficients of pairs in P containing x. If $x \in J$, x is contained in the closure of $\binom{n-1}{i-1}$ i-subsets of J, $1 \leq i \leq n$. Thus

$$(101)\qquad F(x) = \sum_{i=1}^{n}(-1)^{n-i}\binom{n-1}{i-1} = 0 \text{ for } x \in J.$$

If $x \in E - J$, then since J is a maximal independent set, $J \cup \{x\}$ contains a circuit C_x, containing x, and by (1), it is unique. Let $|C_x| = j$; clearly, $j \leq n+1$. Now $(I, x) \in P$ if and only if $C_x \subseteq I \cup \{x\}$. Thus x is contained in the closures of $\binom{n-j+1}{i-j+1}$ i-subsets of J for $j-1 \leq i \leq n$, and x is contained in the closures of no i-subsets of j for $0 \leq i \leq j-2$. Hence $F(x) = \sum_{i=j-1}^{n}(-1)^{n-i}\binom{n-j+1}{i-j+1}$ in this case. Setting $n-j+1 = k$ and $i-j+1 = l$, we have that

$$\sum_{i=j-1}^{n}(-1)^{n-i}\binom{n-j+1}{i-j+1} = \sum_{l=0}^{k}(-1)^{k-l}\binom{k}{l} = \begin{matrix} 0, \text{ for } k>0. \\ 1, \text{ for } k=0, \text{ i.e., for } j=n+1. \end{matrix}$$

Thus $F(x) = 1$ if and only if $x \in E - J$ and $|C_x| = n+1$, i.e., if and only if $J \cup \{x\}$ is a circuit. Since $f(n+1) = \sum_{x \in E} F(x)$, $f(n+1)$ is precisely the number of circuits of cardinality $n+1$ containing J.

By (94), every β-subset of E is contained in exactly μ_n bases of M, where μ_n is as in (95). Further, every circuit C of cardinality $n+1$ contains $n+1-\beta$ bases of M containing a given β subset of C. Hence the number of cardinality $-(n+1)$ circuits of M containing any given β-subset of E is exactly

$$(102)\qquad \eta_{n+1} = \frac{f(n+1)}{n+1-\beta} = \mu_n \frac{t_M(0,1,n) + \sum_{i=1}^{n-1}(-1)^{n-i}\binom{n}{i} t_M(0,1,i)}{n+1-\beta}.$$

(103) For an arbitrary j, $\beta < j \leq n+1$, we consider $M^{(j-1)}$, the $(j-1)$-truncation of M. The circuits of

493-033 OL - 73 - 3

$M^{(j-1)}$ are evidently the circuits of M having cardinality less than or equal to j, together with the j-subsets of E that are independent in M. By (37), $M^{(j-1)}$ has rank $j-1$ and its t-function $t(i, j, k)$ is determined by

$$t(0,1,i) = t_M(0,1,i),\ 0 \leq i \leq j-2,$$

$$t(0,1,j-1) = t_M(0,1,n).$$

Hence (102) applied to $M^{(j-1)}$ implies that every β-subset of E is contained in precisely

$$\mu_{j-1}\left[\frac{t_M(0,1,n) + \sum_{i=1}^{j-2} (-1)^{j-i-1} \binom{j-1}{i} t_M(0,1,i)}{j-\beta}\right] = \frac{\mu_{j-1} f(j)}{j-\beta}$$

cardinality-j circuits of $M^{(j-1)}$. However, μ_j of these circuits are cardinality-j independent sets of M, by (103). Thus every β-subset of E is contained in precisely

$$\eta_j = \frac{\mu_{j-1} f(j)}{j-\beta} - \mu_j$$

cardinality-j circuits of M.
(104) Let us observe that we may have $\eta_j = 0$ for some integers j in (99); in this case $\mathscr{C}_j = \varnothing$ and $(E, \mathscr{C}_j)$ is said to be a *vacuous* β-design.

3.10. Constructions of New *t*-Designs

Before applying the results of (94) and (98) to the construction of new t-designs, we shall point out several very natural ways of obtaining new t-designs from given ones.

The following result generalizes a well-known theorem for BIBD's.
(105) THEOREM: *Let* $(E, \mathscr{H})$ *be a* $\mathrm{t}-(\mathrm{v}, \mathrm{k}, \lambda)$ *design and let* $\mathscr{H}'$ *be the system consisting of the complements in* E *of the blocks of* $\mathscr{H}$ *(including repetitions). Then* $(\mathrm{E}, \mathscr{H}')$ *is a* $\mathrm{t}-(\mathrm{v}, \mathrm{v}-\mathrm{k}, \lambda')$ *design, called the* complementary design *to* M, *and*

$$\lambda' = \lambda \frac{\binom{\mathrm{v}-\mathrm{k}}{\mathrm{t}}}{\binom{\mathrm{k}}{\mathrm{t}}}.$$

PROOF: For integer j, $0 \leq j \leq t$, let λ_j be the number of blocks containing any fixed j-subset of E. For a given j-set E_j and t-set E_t, where $E_j \subseteq E_t \subseteq E$, let η_j be the number of blocks H such that $H \cap E_t = E_j$. Then $\eta_t = \lambda$, and recursively,

$$\eta_j = \lambda_j - \sum_{i=1}^{t-j} \binom{t-j}{i} \eta_{j+i}$$

is independent of the particular sets E_j and E_t. It follows that $(E, \mathscr{H}')$ is a $t-(v, v-k, \eta_0)$ design Hence

$$\lambda \frac{\binom{v}{t}}{\binom{k}{t}} = |\mathscr{H}| = |\mathscr{H}'| = \eta_0 \frac{\binom{v}{t}}{\binom{v-k}{t}}.$$

$$\eta_0 = \lambda \frac{\binom{v-k}{t}}{\binom{k}{t}}.$$

(106) Let $(E, \mathscr{H})$ be a $t-(v, k, \lambda)$ design such that $\mathscr{H}$ contains no repeated blocks and let $\mathscr{H}'$ be the family of k-subsets of E not contained in $\mathscr{H}$. Clearly, $(E, \mathscr{H}')$ is a $t-(v, k, \lambda')$ design, where $\lambda' = \binom{v-t}{k-t} - \lambda$. $(E, \mathscr{H}')$ will be called the *opposite design to M*. This obvious construction seems to have passed unnoticed in the literature on t-designs.

(107) Let $(E, \mathscr{H})$ be a $t-(v, k, \lambda)$ design and suppose that for some integers $l < k$ and λ' there exists a $t-(k, l, \lambda')$ design $(E', \mathscr{H}')$. For each $H \in \mathscr{H}$, let $(H, \mathscr{H}'_H)$ be any design on the set H that is isomorphic to $(E', \mathscr{H}')$, and let $\mathscr{H}''$ be the union (with repetitions) of the systems $\mathscr{H}'_H, H \in \mathscr{H}$. Then it is straightforward to verify that $(E', \mathscr{H}'')$ is a $t-(v, l, \lambda\lambda')$ design, called a *composition of* $(E, \mathscr{H})$ *with* $(E', \mathscr{H}')$. (This construction for BIBD's was pointed out by Hanani [7].)

Now let $M = (E, \mathscr{H})$ be a given $t-(v, k, 1)$ design.

(108) By (64), $r(M) = t+1$ and $\beta(M) = t$. Hence every circuit of M has cardinality $t+1$ or $t+2$. In this case, (94) and (98) have particularly simple interpretations.

(109) The family $\mathscr{C}_{t+1}$ of circuits of cardinality $(t+1)$ consists of precisely the $(t+1)$ subsets of the members of $\mathscr{H}$. Indeed, for any $H \in \mathscr{H}$, $r(H) = r(M) - 1 = t$, so every $(t+1)$-subset of H is dependent, and in fact minimal dependent, since $\beta(M) = t$. Conversely every circuit $\mathscr{C}$ of cardinality $t+1$ is contained in a hyperplane $H \in \mathscr{H}$, since $r(\mathscr{C}) = t$. Thus $(E, \mathscr{C}_{t+1})$ is a composition of $(E, \mathscr{H})$ with a $\sigma(1, t+1, k)$; i.e., $(E, \mathscr{C}_{t+1})$ is a $t-(v, t+1, k-t)$ design.

(110) The family β of bases of M is evidently precisely the collection of $(t+1)$-subsets of E that are not contained in $\mathscr{C}_{t+1}$. Thus (E, β) is a $t-(v, t+1, v-k)$ design, the opposite to $(E, \mathscr{C}_{t+1})$.

(111) Finally, the family $\mathscr{C}_{t+2}$ of cardinality $(t+2)$ circuits of M consists of precisely those $(t+2)$-subsets S of E such that every $(t+1)$-subset of S is a basis of M. Using (162), we find that $(E, \mathscr{C}_{t+2})$ is a

$$t-\left(v, t+2, \frac{(v-k)\ (v-(t-1)\ (k-t+1))}{2}\right)$$

design, which we shall call the *circuit design* of M.

The construction of (111) applies to any $t-(v, k, 1)$ design, and is apparently new. Table 1 shows the parameters of the known $t-(v, k, 1)$ designs with $t \geq 3$, and the associated circuit design parameters.

TABLE 1. *Parameters of known* t-(v, k, 1) *designs,* (t ≥ 3) *and associated circuit designs*

t-Design parameters	Circuit design parameters
$3-(6u+2, 4, 1)$, $u \geq 0$	$3-(6u+2, 5, 6(u-1)(3u-1))$
$3-(6u+4, 4, 1)$, $u \geq 0$	$3-(6u+4, 5, 6u(3u-2))$
$3-(q^n+1, q+1, 1)$, q a prime.	$3-\left(q^n+1, 5, \frac{(q^n-q)(q^n-4q+5)}{2}\right)$
$4-(11, 5, 1)$	$4-(11, 6, 3)$
$4-(23, 7, 1)$	$4-(23, 6, 24)$
$5-(12, 6, 1)$	vacuous, $\lambda = 0$
$5-(24, 8, 1)$	vacuous, $\lambda = 0$

3.11. Self-Dual PMD's

We close our discussion of PMD's by developing an intriguing unsolved problem in the theory of t-designs.

(112) A matroid $M=(E, \mathscr{H})$ is said to be *self-dual* if $M^*=M$; i.e., if the hyperplanes of M^* are identical with the hyperplanes of M.

(113) If M is self-dual, then in particular the bases of M and M^* are identical, so for every basis B of M, $E-B$ is also a basis of M. Hence $|E-B|=|B|$, so $r(M)=\frac{|E|}{2}$.

(114) THEOREM: M *is a simple, nontrivial, self-dual PMD if and only if* M *is a* (k−1)−(2k, k, 1) *design*, k > 2. *Moreover, such an* M *can exist only if* k+1 *is an odd prime.*

PROOF: Let $M=(E, \mathscr{H})$ be a simple, nontrivial, self-dual PMD and let $k(M)=k$. By (89), $k \leqslant \frac{|E|}{2}$. Further, $\frac{|E|}{2}=r(M)$, by (113). But $k=|H| \geqslant r(H)=r(M)-1$ for every $H \in \mathscr{H}$, so $\frac{|E|}{2}-1 \leqslant k \leqslant \frac{|E|}{2}$. If $k=\frac{|E|}{2}-1$, then evidently every hyperplane is a rank $r(M)-1$ independent set. But then every subset of cardinality $r(M)$ is a basis, so M is trivial, contrary to hypothesis. Hence $k=r(M)=\frac{|E|}{2}$, and every hyperplane contains a circuit. But the circuits are identical with the co-circuits, hence they all have cardinality $|E|-k=k$. Thus every hyperplane is a circuit, and conversely.

Since the circuits all have cardinality k, every $(k-1)$-subset of E is independent. Thus, for $0 \leqslant j \leqslant k-2$, the j-flats of M are all simple. Thus, M is a PMD with d-sequence $(k, 2, 1, 1, \ldots, 1)$ containing $k-2$ "1"'s. It follows from (64) that M is a $(k-1)-(2k, k, 1)$ design.

Now $k>2$, for otherwise M would be nonsimple. Suppose that $k+1$ is not a prime, and let p be a prime divisor of $k+1$, where $1<p<k+1$. By (42),

$$t_M(k-p-1, k-1, k)=\frac{(k+2+(p-2))(k+2+(p-3)) \ldots (k+2)}{(2+(p-2))(2+(p-3)) \ldots 2}$$

$$=\frac{(k+p)(k+p-1) \ldots (k+2)}{p(p-1) \ldots 2} \tag{115}$$

must be an integer. However, since p divides $(k+1)$, p does not divide any integer strictly between $k+1$ and $k+1+p$. Thus p does not divide the numerator of (115), which gives a contradiction.

(116) Suppose, conversely, that $M=(E, \mathscr{H})$ is a $D_{k-1}(2k, k, 1)$, $k>2$. Then $\beta(M)=k-1 \geqslant 2$, so M is simple. M is nontrivial, because every $(k-1)$-subset of E is contained in more than one k-subset when $|E|=2k \geqslant 6$. Finally, it has been observed by Mendelsohn [9] that for every $(k-1)-(2k, k, 1)$ design $(V, \mathscr{W})$, $W \in \mathscr{W}$ implies $E-W \in \mathscr{W}$. It follows that for every basis B of M, $E-B$ is also a basis; hence $M=M^*$. Therefore, M is a simple, nontrivial, self-dual PMD and, by the first part of the proof, $k+1$ is an odd prime.

(117) Corresponding to the primes 3, 5, and 7 are the self-dual PMD's $D_1(4, 2, 1)$, $D_3(8, 4, 1)$, and $D_5(12, 6, 1)$, respectively. Moreover, these are the unique simple, nontrivial self-dual PMD's for these orders. The existence of higher order examples is an unsolved problem.

4. Constructions of Matroid Designs and an Analysis of the Witt Design

In this concluding section we shall turn our attention to the general subject of matroid designs. In a matroid design M we only demand that all of the hyperplanes have the same cardinality, which we denote as before by $k(M)$. In particular, the points of a matroid design may have different cardinalities, which allows more structural freedom than is possible in PMD's. However, *simple* matroid designs are virtually as difficult to construct as PMD's. In fact, it might even be imagined that equicardinality of the points and of the hyperplanes of a matroid forces it to be a PMD. However, we shall show that this is not the case. In fact, we shall presently demonstrate a simple matroid design that is a 5-design, but not a perfect matroid design. We shall also present several basic constructions for matroid designs to illustrate the variety and complexity of these interesting structures.

The basis for our analysis is the knowledge that there exists a t-design with parameters 5-(24, 8, 1). This extraordinary design was discovered by Witt [13] and is constructed by considering the action of the Mathie permutation group M_{24} on a certain 8-subset of a 24-element permutation set. He also showed it to be the unique t-design with the given parameters, up to isomorphism. Unfortunately, its presentation as such gives little insight into its structure. However, regarding it as a matroid, and using only the knowledge of its parameters, we can derive considerable information about its properties. Simultaneously, we shall be led to discover a number of interesting and important matroid designs.

Let us denote Witt's 5-(24, 8, 1) design by W_{24}. By (64), W_{24} is a rank 6 PMD with hyperplane family $\mathscr{H}$, and its d-sequence is (16, 4, 1, 1, 1, 1).

(118) THEOREM: *The family $\mathscr{C}$ of circuits of $W_{24}=(E,\mathscr{H})$ is precisely the set of 6-subsets of members of $\mathscr{H}$, and $(E,\mathscr{C})$ is a 5-(24, 6, 3) design.*

PROOF: By (108) every circuit of W_{24} has cardinality 6 or 7. Let $\mathscr{C}_7$ be the set of circuits of cardinality 7. Then, substituting $v=24$, $k=8$, and $t=5$ into the expression for λ in (111), we have that $(E,\mathscr{C}_7)$ is a 5-(24, 7, 0) design; i.e., $\mathscr{C}_7=\emptyset$. Hence every circuit of W_{24} has cardinality 6, and it follows from (109) that the circuits of W_{24} are precisely the 6-subsets of members of $\mathscr{H}$. Therefore $(E,\mathscr{C})$ is the composition of $(E,\mathscr{H})$ with a $\sigma(1,6,8)$, so $(E,\mathscr{C})$ is a 5-(24, 6, 3) design.

(119) THEOREM: *The dual of W_{24}, W_{24}^*, is a simple rank 18 matroid design that is a 5-design but not a PMD.*

PROOF: Let $W_{24}=(E,\mathscr{H})$, with circuit family $\mathscr{C}$. By (8), the set $\mathscr{H}^*$ of hyperplanes of W_{24}^* is precisely the set of complements in E of the circuits of W_{24}; i.e., $(E,\mathscr{H}^*)$ is the complementary design to $(E,\mathscr{C})$. By (118), $(E,\mathscr{C})$ is a 5-(24, 6, 3) design, so it follows from (105) that $(E,\mathscr{H}^*)$ is a 5-(24, 18, $\binom{18}{5}/2$) design. Moreover, W_{24}^* is a matroid design, $k(W_{24}^*)=18$, and $r(W_{24}^*)=|E|-r(W_{24})=18$. The circuits of W_{24}^* are the complements of hyperplanes of W_{24}; hence they all have cardinality 16. In particular, W_{24}^* is simple. Hence W_{24}^* is a simple rank 18 matroid design that is a 5-design.

If W_{24}^* were a PMD, then by (118) it would either be a trivioid (which is clearly not the case), or it would satisfy $k(W_{24}^*)\leq|E|/2$, which is also not the case.

Using (119) and the basic properties of matroid flats, we can describe the flats of W_{24}^* exactly.

(120) THEOREM: (i) *For $0\leq j\leq 14$, the j-flats of $W_{24}^*=(E,\mathscr{H}^*)$ are just the j-subsets of E.*

(ii) *The 15-flats consist of all circuits, and all 15-subsets of E not contained in a circuit.*

(iii) *The 16-flats consist of all subsets of form $C\cup\{x\}$, where C is a circuit and $x\in E-C$, and all 16-subsets of E no 15 of which are contained in a circuit.*

(iv) *The 17-flats (hyperplanes) consist precisely of the sets of form $C\cup\{x,y\}$, where C is a circuit and $x, y\in E-C$, $x\neq y$.*

PROOF: For $0\leq j\leq 14$, let T be any j-subset of E. Since the circuits of W_{24}^* all have cardinality 16, T is independent, and $cl(T)=T$ by definition of closure. Hence, for $0\leq j\leq 14$, the j-flats or W_{24}^* are just the j-subsets of E, and (i) is proved.

(121) Let F^{15} be any 15-flat of W_{24}^*, and let H be a hyperplane containing F^{15}. Since $r(H)=r(F^{15})+2$, $|H|\geq|F^{15}|+2$, and since $|H|=18$, we have $|F^{15}|\leq 16$. If $|F^{15}|=16$, F^{15} must be dependent, so F^{15} is a circuit. Otherwise, $|F^{15}|=15$, and since F^{15} is closed, F^{15} is a set of 15 elements contained in no circuit. Conversely, every circuit C has rank 15, hence is contained in some 15-flat F^{15}; since $|F^{15}|\leq 16$, $C=F^{15}$. If T is a 15-subset of E contained in no circuit, then $r(T)=15$ and $cl(T)=T$, so T is a 15-flat. This proves (ii).

Let F^{16} be an arbitrary 16-flat of W_{24}^*. Using an argument like that of (121), we may show that

$$16\leq|F^{16}|\leq 17. \tag{122}$$

If $|F^{16}|=17$, F^{16} must be dependent; hence it is of form $C \cup \{x\}$ for some circuit C and $x \in E-C$. If $|F^{16}|=16$, then $cl(F^{16})=F^{16}$, so $F^{16} \cup \{x\}$ contains no circuit for any $x \in E$; hence no 15-subset of F^{16} is contained in a circuit. Conversely, any set $C \cup \{x\}$, where C is a circuit and $x \in E-C$, has rank 16 (since C is a 15-flat) and cardinality 17, so, by (122), $C \cup \{x\}$ is a 16-flat. If T is a 16-subset of E such that no 15-subset of T is contained in a circuit, then $cl(T)=T$ and T is independent, so T is a 16-flat. This proves (iii).

The characterization of the hyperplanes (iv) follows immediately from (118) and the fact that the hyperplanes and circuits of W_{24}^* are the complements, respectively, of the circuits and hyperplanes of W_{24}.

Using matroid theory alone, the possible structures of all contractions $W_{24}^* \cdot (E-F)$, where F is a flat of W_{24}^*, can be identified. As a way of introducing both concrete examples and general constructions of new matroid designs, we shall identify all the structures of $W_{24}^* \cdot (E-F)$ for $r(F)=14$ and $r(F)=15$.

We begin by describing a general matroid construction due to U.S.R. Murty. Let $M=(E, \mathscr{H})$ be a rank n matroid (not necessarily a matroid design) and let $\mathfrak{F}_{n-2}$ be the set of $(n-2)$-flats of M. For a given positive integer m, let $P(m)$ denote the matroid consisting of a single point on m elements (we shall identify $P(m)$ with the set of m elements itself), and choose $P(m)$ disjoint from E. Then it may easily be verified that $\mathscr{H}'=\mathscr{H} \cup \{P(m) \cup F : F \in \mathfrak{F}_{n-2}\}$ satisfies (H1) and (H2); hence $\mathscr{H}'$ is the family of hyperplanes of a matroid on the set $E'=E \cup P(m)$. $(E', \mathscr{H}')$ is called the *one-point extension of M by $P(m)$*, and denoted by $M \oplus P(m)$.

(123) Suppose now that M is a matroid design, $k(M)=k$, and suppose further that the $(n-2)$-flats of M all have cardinality $h<k$. Then clearly $M \oplus P(k-h)$ will be a matroid design with hyperplane size k.

We then have the following structural theorem about W_{24}^*. (For the proofs of this and the next theorem, the reader is referred to [15].)

(124) THEOREM: *For any 15-flat* F *of* W_{24}^*, $W_{24}^* \cdot (E-F)$ *has rank 3 and is either a* $\sigma(1,2,8)$ *or a* PG(2, 2) ⊕ P(2), *or an* EG(2, 3).

PG(2, 2) ⊕ *P*(2) is shown in figure 1. In this and subsequent matroid diagrams, the simple points will be represented by solid nodes, and points with $m>1$ elements will be represented by a hollow node containing the number m. 2-flats will be represented by lines, and 3-flats by planes, where convenient.

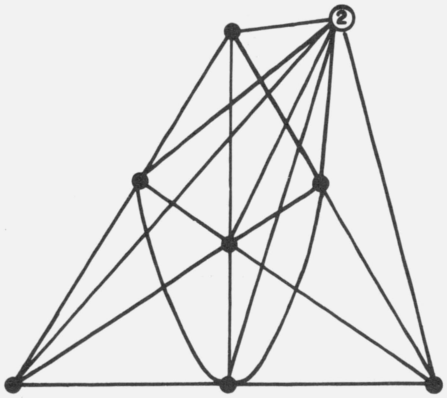

FIGURE 1. *The matroid design* PG (2, 2) ⊕ P (2).

The following matroid design arises as a rank 4 contraction of W_{24}^*. It is the smallest example of a simple matroid design that is not a PMD.

(125) Let L_1, L_2 be disjoint sets of three elements each, and let Q be the set of all nine pairs $\{x, y\}$ such that $x \in L_1$, $y \in L_2$. Let Q be partitioned into three sets P_1, P_2, P_3, each containing three pairs, such that the pairs in each P_i are mutually disjoint, $1 \leq i \leq 3$. Now let A be a set of four

elements disjoint from $L_1 \cup L_2$, and let Q' be the set of six distinct pairs $\{x, y\}$ in A. Let P'_1, P'_2, P'_3 be a partitioning of Q' into three sets, each containing two disjoint pairs of Q'. We define

$$E = A \cup L_1 \cup L_2;$$

$$Y_i = \{L_i \cup \{y\}:\ y \in E - L_i\}, \qquad \text{for } i = 1, 2,$$

$$Z_j = \{q \cup q':\ q \in P_j, \qquad q' \in P'_j\}, \qquad j = 1, 2, 3,$$

and

$$\mathscr{H} = \left(\bigcup_{j=1}^{3} Z_j\right) \cup \left(\bigcup_{i=1}^{2} Y_i\right) \cup \{A\}.$$

It is straightforward to verify that $(E, \mathscr{H})$ satisfies (H1) and (H2), hence is a matroid. We shall denote any matroid of this form by Ψ. By construction, Ψ is a matroid design, and $k(\Psi) = r(\Psi) = 4$. The lines of Ψ are precisely the sets of form $L = H_1 \cap H_2$ such that $|H_1 \cap H_2| \geqslant 2$ and H_1, H_2 are distinct members of $\mathscr{H}$. In particular, L_1 and L_2 are lines of Ψ, and every other line of Ψ is simple. Therefore Ψ is not a PMD. Finally, for every two distinct elements $x, y \in E$, there is a hyperplane containing x but not y, so Ψ itself is simple.

Representative lines and planes of Ψ are shown in figure 2.

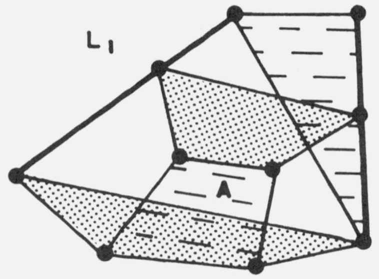

FIGURE 2. *The matroid design* Ψ.

(126) THEOREM: *For any 14-subset* F *of* W_{24}^*, $M = W_{24}^* \cdot (E - F)$ *is either*

(i) *an* $EG(3, 2) \oplus P(2)$

or (ii) Ψ

or (iii) *an* IP(3).

Moreover, each of these matroids actually occurs for some choice of F.

The complete analysis of the higher-rank contractions of W_{24}^* becomes quite tedious, and we shall forego it here. However, to illustrate the intricacy of structure possible in matroid designs, we shall present one example of a simple rank 5 matroid design that arises as a contraction $W_{24}^* \cdot (E - F)$, where F is a 13-flat of W_{24}^* contained in a circuit. We shall call this matroid $\Phi = (E', \mathscr{H}')$, and we describe it as follows.

(127) $|E'| = 11$, and all points of Φ are simple. Φ has one line of cardinality 3, $L = \{a, b, c\}$, and all other lines are simple. The remaining eight points of Φ are divided into two disjoint 3-flats having 4 elements each: F_1^3: $\{\alpha, \beta, \gamma, \delta\}$ and $F_2^3 = \{1, 2, 3, 4\}$. The sets of form $\{x\} \cup L$, where $x \in E' - L$, are also 3-flats of M. All other 3-flats are simple.

(128) $k(\Phi) = 5$ and for each $x \in L$, $\Phi \cdot (E - \{x\})$ is an $EG(3, 2) \oplus P(2)$, where $P(2) = L - \{x\}$. In other words, for each $x \in$ L, the family $\mathscr{H}'_x$ of hyperplanes containing x but not L, when restricted to the set $E - L$, form an $EG(3, 2)$ on $E - L$. In particular, $F_i^3 \cup \{x\} \in \mathscr{H}'_x$ for $i = 1, 2$ and each $x \in L$.

Let $\mathscr{H}''_x = \{H - \{x\}:\ H \in \mathscr{H}'_x\}$ for each x, $x = a, b, c$. Then $F_i^3 \in H''_x$ for each $x \in L$ and $i = 1, 2$. Moreover, F_1^3 and F_2^3 are the only sets common to any two of the families $\mathscr{H}''_x$, because they are the only 3-flats of Φ having cardinality 4 *and* contained in $E - L$.

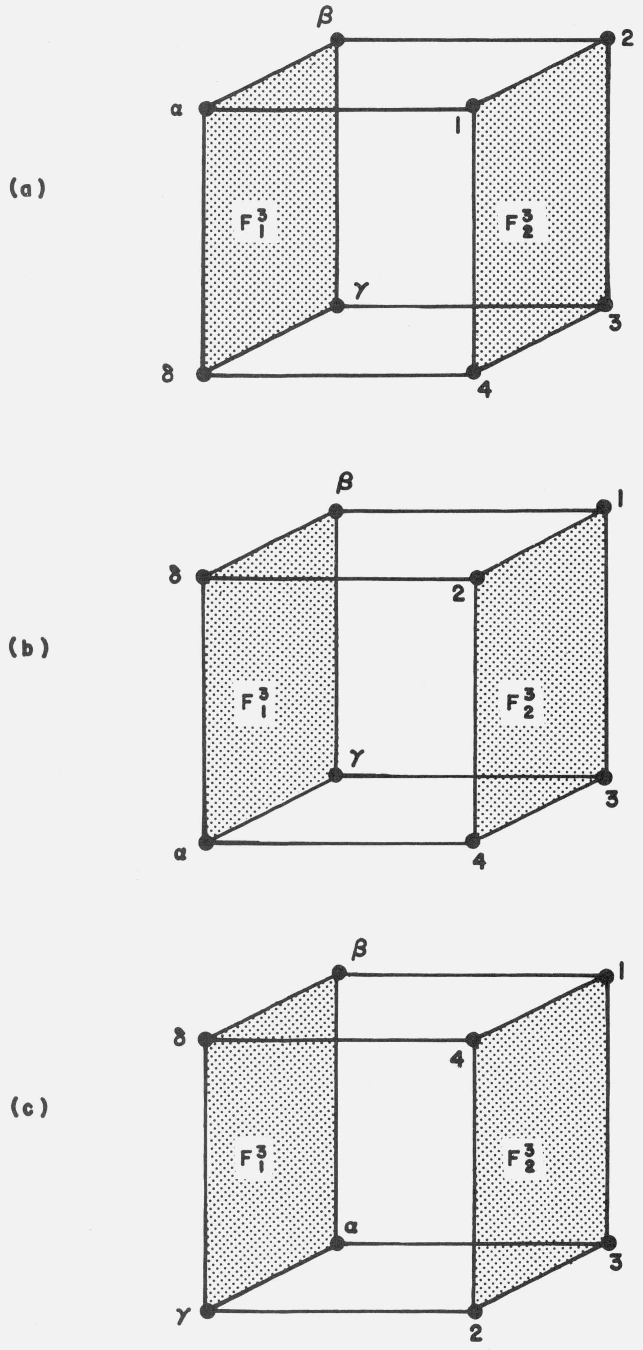

FIGURE 3. *Three copies* of EG (3, 2) *containing exactly two parallel hyperplanes in common.*

Thus, for $x=a, b, c$, the pairs $(E-L, \mathscr{H}_x'')$ constitute three copies of $EG(3,2)$ on the set $E-L$, each containing $F_1^3=\{\alpha, \beta, \gamma, \delta\}$ and $F_2^3=\{1, 2, 3, 4\}$ as their only common hyperplanes. Up to isomorphism there is only one way in which three sets of hyperplanes of an $EG(3, 2)$ may be so chosen. Three such sets are listed below, and the corresponding hyperplanes are diagrammed in Figure 3.

(a)	(b)	(c)
$\{\alpha,\beta,\gamma,\delta\}$	$\{\alpha,\beta,\gamma,\delta\}$	$\{\alpha,\beta,\gamma,\delta\}$
$\{1,2,3,4\}$	$\{1,2,3,4\}$	$\{1,2,3,4\}$
$\{1,2,\alpha,\beta\}$	$\{1,2,\alpha,\gamma\}$	$\{1,2,\alpha,\delta\}$
$\{1,2,\gamma,\delta\}$	$\{1,2,\beta,\delta\}$	$\{1,2,\beta,\gamma\}$
$\{1,3,\alpha,\gamma\}$	$\{1,3,\alpha,\delta\}$	$\{1,3,\alpha,\beta\}$
$\{1,3,\beta,\delta\}$	$\{1,3,\beta,\gamma\}$	$\{1,3,\gamma,\delta\}$
$\{1,4,\alpha,\delta\}$	$\{1,4,\alpha,\beta\}$	$\{1,4,\alpha,\gamma\}$
$\{1,4,\beta,\gamma\}$	$\{1,4,\gamma,\delta\}$	$\{1,4,\beta,\delta\}$
$\{2,3,\alpha,\delta\}$	$\{2,3,\alpha,\beta\}$	$\{2,3,\alpha,\gamma\}$
$\{2,3,\beta,\gamma\}$	$\{2,3,\gamma,\delta\}$	$\{2,3,\beta,\delta\}$
$\{2,4,\alpha,\gamma\}$	$\{2,4,\alpha,\delta\}$	$\{2,4,\alpha,\beta\}$
$\{2,4,\beta,\delta\}$	$\{2,4,\beta,\gamma\}$	$\{2,4,\gamma,\delta\}$
$\{3,4,\alpha,\beta\}$	$\{3,4,\alpha,\gamma\}$	$\{3,4,\alpha,\delta\}$
$\{3,4,\gamma,\delta\}$	$\{3,4,\beta,\delta\}$	$\{3,4,\beta,\gamma\}$

For each x, $x=a, b, c$, adjoin the element x to each of the sets in list (x), and let $\mathscr{S}_1$ be the resulting collection of 5-subsets of E'. Further, let $\mathscr{S}_2=\{\{x\} \cup F_i^3\colon x \in F_j^3, i \neq j\}$ and $\mathscr{S}_3=\{\{x, y\} \cup L\colon x, y \in E'-L \text{ and } x \neq y\}$. We claim that $\mathscr{H}'=\mathscr{S}_1 \cup \mathscr{S}_2 \cup \mathscr{S}_3$ is the hyperplane family of the matroid Φ having points, lines and 3-flats as described in (127). To show that $(E', \mathscr{H}')$ is a matroid, the principal facts that need to be checked are:
(i) that every two distinct hyperplanes intersect in a j-flat for some $j \leqslant 3$; and (ii) that for $0 \leqslant j \leqslant 3$ every j-flat F and element $x \in E-F$ lie in a common $(j+1)$-flat. The verification of (i) and (ii) is a straightforward matter of consideration by cases, and is left to the reader.

The preceding examples suggest the intricacy and variety of structure possible in matroid designs. Yet it is a remarkable fact that for large classes of integers γ, no matroid designs (other than trivioids) exist with cocircuit cardinality γ. And for many other classes of integers, all matroid designs with cocircuit cardinalities of that class can be described completely.

These and other results in the theory of matroid designs may be found in [14].

5. Appendix. Nontrivial *D*-Consistent Sequences With Leading Term *N*, $1 \leqslant N \leqslant 40$, and Associated PMD's

We list below all nontrivial D-consistent sequences of maximal length with leading term N, $1 \leqslant N \leqslant 40$. Those values of N, $1 \leqslant N \leqslant 40$, for which no such sequences exist are not listed. Each nontrivial D-consistent sequence D' having leading term N is an initial subsequence of some maximal such sequence D. The known PMD's having d-sequence D' are then listed after D and the symbol (m), where m is the length of D'. ($m \geqslant 3$ since D' is nontrivial.)

A $t-(v, k, \lambda)$ design (see Sec. 3.2) is denoted here by $D_t(v, k, \lambda)$. $PG(n, s)$ and $EG(n, s)$ denote, respectively, the finite projective and affine geometries of dimension n and order s, and $IP(s)$ denotes an inversive plane of order s. The inversive planes are discussed in (67). Finally, $M^{(l)}$ denotes the truncation of the matroid M at level l (see (37)).

Sources for the construction of all PMD's listed are given by paragraph number or reference number. In several cases it may be proved that some initial subsequence of a D-consistent sequence D is not realizable. This implies, by (81), that D itself is not realizable. Reference is made in these cases to the appropriate theorems in the text.

N	Maximal D-consistent sequences	Initial sub-sequence lengths	Associated PMD's	References
4	4, 2, 1, 1	(3)	$PG(2, 2)$	(72)
		(4)	$EG(3, 2)$	(77)
6	6, 2, 1, 1, 1, 1	(3)	$EG(2, 3)$	(77)
		(4)	$IP(3)$	(67)
		(5)	$D_4(11, 5, 1)$	[13]
		(6)	$D_5(12, 6, 1)$	[13]
8	8, 4, 2, 1, 1	(4)	$PG(3, 2)$	(72)
		(5)	$EG(4, 2)$	(77)
9	9, 3, 1	(3)	$PG(2, 3)$	(72)
10	$10, 2, \underbrace{1, \ldots, 1}_{8\ \text{terms}}$	(3)	$D_2(13, 3, 1)$	[3]
		(4)	$D_3(14, 4, 1)$	[4]
		(5)–(10)	unknown	
12	$12, 2, \underbrace{1, \ldots, 1}_{10\ \text{terms}}$	(3)	$D_2(15, 3, 1)$	[3]
		(4)	$D_3(16, 4, 1)$	[4]
		(5)–(12)	unknown	
	12, 3, 1, 1, 1	(3)	$EG(2, 4)$	(77)
		(4)	$IP(4)$	(67)
		(5)	unknown	
16	$16, 2, \underbrace{1, \ldots, 1}_{14\ \text{terms}}$	(3)	$D_2(19, 3, 1)$	[3]
		(4)	$D_3(20, 4, 1)$	[4]
		(5)–(16)	unknown	
	16, 4, 1, 1, 1, 1	(3)	$PG(2, 4)$	(72)
		(4)	$D_3(22, 6, 1)$	[13]
		(5)	$D_4(23, 7, 1)$	[13]
		(6)	$D_5(24, 8, 1)$	[13]
	16, 8, 4, 2, 1, 1	(5)	$PG(4, 2)$	(72)
		(6)	$EG(5, 2)$	(77)
18	$18, 2, \underbrace{1, \ldots, 1}_{16\ \text{terms}}$	(3)	$D_2(21, 3, 1)$	[3]
		(4)	$D_3(22, 4, 1)$	[4]
		(5)–(18)	unknown	
	18, 6, 2, 1	(4)	$EG(3, 3)$	(77)
20	20, 4, 1, 1	(3)	$EG(2, 5)$	(77)
		(4)	$IP(5)$	(67)
21	$21, 3, \underbrace{1, \ldots, 1}_{7\ \text{terms}}$	(3)	$D_2(25, 4, 1)$	
		(4)–(9)	unknown	
	$22, 2, \underbrace{1, \ldots, 1}_{20\ \text{terms}}$	(3)	$D_2(25, 3, 1)$	[3]
		(4)	$D_3(26, 4, 1)$	[4]
		(5)–(22)	unknown	
24	24, 2, 1, 1	(3)	$D_2(27, 3, 1)$	[3]
		(4)	$D_3(28, 4, 1)$	[4]

N	Maximal D-consistent sequences	Initial subsequence lengths	Associated PMD's	References
	24, 3, 1	(3)	$D_2(28, 4, 1)$	[5]
	24, 4, 2, 1, 1	(4) (5)	$PG(4, 2)^{(4)}$ $EG(5, 2)^{(5)}$	(72) (77)
25	25, 5, 1	(3)	$PG(2, 5)$	(72)
27	27, 9, 3, 1	(4)	$PG(3, 3)$	(72)
28	$28, 2, \underbrace{1, \ldots, 1}_{26 \text{ terms}}$	(3) (4) (5) – (28)	$D_2(31, 3, 1)$ $D_3(32, 4, 1)$ unknown	[3] [4]
30	$30, 2, \underbrace{1, \ldots, 1}_{28 \text{ terms}}$	(3) (4) (5) – (30)	$D_2(33, 3, 1)$ $D_3(34, 4, 1)$ unknown	[3] [4]
	30, 5, 1, 1	(3)	$EG(2, 6)$ – does not exist	[3]
32	32, 16, 8, 4, 2, 1	(6) (7)	$PG(5, 2)$ $EG(6, 2)$	(72) (77)
33	33, 3, 1	(3)	$D_2(37, 4, 1)$	[5]
34	34, 2, 1, 1	(3) (4)	$D_2(37, 3, 1)$ $D_3(38, 4, 1)$	[3] [4]
36	$36, 2, \underbrace{1, \ldots, 1}_{34 \text{ terms}}$	(3) (4) (5) – (36)	$D_2(39, 3, 1)$ $D_3(40, 4, 1)$ unknown	[3] [4]
	$36, 3, \underbrace{1, \ldots, 1}_{15 \text{ terms}}$	(3) (14) – (17)	$D_2(40, 4, 1)$ unknown	[3]
	$36, 4, \underbrace{1, \ldots, 1}_{8 \text{ terms}}$	(3) (4) – (10)	$D_2(41, 5, 1)$ unknown	[3]
	36, 6, 1	(3)	$PG(2, 6)$ – does not exist	[3]
	$36, 4, 2, \underbrace{1, \ldots, 1}_{6 \text{ terms}}$	(4) – (9)	does not exist	(75)
40	$40, 2, \underbrace{1, \ldots, 1}_{38 \text{ terms}}$	(3) (4) (5) – (40)	$D_2(43, 3, 1)$ $D_3(44, 4, 1)$ unknown	[3] [4]
	40, 4, 1, 1	(3) (4)	$D_2(45, 5, 1)$ unknown	[5]
	40, 5, 1	(3)	unknown	

6. References

[1] Birkhoff, G., Lattice Theory, Amer. Math. Soc., Coll. Pubns. **25** (1967).
[2] Edmonds, J., 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).
[3] Hall, M., Jr., Combinatorial Theory (Blaisdell, Waltham, Mass. 1967).
[4] Hanani, H., On Quadruple Systems, Can. J. Math. **12**, 145–157 (1960).
[5] Hanani, H., The existence and construction of balanced incomplete block designs, Ann. Math. Stat. **32**, 361–386 (1961).
[6] Hanani, H., On some tactical configurations, Can. J. Math. **15**, 702–722 (1963).
[7] Hughes, D. R., On *t*-designs and groups, Amer. J. Math. **87**, 761–778 (1965).
[8] Lenz, H., Zur Begrundung der analytischen Geometrie, Sitzber. Bayer. Akad: Wiss. Math. Naturw. Kl. 17–72, (1954).
[9] Mendelsohn, N. S., Intersection numbers of *t*-designs, Studies in Pure Mathematics (Academic Press, to appear).
[10] Murty, U.S.R., Equicardinal matroids and finite geometries, in Combinatorial Structures and their Applications (Gordon and Breach, New York, 1970).
[11] Riordan, J., Combinatorial Identities (Wiley, New York, 1968).
[12] Seidenberg, A., Lectures in Projective Geometry (Van Nostrand, Princeton, N.J., 1962).
[13] Witt, E., Uber Steinersche Systeme, Abh. Hamburg **12**, 265–275 (1938).
[14] Young, H. P., Existence theorems for matroid designs, submitted to Trans. Amer. Math. Soc.
[15] Young, H. P., Equicardinal matroids and matroid designs, Ph.D. Dissertation, University of Michigan, December, 1970.

(Paper 77–376)