71-15,351

YOUNG, Hobart Peyton, 1945-
EQUICARDINAL MATROIDS AND MATROID DESIGNS.

The University of Michigan, Ph.D., 1970
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED

# EQUICARDINAL MATROIDS

# AND

# MATROID DESIGNS

by
Hobart Peyton Young

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
1970

Doctoral Committee:

Professor Jack Edmonds, University of Waterloo, Co-Chairman
Assistant Professor Thomas F. Storer, Co-Chairman
Assistant Professor Peter G. Hinman
Professor Roger C. Lyndon
Assistant Professor Katta G. Murty
Professor Crispin St. J. A. Nash-Williams, University of Waterloo

ABSTRACT

EQUICARDINAL MATROIDS AND MATROID DESIGNS

by

Hobart Peyton Young

Co-Chairmen: Jack Edmonds, Thomas F. Storer

In this paper we investigate matroids in which equicardinality conditions are imposed on the flats (closed sets). An equicardinal matroid is a matroid in which all the maximal proper flats (hyperplanes) have the same cardinality. A matroid design is a matroid in which the flats of each given rank have the same cardinality. Equicardinal matroids and matroid designs turn out to be closely related to BIBD's. Every nontrivial simple matroid design is, in particular, a BIBD; in fact, the families of flats of any two different ranks in a matroid design constitute the objects and blocks of a BIBD. Examples of matroid designs are the finite projective, affine and inversive geometries, certain t-designs (Steiner systems) and so-called trivioids. In addition, the class of matroid designs apparently includes a whole collection of complex combinatorial structures never suspected before.

We develop a general parametric description of the inclusion relations among the flats of a matroid design, together with consistency conditions on these parameters that extend the well-known parametric relations of BIBD theory. We also develop

several new types of existence conditions that arise specifically from the matroid structure of a matroid design. We prove that, in any matroid design, the number of flats of rank $i$ is a unimodal function of $i$. We then use the parametric conditions to show that, in any matroid design containing $v$ points, the number $k$ of points in any hyperplane is bounded by $v/2$, and the rank is bounded by $v-k$.

By viewing certain BIBD's as matroid designs, we are led to discover several new ways of constructing BIBD's. We present three new series of 3-designs and two new 4-designs obtained by these methods.

The equicardinality of the hyperplanes of a matroid does not imply the equicardinality of the flats of lower ranks, and hence equicardinal matroids are more general than matroid designs. However, it turns out that they also are closely related to BIBD's. They are also surprisingly difficult to find (except for the trivial ones, such as Boolean algebras). We analyze in detail the 5-(24,8,1) design discovered by E. Witt and produce a rank 18 equicardinal matroid based on it that is a 5-design but not a matroid design. We also give general methods for constructing equicardinal matroids that are not matroid designs. Finally, we develop a theory of equicardinal

matroids that allows us to give a virtually complete characterization of all equicardinal matroids of rank 4 or less on a set of $v$ elements and having hyperplane cardinality $k$, where $v-k$ is a prime, a prime squared, or the product of distinct primes $p$ and $q$ such that $p < \frac{2q}{3} + 1$. For $1 \leq v-k \leq 100$, we list all such nontrivial equicardinal matroids explicitly.

## ACKNOWLEDGEMENTS

The author wishes to acknowledge a special debt to U. S. R. Murty, who first introduced equicardinal matroids, and who provided many fruitful ideas to the development of the subject. The author also wishes to thank C. St. J. A. Nash-Williams for generous financial support while the dissertation was being written, T. Storer, who provided helpful comments on the final draft, and Rene Banks, who did a commendable job of typing the manuscript. Finally, the author expresses his particular appreciation for the encouragement and instruction offered by his supervisor, Jack Edmonds.

TABLE OF CONTENTS


Page

ACKNOWLEDGEMENTS . . . . . ii

LIST OF TABLES . . . . . vi

LIST OF ILLUSTRATIONS . . . . . vii

Chapter

I. INTRODUCTION . . . . . 1

II. MATROIDS . . . . . 6

III. MATROID DESIGNS . . . . . 17

3.1. The geometry of flats in a matroid design . . . . . 17

3.2. t-designs . . . . . 21

3.3. Consequences of Fisher's inequality for matroid designs . . . . . 23

3.4. Further properties of matroids and matroid designs . . . . . 25

3.5. Trivioids . . . . . 33

3.6. t-designs as examples of matroid designs . . . . . 34

3.7. Finite projective and affine geometries as examples of matroid designs . . . . . 37

3.8. d-sequences and D-consistency . . . . . 44

3.9. Unimodality in matroid designs . . . . . 52

3.10. Characterization of matroid designs by d-sequences . . . . . 54

3.11. Computation of D-consistent sequences. . . 68

3.12. Bounds on rank of nontrivial matroid designs with given co-circuit cardinality. . 72

3.13. The t-designs in a matroid design . . . . 78

3.14. Some new t-designs . . . . . 87

3.15. Self-dual matroid designs . . . . . 91

IV. EQUICARDINAL MATROIDS . . . . . 95

4.1. Equicardinal matroids that are not matroid designs . . . . . 95

4.2. The characterization problem . . . . . 117

4.3. A diophantine analysis of rank 3 equicardinal matroids . . . . . 127

4.4. Rank 3 equicardinal matroids with co-circuit cardinality a prime or prime squared . . . . . 130

4.5. Affine extension . . . . . 133

4.6. Rank 3 equicardinal matroids with co-circuit cardinality pq, p and q distinct primes . . . . . 140

4.7. Characterization of higher rank equicardinal matroids . . . . . 160

4.8. Transversal designs . . . . . 181

4.9. Conclusion . . . . . 188

Appendix

I. NONTRIVIAL D-CONSISTENT SEQUENCES WITH LEADING TERM N, $1 \leq N \leq 40$, AND ASSOCIATED MATROID DESIGNS . . . . . 191

II. NONTRIVIAL RANK 3 AND 4 EQUICARDINAL MATROIDS HAVING CO-CIRCUIT CARDINALITY $\gamma$ SUCH THAT $1 \leq \gamma \leq 100$ AND $\gamma$ IS NOT DIVISIBLE BY THREE DISTINCT PRIMES . . . . . 196

LIST OF REFERENCES . . . . . 201

## LIST OF TABLES

Page

Table

1. Parameters of known t-(v,k,1) designs ($t \geq 3$) and associated circuit designs . . . . . 91

2. Three infinite series of simple equicardinal matroids that are not matroid designs . . . . . 188

## LIST OF ILLUSTRATIONS


Page

Figure

1. The equicardinal matroid $PG(2,2) \oplus P(2)$ . . . . . 104
2. The equicardinal matroid $\Upsilon$ . . . . . 105
3. Three copies of EG(3,2) containing exactly two parallel hyperplanes in common . . . . . 116
4. A connected matroid having a disconnected contraction . . . . . 122
5. Two examples of affine extension . . . . . 137
6. The complete graph extension of order 3 . . . . 138
7. The equicardinal matroid $\Lambda$ . . . . . 179
8. The equicardinal matroid $\Omega$ . . . . . 181

## LIST OF APPENDICES

Page

Appendix

I. Nontrivial D-consistent sequences with leading term N, $1 \leq N \leq 40$, and associated matroid designs . . . . . 191

II. Nontrivial rank 3 and 4 equicardinal matroids having co-circuit cardinality $\gamma$ such that $1 \leq \gamma \leq 100$ and $\gamma$ is not divisible by three distinct primes . . . . . 196

# CHAPTER I

## INTRODUCTION

In this paper we shall investigate mathematical structures that bring together matroid theory and the theory of balanced incomplete block designs. From this unification we shall derive a number of new results in both of these fields.

A matroid may be viewed as a geometrical structure consisting of flats (closed sets) and a rank function on these flats. The rank 1 flats are the points, and the flats having rank one less than the rank of the whole space are the hyperplanes. An equicardinal matroid [13] is a matroid in which all the hyperplanes have the same cardinality. Equicardinal matroids are closely related to certain types of block designs; frequently, they consist of block designs that have been modified by the addition or deletion of certain objects and blocks. However, relatively few block designs are matroids. Indeed, equicardinal matroids (other than trivial ones such as Boolean algebras) are quite rare. We are, therefore, able to completely characterize certain general classes of equicardinal matroids.

In fact, we shall show that for certain integers v and k, there exist no nontrivial equicardinal matroids on a set of v elements with hyperplane cardinality k. These results are presented in Chapter IV.

In Chapter IV we shall also introduce a certain generalization of block designs, called transversal designs, that give rise to a broad class of equicardinal matroids. The elements of a theory for the existence of transversal designs are established, and several infinite classes are constructed. The subject of transversal designs appears to have important applications to the construction of balanced and partially balanced block designs, although we shall concentrate mainly on its relation to equicardinal matroids.

Surprisingly, the equicardinality of the hyperplanes in a matroid does not imply the equicardinality of the flats in lower ranks. A matroid in which the flats of any given rank are equicardinal is called a matroid design. By assigning appropriate cardinalities to the points of classical finite projective geometrics, equicardinal matroids that are not matroid designs may be constructed. In fact, we are able to exhibit a rank 18 equicardinal matroid in which all of the flats of any given rank, except ranks 15 and 16, are equicardinal. This extraordinary matroid is derived from a

5-(24,8,1) design discovered by Witt [19], and is itself a 5-design. Along the way we shall analyze the structure of the Witt design, using just the matroid theory developed in Chapter II.

In Chapter III we shall study matroid designs, which are considerably rarer than either equicardinal matroids or block designs. Matroid designs are endowed with the type of regularity conditions found in the classical finite geometries; however, they also include certain t-designs (Steiner systems), so-called trivioids, and apparently a whole collection of highly complex combinatorial designs never suspected before. The complexity of a (nontrivial) matroid design is illustrated by the fact that the families of flats of any two different ranks constitute the objects and blocks of a balanced incomplete block design.

In the other direction, we may view certain classes of block designs as matroid designs, and by this observation obtain new ways of constructing block designs. We shall present several new series of 3-designs, and two new 4-designs obtained by these methods.

The theory of matroid designs is based on a parametric description of inclusion relations among the flats, together with consistency conditions on the parameters that extend the

standard parametric relations of block design theory. In addition, we shall point out several new types of existence conditions that arise from the matroid structure of a matroid design. We shall also provide an efficient method for determining which sets of parameters (called d-sequences) are consistent. In certain cases it will be shown that a consistent d-sequence is associated with a unique matroid design.

The properties of d-sequences will be used to prove the following result: in any matroid design containing $v$ points, the number $k$ of points in any hyperplane is bounded by $v/2$, and the rank is bounded by $v-k$. We shall also show that the number of flats of rank $i$ in a matroid design is a unimodal function of $i$. This result supports a similar conjecture for general matroids that is still unresolved.

A particularly interesting class of matroid designs are the self-dual matroid designs, i.e., those in which the complement of a hyperplane is also a hyperplane. It will be shown that a necessary condition for the existence of a self-dual matroid design is that its rank be one less than an odd prime. We also conjecture that, for every odd prime, there exists such a matroid and it is unique. The conjecture is observed to be true for the primes 3, 5, and 7.

We begin the development of this theory by establishing some of the basic properties of matroids, and then proceed to analyze the structure of matroid designs. From there we shall pass to a presentation of examples and an analysis of the Witt design. We conclude with a discussion of transversal designs and the major characterization theorems for equicardinal matroids.

# CHAPTER II

## MATROIDS

Matroids were originally defined by Whitney [18] to represent abstractly certain properties of linear dependence among vectors. Since then matroid theory has been further developed by other authors, in differing contexts and sometimes using different terminology than that introduced by Whitney. Since no really standard references for the subject exist, we shall develop the basic concepts and theorems necessary for our purposes here. For a more detailed treatment of certain topics, the reader is referred to Whitney [18], Tutte [17], and Edmonds [4].

(1) A <u>matroid</u> $M = (E, \mathcal{I})$ is defined to be a finite set $E$ together with a non-empty set $\mathcal{I}$ of subsets of $E$, called <u>independent</u> sets, such that: (I1) Every subset of an independent set is independent; (I2) For every $A \subseteq E$, all maximal independent subsets of $A$ have the same cardinality, called the <u>rank</u> of $A$, $r(A)$.

A maximal independent subset of $A$ is called a <u>basis of A</u>, or <u>M-basis of A</u>, if we wish to specify the matroid under consideration. A <u>basis of M</u> is just an M-basis of $E$, and $r(M)$, the <u>rank of M</u>, 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 matroid may be characterized by its bases as follows.

(2) Theorem. A set $\mathcal{B}$ of subsets of a finite set $E$ constitute the bases of a matroid on the set $E$ if and only if

(B1) $\mathcal{B}$ is nonempty and no member of $\mathcal{B}$ is a proper subset of another.

(B2) For every pair $B_1$, $B_2 \in \mathcal{B}$ and $x \in B_1$ there is a $y \in B_2$ such that $(B_1-\{x\}) \cup \{y\} \in \mathcal{B}$.

Proof. Let $E$ together with $\mathcal{B}$ satisfy (B1) and (B2), and let $\mathcal{J}$ be the family of subsets of members of $\mathcal{B}$. We shall show that $(E,\mathcal{J})$ satisfies (I1) and (I2), and hence that $\mathcal{J}$ is the set of independent sets of a matroid with basis family $\mathcal{B}$. (I1) is satisfied by definition of $\mathcal{J}$.

To verify (I2), we show first that every two members of $\mathcal{B}$ have the same cardinality. Suppose to the contrary that $|B_2| > |B_1|$ for some pair $B_1$, $B_2 \in \mathcal{B}$, and let $|B_1 \cap B_2|$ be maximum among all such pairs. Let $x \in B_1-B_2$ ($B_1 \not\subseteq B_2$ by hypothesis (B1)), and let $y \in B_2$ such that $B = (B_1-\{x\})\cup\{y\} \in \mathcal{B}$. Then $y \in B_2-B_1$, for otherwise we would have $B \supsetneq B_1$; hence

$|B \cap B_2| > |B_1 \cap B_2|$, a contradiction. Thus $|B_1| = |B_2|$ for every pair $B_1, B_2 \in \mathcal{B}$.

Now let $A \subseteq E$ and let $I_1, I_2$ be two maximal members of $\mathcal{I}$ contained in $A$. Let $I_1 \subseteq B_1 \in \mathcal{B}$, and choose $B_2 \in \mathcal{B}$ such that $I_2 \subseteq B_2$ and $|B_2 \cap (B_1 \cup A)|$ is maximum. If $B_2 \not\subseteq B_1 \cup A$, let $x \in B_2 - (B_1 \cup A)$, and (using (B2)) choose $y \in B_1$ such that $B = (B_2 - \{x\}) \cup \{y\} \in \mathcal{B}$. Now $I_2 \subseteq B$, and since $|B| = |B_2|$ by the above, we must have $|B \cap (B_1 \cup A)| > |B_2 \cap (B_1 \cup A)|$, contradicting the choice of $B_2$. Hence $B_2 \subseteq B_1 \cup A$. $I_2 \subseteq B_2 \cap A$, and $B_2 \cap A$ is an independent subset of $A$, so $I_2 = B_2 \cap A$ by the maximality of $I_2$. Thus $B_1 - I_1 \supseteq B_2 - I_2$. Since $|B_1| = |B_2|$, we have $|I_1| \leq |I_2|$. A similar argument shows that $|I_2| \leq |I_1|$, and so (I2) is proved.

Conversely, let $(E, \mathcal{I})$ satisfy (I1) and (I2), and let $\mathcal{B}$ be the set of maximal members of $\mathcal{I}$. Since $\mathcal{I} \neq \emptyset$, $\mathcal{B} \neq \emptyset$, and clearly no member of $\mathcal{B}$ is a proper subset of another. Thus (B1) is proved.

Let $B_1, B_2 \in \mathcal{B}$, let $x \in B_1$, and consider $A = B_1 \cup B_2 - \{x\}$. $|B_1| = |B_2|$, by (I2), and $r(A) = |B_1|$. Since $B_1 - \{x\}$ is independent, $B_1 - \{x\}$ is contained in a basis $B$ of $A$, where $|B| = |B_1|$. Thus $B - (B_1 - \{x\}) = \{y\}$ for some $y \in B_2$, which establishes (B2). ∎

(3) Let $M = (E,\mathcal{J})$ be a matroid. A subset of $E$ is called dependent if it is not independent, and a minimal dependent set is called a circuit. 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 $M$.

(4) It follows easily from the definition (3) that the intersection of a family of closed sets is closed.

(5) It is also clear that if $A \subseteq B$, then $cl(A) \subseteq cl(B)$.

We may characterize the closure of a set as follows.

(6) 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 $C$ that is not contained in $J$; hence $x \in cl(A)$. Therefore $S \subseteq cl(A) \subseteq S$, so $S = cl(A)$. ∎

(7) Corollary. $cl(cl(A) \cup B) = cl(A \cup B)$ for any subsets $A, B$ of $E$.

A k-flat of $M$ is a closed subset of $E$ having rank $k$, i.e., a maximal subset of $E$ having rank $k$. The hyperplanes of $M$ are its $(r(M)-1)$-flats. In other words, the hyperplanes of $M$ are the maximal subsets of $E$ that contain no basis of $M$. We shall usually denote the family of hyperplanes of the matroid $M$ by $\mathcal{H}$.

(8) Any matroid $M$ is determined by the set $E$ on which it is defined and its hyperplanes, since $B \subseteq E$ is a basis of $M$ if and only if it is a minimal set contained in no hyperplane.

(9) Theorem. Let $\mathcal{H}$ be a family of subsets of a finite set $E$. $\mathcal{H}$ is the hyperplane family of a matroid on the set $E$ if and only if

(H1) $\mathcal{H}$ is a family of proper subsets of $E$ such that no member of $\mathcal{H}$ is a proper subset of another.

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

Proof. Let $\mathcal{H}$ be the hyperplane family of a matroid $M$ on the set $E$. (H1) is clearly satisfied. To prove (H2), we shall prove the following stronger statement.

(H2)′ For any two distinct members $H_1$ and $H_2$ of $\mathcal{H}$, and for any $x \in E - (H_1 \cup H_2)$ and $y \in H_1 - H_2$, $\{x\} \cup (H_1 \cap H_2)$ is contained

in some member of $\mathcal{H}$ not containing $y$.

Let $H_1$, $H_2$, $x$, and $y$ be as in (H2)'. By (4), $F = H_1 \cap H_2$ is closed; let $J$ be a basis of $F$. Since $F$ is closed and $y \notin F$, $J \cup \{y\}$ is independent. By (6), $cl(J) = F$, so $F \subseteq cl(J \cup \{y\}) \subseteq cl(H_1) = H_1$, by (5). Therefore, $x \notin cl(J \cup \{y\})$, and so $J \cup \{x,y\}$ is independent. Let $B$ be a basis of $M$ containing $J \cup \{x,y\}$. Then $H = cl(B-\{y\}) \in \mathcal{H}$ and $F \cup \{x\} \subseteq cl(J \cup \{x\}) \subseteq H$, while $y \notin H$ by (6). Hence (H2)' is proved, and (H2) follows.

Conversely, let $\mathcal{H}$ be a set of subsets of the set $E$ such that (H1) and (H2) are satisfied. Let $\mathcal{B}$ be the set of minimal subsets of $E$ contained in no member of $\mathcal{H}$. We shall show that $\mathcal{B}$ satisfies (B1) and (B2). $\mathcal{B} \neq \emptyset$, because by (H1) $E$ is a set contained in no member of $\mathcal{H}$, and hence there exists a minimal such set. Further, no member of $\mathcal{B}$ is contained in another, by definition; hence (B1) is satisfied.

(9a) For any $B \in \mathcal{B}$ and $x \in B$, there is a unique member $H_{B,x}$ of $\mathcal{H}$ containing $B-\{x\}$; for if $B-\{x\} \subseteq H_1 \cap H_2$ for distinct $H_1$, $H_2 \in \mathcal{H}$, then, by (H2), $B \subseteq H$ for some $H \in \mathcal{H}$, which is impossible.

(9b) Suppose that $|B-H| = 1$ for some $H \in \mathcal{H}$ and $B \in \mathcal{B}$; say $B-H = \{x\}$. For any $y \in E-H$, $B_y = (H \cap B) \cup \{y\}$ is not contained in $H$, and it is contained in no other member of $\mathcal{H}$, by (9a). $B_y$ is also minimal with this property. Indeed, $B_y-\{y\} \subseteq H$;

and for any $z \in H \cap B$, $H \cap B - \{z\} \subseteq H_{B,z} \cap H_{B,x}$, so there is an $H \in \mathcal{H}$ such that $B_y - \{z\} = (H \cap B - \{z\}) \cup \{y\} \subseteq H$, by (H2). Therefore, $B_y \in \mathcal{B}$ for every $y \in E-H$.

Now let $B_1$ and $B_2$ be two members of $\mathcal{B}$, and let $x \in B_1$. Since, $B_2 \not\subseteq H_{B_1,x}$, there exists $y \in B_2 - H_{B_1,x}$, and $\{y\} \cup H_{B_1} \cap B_1 = \{y\} \cup (B_1 - \{x\}) \in \mathcal{B}$, by (9b). Thus (B2) is proved, and $M$ is a matroid.

For any hyperplane $K$ of $M$, let $B \in \mathcal{B}$ such that $|B-K| = 1$; say $B-K = \{x\}$. If $K \not\subseteq H_{B,x}$, say $y \in K - H_{B,x}$, then $B' = \{y\} \cup (B-\{x\}) \in \mathcal{B}$ and $B' \subseteq K$, which is absurd. Hence $K \subseteq H_{B,x}$. Since $K$ is a maximal subset containing no member of $\mathcal{B}$, $K = H_{B,x}$, so $K \in \mathcal{H}$. Conversely, every member of $\mathcal{H}$ is certainly contained in some hyperplane. Since no member of $\mathcal{H}$ properly contains another, it follows that $\mathcal{H}$ is precisely the hyperplane family of $M$. ∎

Depending on the context we shall sometimes denote a matroid $M$ by $(E,\mathcal{H})$, where $\mathcal{H}$ is its family of hyperplanes, and sometimes by $(E,\mathcal{J})$, where $\mathcal{J}$ is its family of independent sets.

(10) From the proof of (9 ), it is easily seen that $M = (E,\mathcal{H})$ is a matroid if and only if it satisfies the "Strong Hyperplane Axioms" (H1) and (H2)′.

The total collection of flats of a matroid $(E,\mathcal{H})$ is easily found from the hyperplanes as follows.

(11) Theorem. $F$ is a flat of a matroid $M = (E,\mathcal{H})$ if and only if $F = E$ or $F$ is the intersection of a set of hyperplanes of $M$.

Proof. The intersection of any set of hyperplanes of $M$ is a flat, by (4), and $E$ itself is certainly a flat.

Conversely, let $F$ be any flat of $M$ such that $F \neq E$, and let $\mathcal{H}'$ be the set of all hyperplanes containing $F$. Since $F \neq E$, $\mathcal{H}' \neq \emptyset$, so the flat $F' = \bigcap_{H \in \mathcal{H}'} H$ contains $F$. If $F' \neq F$, let $y \in F'-F$. Where $J$ is any basis of $F$, $J \cup \{y\}$ is independent, since $F$ is closed. Let $B$ be a basis of $M$ containing $J \cup \{y\}$, and let $H = cl(B-\{y\})$. Then $H \in \mathcal{H}'$ but $F' \not\subseteq H$, a contradiction. Hence $F = F'$; that is, $F$ is the intersection of hyperplanes containing it. ∎

(12) Given any matroid $M$ on the set $E$, with basis family $\mathcal{B}$, the dual of $M$, $M^*$, is the matroid on the set $E$ with basis family $\mathcal{B}^* = \{E-B : B \in \mathcal{B}\}$. It is straightforward to verify that (B1) and (B2) hold for $\mathcal{B}^*$. We also note the obvious fact that $M^{**} = M$.

(13) With $M$ and $\mathcal{B}$ as in (12), the set $\mathcal{H}$ of hyperplanes of $M$ is precisely the set of maximal subsets of $E$ containing no member of $\mathcal{B}$. Hence the set $C^* = \{E-H : H \in \mathcal{H}\}$ is precisely the

set of minimal subsets of $E$ contained in no member of $\mathcal{B}^*$; i.e., $C^*$ is the set of circuits of $M^*$, also called the cocircuits of $M$. Likewise, the complements in $E$ of the circuits of $M$ are the hyperplanes of $M^*$.

(14) It follows from (13) that a set $C$ of subsets of $E$ are the circuits of a matroid if and only if $\mathcal{H} = \{E-C : C \in C\}$ satisfies the Strong Hyperplane Axioms (H1) and (H2)'. Applying straightforward set operations to the statements of (H1) and (H2)' we conclude that $C$ is the set of circuits of a matroid on $E$ if and only if the following Circuit Axioms are satisfied.

(C1) $C$ is a family of nonempty subsets of $E$ such that no member of $C$ is a proper subset of another.

(C2) For any two distinct members $C_1$ and $C_2$ of $C$, and for any $x \in C_1 \cap C_2$ and $y \in C_2 - C_1$, there is a $C \in C$ such that $y \in C \subseteq C_1 \cup C_2 - \{x\}$.

We have seen that a matroid may be characterized by its underlying set $E$ and any one of the following families of subsets of $E$: independent sets, bases, hyperplanes, and circuits. For our purposes, we shall find it most useful to characterize a matroid "geometrically" in terms of its hyperplanes, or, more generally, its flats.

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

(15) Theorem. Let $M$ be a rank $n$ matroid. For any $i$-flat $F^i$ and $k$-flat $F^k$ of $M$ such that $F^i \subsetneq F^k$, $0 \leq i < k \leq n$, $F^k - F^i$ 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 (7), $cl(J \cup \{x\}) = cl(F^i \cup \{x\})$. 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 $F^k - F^i$. ∎

Let $M$ be any matroid.

(16) 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 definition of closure (3), $F^0$ is a subset of every flat. Hence we may exclude all loops from M without essentially altering the set - relationships among the various flats.

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

(17) 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 (15) and the assumption that the 0-flat of M is null.

(18) 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 clearly 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 $cl(a \cup b)$.

# CHAPTER III

## MATROID DESIGNS

### 3.1 The geometry of flats in a matroid design

The geometric structure imposed on the flats of a matroid by (15) is not nearly as tight 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.

(19) A matroid $M$ is called equicardinal if all of its hyperplanes have the same cardinality, which we denote by $k(M)$. If, for every integer $j$, $0 \leq j \leq r(M)$, all of the $j$-flats of $M$ have the same cardinality $\alpha(j)$, then $M$ is called a matroid design. Like the finite geometries whose properties it generalizes, a matroid design exhibits strong regularities of structure in addition to the equicardinality of the flats of a given rank.

(20) Theorem. Let $M$ be a rank $n$ matroid design. For any integers $i,j,k$ such that $0 \leq i \leq j \leq k \leq n$, 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) $$t_M(i,i,k) = 1, \quad 0 \leq i \leq k \leq n,$$

and

$$t(0,1,i+1) > t(0,1,i), \quad 1 \leq i \leq n-1.$$

(T1) $$t_M(i,i+1,k) = \frac{t_M(0,1,k) - t_M(0,1,i)}{t_M(0,1,i+1) - t_M(0,1,i)}, \quad \text{for}$$

$$0 \leq i < k \leq n.$$

(T2) $$t_M(i,j,k) = \frac{t_M(i,\ell,k)\, t_M(\ell,j,k)}{t_M(i,\ell,j)}, \quad \text{for}$$

$$0 \leq i \leq \ell \leq j \leq k \leq n .$$

Proof. For given $i$ and $k$, $0 \leq i \leq k \leq n$, 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 $F^i \subsetneq F^{i+1}$, and hence, by (17), $F^{i+1}$ contains more points than does $F^i$.

(21) 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, $0 \leq k \leq n$. 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 (15) that the number of $(i+1)$-flats $F^{i+1}$ such that $F^i \subseteq F^{i+1} \subseteq F^k$ is $\dfrac{\alpha(k) - \alpha(i)}{\alpha(i+1) - \alpha(i)} = \dfrac{t_M(0,1,k) - t_M(0,1,i)}{t_M(0,1,i+1) - t_M(0,1,i)}$ 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 $F^i \subseteq F^{j_0+1} \subseteq F^k$.

(22) Every member of $V^{j_0}$ is contained in $t_M(j_0,j_0+1,k)$ members of $V^{j_0+1}$, by (21), 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 $|V^{j_0+1}| = \dfrac{t_M(i,j_0,k)\, t_M(j_0,j_0+1,k)}{t_M(i,j_0,j_0+1)}$, 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 (22). ∎

The function $t_M(i,j,k)$ of (20) is called the <u>t-function of M</u>.

(23) <u>Theorem</u>. The t-function $t_M(i,j,k)$ of a rank $n$ matroid design $M$ is uniquely determined by the values $t_M(0,1,k)$, $1 \leq k \leq n$, and the relations (T1) and (T2).

<u>Proof</u>. Let the values $t_M(0,1,k)$, $1 \leq k \leq n$, be given. $t_M(i,i+1,k)$ is then determined uniquely by (T1) for all $i$ and $k$, $0 \leq i < k \leq n$. Let us assume then, inductively, that

$t_M(i,j,k)$ is uniquely determined whenever $j-i \leq u$ for some integer $u$, where $u \geq 1$. Let $j-i = u+1$ for some $i$ and $j$ such that $0 \leq i+1 < j \leq n$. Then for any $k$, $j \leq k \leq n$, (T2) implies that $t_M(i,j,k) = \dfrac{t_M(i,i+1,k)\, t_M(i+1,j,k)}{t_M(i,i+1,j)}$. By the induction hypothesis, the three numbers on the right-hand side are uniquely determined; hence $t_M(i,j,k)$ is also. By induction, $t_M(i,j,k)$ is therefore uniquely determined for all $i,j,k$, $0 \leq i \leq j \leq k \leq n$. ∎

## 3.2. t-designs

(24) Matroid designs form a special class of structures called t-designs, which we shall now introduce. A t-design, or more specifically, a t - $(v,k,\lambda)$ design, $(V,\mathfrak{b})$, is a $v$-set $V$ and a set $\mathfrak{b}$ of $k$-subsets of $V$, $k < v$, called blocks, such that every $t$-subset of $V$, $t \geq 2$, is contained in exactly $\lambda$ blocks. We shall sometimes refer to any such pair $(V,\mathfrak{b})$ as a $D_t(v,k,\lambda)$.

(25) For any t - $(v,k,\lambda)$ design $(V,\mathfrak{b})$ and integer $i$, $0 \leq i \leq t$, we let $\lambda_i$ denote the number of blocks containing any fixed $i$-subset of $V$. Thus, $\lambda_t$ is identical with $\lambda$.

Now every i-subset $V_i$ of $V$ is contained in $\binom{v-i}{t-i}$ t-subsets of $V$, each of which is contained in $\lambda$ blocks; moreover, each of these blocks contains $\binom{k-i}{t-i}$ t-subsets that contain $V_i$. Thus $\lambda_i$ is well-defined, and

$$\lambda_i = \lambda\binom{v-i}{t-i} \Big/ \binom{k-i}{t-i} \text{ for } 0 \leq i \leq t. \tag{26}$$

In particular, $(V,\mathfrak{b})$ 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 $t,v,k,\lambda$, the numbers $\lambda_i$ given by (26) must be integers for a $t - (v,k,\lambda)$ design to exist.

Of particular interest are the 2-designs, also called balanced incomplete block designs (BIBD's). There is an extensive literature on BIBD's, and some of the standard results in the subject will be assumed in the sequel. (Proofs of the results used may be found in Hall [5 ].)

(27) A particularly useful result is the so-called Fisher inequality, which states that, if a $t - (v,k,\lambda)$ design exists, then the number of blocks, $\lambda_o$, is greater than or equal to the number of elements, v. Using (26), we may then state this condition as

$$\frac{\lambda\binom{v}{t}}{\binom{k}{t}} \geq v. \tag{28}$$

## 3.3. Consequences of Fisher's inequality for matroid designs

Let $M$ be a rank $n$ matroid design. 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 $F^i \subseteq F^j \subseteq F^k$.

(29) Theorem. For any matroid design $M$ and integers $i,j,k$ such that $2 \leq i+2 \leq j < k \leq r(M)$, and any $i$-flat $F^i$ and $k$-flat $F^k$ of $M$ such that $F^i \subseteq F^k$, the set

$$\mathfrak{b} = \{I_{i+1}(F^i,F^j): F^i \subseteq F^j \subseteq F^k \text{ and } F^j \text{ is a } j\text{-flat of } M\}$$

is the set of blocks of a BIBD on the set $V = I_{i+1}(F^i,F^k)$ with $\lambda = t_M(i+2,j,k)$.

Proof. For any member $I_{i+1}(F^i,F^j)$ of $\mathfrak{b}$, $F^i \subseteq F^j \subsetneq F^k$ 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 not contained in $I_{i+1}(F^i,F^j)$. Thus the members of $\mathfrak{b}$ 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 (15). 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 $(V,\mathfrak{b})$ is a BIBD with $\lambda = t_M(i+2,j,k)$. ∎

(30) In (29), the members of $\mathfrak{b}$ are in one-to-one correspondence with the $j$-flats $F^j$ such that $F^i \subseteq F^j \subseteq F^k$. Hence $|\mathfrak{b}| = t_M(i,j,k)$. Likewise, $|V| = t_M(i,i+1,k)$.

(31) Applying Fisher's inequality to the results of (29) and (30), we obtain, for any matroid design $M$

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

(32) A function $t(i,j,k)$ of integers $i,j,k$ such that $0 \leq i \leq j \leq k \leq n$ for some integer $n$ is said to be <u>T-consistent</u> if it is positive integer-valued and satisfies the relations (T0), (T1), (T2) of (15) and (T3) of (31). In particular, we have the following result.

(33) Theorem. The t-function of any matroid design is T-consistent.

Any T-consistent function that is actually the t-function of some matroid design will be called a realizable T-consistent function.

## 3.4. Further properties of matroids and matroid designs

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

(34) For any subset $E'$ of $E$, let $\mathcal{I}' = \{J \subseteq E' : J \in \mathcal{I}\}$. $M' = (E',\mathcal{I}')$ 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 $E'$.

(35) Theorem. If $F$ is a flat of a matroid $M = (E,\mathcal{I})$, then the flats of $M \times F$ are precisely the flats of $M$ contained in $F$.

Proof. Let $F'$ be a flat of $M' = M \times F$. Suppose that for some $x \in E - F'$ there is a circuit $C$ of $M$ such that $x \in C \subseteq F' \cup \{x\}$. Then $C \subseteq F \cup \{x\}$, so $F$ closed implies $C \subseteq F$. But then $C$ is a circuit of $M \times F$, so $C \subseteq F'$, contradicting the choice of $x$. Hence $F'$ is a flat of $M$. Conversely, any flat $F'$ of $M$ contained in $F$ is clearly closed in $M \times F$. ∎

(36) Let $E'$ be a subset of $E$, and let $\mathcal{J}' = \{J' \subseteq E' : J' \cup J \in \mathcal{J}$ for some M-basis $J$ of $E-E'\}$. It is easily verified that $(E',\mathcal{J}')$ satisfies (I1) and (I2), hence it is a matroid, called the contraction of $M$ to $E'$, and denoted by $M \cdot E'$. For any $A \subseteq E'$ and $M \cdot E'$ - basis $J'$ of $A$, there is an M-basis $J$ of $E-E'$ such that $J \cup J'$ is an M-basis of $(E-E') \cup A$. Hence the rank function, $r'$, of $M \cdot E'$ is given by

(37) $$r'(A) = r(A \cup (E-E')) - r(E-E'),$$

where $r$ is the rank function of $M$. In particular,

(38) $$r(M \cdot E') = r(M) - r(E-E').$$

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

(39) 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 (6). 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 (37), $r'(F) = j$ 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 $M$. ∎

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

Since the set $\mathcal{F}$ of flats of a matroid M includes E and is closed under intersections, $\mathcal{F}$ may be viewed as a lattice, ordered by inclusion. Such a lattice is called a <u>matroid lattice</u>, or <u>geometric lattice</u> [2].

(41) By (35) and (39) 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.

(42) <u>Theorem.</u> If M is a rank n matroid design with t-function $t_M(i,j,k)$, and $F^h \subseteq F^\ell$ are an h-flat and $\ell$-flat of M respectively, then $M(F^h,F^\ell)$ is a rank $\ell$-h matroid design with t-function

$$t(i,j,k) = t_M(i+h,j+h,k+h),\ 0 \leq i \leq j \leq k \leq \ell-h.$$

(43) For any integer $\ell$, $0 \leq \ell \leq r(M)$, let $\mathcal{J}' = \{J \subseteq E : J \in \mathcal{J}$ and $|J| \leq \ell\}$. Clearly, $M' = (E,\mathcal{J}')$ is a matroid having rank function $r'(A) = \min(\ell, r(A))$. M' is called the <u>$\ell$-truncation of M</u>, and denoted by $M^{(\ell)}$. The flats of $M^{(\ell)}$ are the

flats of $M$ having rank at most $\ell-1$, and $E$. If $M$ is a matroid design having t-function $t_M(i,j,k)$, then $M^{(\ell)}$ is a rank $\ell$ matroid design having t-function

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

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

and

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

(44) 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.

(45) Let $M = (E,\mathcal{H})$ be any matroid, and $\alpha$ a positive integer. For each element $x \in E$ choose a set $S_x$ of $\alpha$ 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 $\mathcal{H}' = \{ \bigcup_{x \in H} S_x : H \in \mathcal{H} \}$. Clearly, $M' = (E', \mathcal{H}')$ satisfies (H1) and (H2), hence $M'$ is a matroid. $M'$ is said to be an $\alpha$-inflation of $M$, and $M$ is an $\alpha$-deflation of $M'$. It follows from (11) that $F'$ is a flat of $M'$ if and only if

$F' = \bigcup_{e \in F} S_e$ for some flat $F$ of $M$. This relation establishes a one-to-one correspondence between the flats of $M$ and $M'$ that preserves inclusion.

(46) It is also apparent from the above construction that for any matroid $M$ and positive integer $\alpha$, an $\alpha$-inflation of $M$ always exists, whereas an $\alpha$-deflation of $M$ exists if and only if every point of $M$ has a cardinality divisible by $\alpha$.

(47) From (45) and (46) it follows that if $M$ is a matroid design whose points have cardinality $\alpha$, then there exists an $\alpha$-deflation $M'$ of $M$ such that $M'$ is simple, and the lattices of $M$ and $M'$ are isomorphic. In particular, $M$ is a matroid design 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 matroid designs. This stands in marked contrast to the case of general equicardinal matroids where non-simple points play a crucial role (see Chapter IV).

(48) A <u>separator</u> of a matroid $M = (E, \mathcal{J})$ is a subset $S$

of $E$ such that for any circuit $C$ of $M$, $C \subseteq S$ or $C \subseteq E-S$.

A separator of a matroid may also be specified in terms of the hyperplanes as follows.

(49) Theorem. $S$ is a separator of a matroid $M = (E,\mathcal{H})$ if and only if for every $H \in \mathcal{H}$, $S \subseteq H$ or $E-S \subseteq H$.

Proof. Let $S$ be a separator of $M$, and suppose that for some hyperplane $H$ of $M$, $S-H \neq \emptyset$ and $E-(S \cup H) \neq \emptyset$. Let $x \in S-H$, $y \in E-(S \cup H)$, and let $J$ be any basis of $H$, $|J| = r(M)-1$. $J \cup \{x\}$ and $J \cup \{y\}$ are both independent, since $H$ is closed. However, $J \cup \{x,y\}$ must be dependent, because $|J \cup \{x,y\}| > r(M)$. Thus $J \cup \{x,y\}$ contains a circuit $C$, which is contained in neither $J \cup \{x\}$ nor $J \cup \{y\}$. Hence $C$ contains both $x$ and $y$, so $C \not\subseteq S$ and $C \not\subseteq E-S$, contradicting the assumption that $S$ is a separator.

Conversely, suppose that $S$ is not a separator of $M$, and let $C$ be a circuit meeting both $S$ and $E-S$. Say $x \in C \cap S$, and $y \in C \cap (E-S)$. Let $B$ be a basis of $M$ containing the independent set $C-\{x\}$, and let $E' = B \cup \{x\}$. Clearly $r(E') = |B| = r(M)$. Now $C-\{y\}$ is an independent subset of $E'$ and hence $C-\{y\}$ is contained in a basis $B'$ of $E'$,

where $|B'| = |B| = |E'| - 1$. Since $B'$ is independent, $y \notin B'$, and so $B' = E' - \{y\}$. Thus both $B = E' - \{x\}$ and $B' = E' - \{y\}$ are bases of $M$, and hence $H = cl(E' - \{x,y\})$ is a hyperplane that contains neither $x$ nor $y$; that is, $H$ contains neither $S$ nor $E-S$, and hence $S$ is not a separator of $M$. ∎

(50) Corollary. The separators of $M$ and $M^*$ are identical.

Proof. Since the circuits of $M^*$ are the complements in $E$ of the hyperplanes of $M$, it follows at once from (49) that $S$ is a separator of $M$ if and only if $C^* \subseteq S$ or $C^* \subseteq E-S$ for every circuit $C^*$ of $M^*$, that is, if and only if $S$ is a separator of $M^*$. ∎

As we shall usually present a matroid in terms of its hyperplanes, we shall also use (49) to identify its separators.

(51) It follows easily from (49) that, for any matroid $M = (E,\mathcal{H})$, the intersection of any two separators is a separator, and the complement of a separator is a separator. Therefore the minimal nonempty separators of $M$ partition $E$. Where $S$ is such a separator, $M \cdot S$ is called a component of $M$. $M$ is called connected, or inseparable, if

$M$ is its sole component. Any matroid $M$ is determined by its components, for if $M_i = (S_i, \mathcal{H}_i)$, $i = 1, \cdots t$, are the components of $M$, then by (39) the hyperplanes of $M$ are precisely the sets of form $H \cup \bigcup_{\substack{i=1 \\ i \neq k}}^{t} S_i$ where $H \in \mathcal{H}_k$.

The following result is also an immediate consequence of (39).

(52) Theorem. Every component of an equicardinal matroid (matroid design) is an equicardinal matroid (matroid design).

A matroid is said to be totally disconnected if it contains no circuits.

(53) Theorem. If a simple matroid design is disconnected, then it is totally disconnected.

Proof. Let $M$ be a disconnected, simple matroid design with components $M_i = (E_i, \mathcal{H}_i)$, $i = 1, \cdots, t$, $t \geq 2$. Let $C$ be a circuit of $M$ having minimum cardinality, say $|C| = \gamma$. $\gamma \geq 3$ because $M$ is simple and contains no loops. We may also suppose without loss of generality that $C \subseteq E_1$. Since $C$ is a minimal dependent set, $r(C) = \gamma - 1$, so $cl(C)$ is a $(\gamma-1)$-flat and $|cl(C)| \geq \gamma \geq 3$.

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 $z \in E_2$,

since no circuit of M meets both $E_1$ and $E_2$ 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}) U{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 $\gamma-1$.

Hence I and $cl(C)$ are two $(\gamma-1)$-flats having distinct cardinalities, contrary to the definition of matroid design. Hence M contains no circuits; that is, M is totally disconnected. ∎

In the next three sections we will present several classes of matroid designs.

## 3.5 Trivioids

(54) For any integers v and k such that $v > k \geq 0$, there exists a matroid design 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 $\alpha$ is a positive in-

teger, any $\alpha$-inflation $M(\alpha)$ of such an $M$ is called an $(\alpha,k,v)$-trivioid, denoted by $\sigma(\alpha,k,v)$, and $M(\alpha)$ is said to be a trivial equicardinal matroid. The hyperplanes of $M(\alpha)$ are precisely the subsets of $E$ that are unions of any $k$ distinct points.

In Chapter IV we shall show that for certain values of $\gamma$, every equicardinal matroid with cocircuit cardinality $\gamma$ is trivial.

## 3.6 t-designs as examples of matroid designs

A second class of matroid designs comes from the t-designs.

(55) Theorem. For any integer $t \geq 2$, $M$ is a $t-(v,k,1)$ design such that $k < v$ if and only if $M$ is a simple rank $t+1$ matroid design such that

(56) $$t_M(0,1,j) = j, \quad \text{for } 0 \leq j \leq t-1,$$
$$t_M(0,1,t) = k,$$
$$t_M(0,1,t+1) = v.$$

Proof. Let $t \geq 2$, and let $M = (E,\mathcal{H})$ be a $t-(v,k,1)$ design such that $k < v$. First we shall show that $(E,\mathcal{H})$ satisfies (H1) and (H2). Since $k < v$, the members of $\mathcal{H}$ are proper subsets of $E$. Further, no member of $\mathcal{H}$ is pro-

perly 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 $\mathcal{H}$. By (8), 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 $H \subsetneq E$, 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, $0 \leq j \leq t-1$, is simple. In particular, since $t \geq 2$, M is simple. The expression (56) for the t-function of M follows immediately.

Suppose, conversely, that $t \geq 2$ and M is a simple rank t+1 matroid design with t-function satisfying (56). Then, for $0 \leq j \leq t-1$, every j-flat of M is simple, and hence every t-subset of E must be independent in M. Thus, every t-subset T of E is contained in a unique member of $\mathcal{H}$, namely $cl(T)$, and M is a $t-(v,k,1)$ design. ∎

(57) As a special case of (55), it follows that every BIBD with $\lambda = 1$ is a rank 3 matroid design. Many such BIBD's are known. (See, for example, Hall [5 ].)

In analogy with matroid designs, we say that a $t - (v,k,\lambda)$ design $(E,\mathcal{B})$ is <u>trivial</u>, if $\mathcal{B}$ consists of all k-subsets of E.

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

(58) For any prime power q and integer $f \geq 1$, 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 $Q = \{\frac{ax^{q^i}+b}{cx^{q^i}+d} : a,b,c,d \in GF(q^f),\ ad-bc \neq 0,\ 0 \leq i \leq f\}$ 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 $3 - (q^2+1,\ q+1,\ 1)$ of this type is called an <u>inversive plane of order q</u>, abbreviated by IP(q). An IP(q) has the property that its contraction at any point is an EG(2,q). (For a more detailed treatment of inversive planes, the reader is referred to [8 ] and [10].)

(59) 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 $4 \pmod 6$.

(60) The only other $t - (v,k,1)$ designs known for $t \geq 3$ are due to Witt [19]. 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 $M_{24}$.

## 3.7 Finite projective and affine geometries as examples of matroid designs

(61) Perhaps the most natural examples of matroid designs are the finite projective and affine geometries. A finite projective geometry $(E,\mathcal{L})$ is a finite set $E$ of elements (called points) and a set $\mathcal{L}$ of subsets of $E$ called lines satisfying the following three axioms [15].

(PG1) There is one and only one line containing any two distinct points.

(PG2) If $a,b,c,d$ are distinct points and the lines containing $\{a,b\}$ and $\{c,d\}$ contain a common point, then the lines containing $\{a,c\}$ and $\{b,d\}$ contain a common point.

(PG3) Every line contains at least three points.

We shall present some basic and well-known facts about finite projective geometries. (For further details, the reader is referred to [15].)

Let $(E,\mathcal{L})$ be a fixed finite projective geometry.

(62) Every line contains the same number, $s+1$, of points. $s$ is called the order of $(E,\mathcal{L})$. Note that (PG3) implies that $s \geq 2$.

A subset $A$ of $E$ is said to be a line-closed set or subspace of $(E,\mathcal{L})$ if, for any distinct points $x,y \in A$, the line $L_{xy}$ containing $x$ and $y$ is contained in $A$. For any point $x$ and subset $A$ of $E$, we let $L(x,A)$ denote the union of all lines that contain $x$ and meet $A$.

(63) $\emptyset$ is line-closed, and for every $x \in E$, $\{x\}$ is line-closed. Let $A \subseteq E$ such that $|A| \geq 2$. Then, using (PG2), it may be shown that $A$ is line-closed if and only if $A = L(x,A')$ for some line-closed set $A'$ and $x \in A - A'$.

(64) By (PG1) and (62), it follows that $|L(x,A)| = |A| + (s-1)|A| + 1$ for any subset $A$ of $E$. Using (63), it is then easy to prove by induction that every line-closed set $A \subseteq E$ has cardinality $\frac{s^h-1}{s-1}$ for some integer $h$. $(h-1)$ is called the dimension of $A$, $d(A)$. The dimension of $(E,\mathcal{L})$ is $d(E)$. For any proper subspace $A$ of $E$ and $x \in E-A$, $d(L(x,A)) = d(A) + 1$. We also note that, by the above defini-

tion, $d(\emptyset) = -1$.

For short, we refer to any finite projective geometry of dimension $n$ and order $s$ as a PG(n,s). The $(n-1)$-dimensional subspaces of a PG(n,s) will be called its hyperspaces.

(65) Lemma. Let $(E,\mathcal{L})$ be a PG(n,s). For any nonempty subspace $F$ and hyperspace $H$ of $(E,\mathcal{L})$ not containing $F$, $d(F\cap H) = d(F) - 1$.

Proof. Let $F$ be a nonempty subspace of $(E,\mathcal{L})$ and $H$ a hyperspace not containing $F$. For any $x \in F-H$, $d(L(x,H)) = d(H) + 1 = n$, by (64); hence $L(x,H) = E$. Since $F$ is line-closed, $F \cap L(x,H) = L(x,F\cap H)$, and therefore $F = L(x, F\cap H)$. The lemma now follows from (64). ∎

(66) Theorem. Let $(E,\mathcal{L})$ be a PG(n,s), and let $\mathcal{H}$ be the collection of hyperspaces of $(E,\mathcal{L})$. Then $M = (E,\mathcal{H})$ is a rank $n+1$ matroid design whose h-flats are precisely the $(h-1)$-dimensional subspaces of $(E,\mathcal{L})$, and the t-function of $M$ is given by $t_M(0,1,h) = \frac{s^h-1}{s-1}$, $1 \leq h \leq n+1$.

Proof. By definition, the members of $\mathcal{H}$ all have cardinality $\frac{s^n-1}{s-1}$, and $|E| = \frac{s^{n+1}-1}{s-1}$. Hence every member of $\mathcal{H}$ is a proper subset of $E$, and no member of $\mathcal{H}$ is properly contained in another. Thus (H1) holds for $(E,\mathcal{H})$.

(67) Now let $H_1$ and $H_2$ be any two distinct members of $\mathcal{H}$. By (65), $d(H_1 \cap H_2) = n-2$; hence, for any $x \in E - H_1 \cap H_2$, $L(x, H_1 \cap H_2) \in \mathcal{H}$. If $x \in H_1 \cap H_2$, then $\{x\} \cup (H_1 \cap H_2) \subseteq H_1 \in \mathcal{H}$. Thus, for any $x \in E$, there is a member of $\mathcal{H}$ containing $\{x\} \cup (H_1 \cap H_2)$, so (H2) holds for $(E,\mathcal{H})$.

(68) Therefore $(E,\mathcal{H})$ is a matroid with hyperplane family $\mathcal{H}$.

(69) We shall now show that every proper subspace of $(E,\mathcal{L})$ is an intersection of members of $\mathcal{H}$, and hence is a flat of M. This obviously holds for every member of $\mathcal{H}$. For any $(n-2)$-dimensional subspace $S^{n-2}$ of $(E,\mathcal{L})$, let $x \in E - S^{n-2}$ and let $y \in E - L(x,S^{n-2})$. By (64), $H_x = L(x,S^{n-2}) \in \mathcal{H}$ and $H_y = L(y,S^{n-2}) \in \mathcal{H}$, and $S^{n-2} \subseteq H_x \cap H_y$ by construction. Since $H_x \cap H_y$ is also a subspace of $(E,\mathcal{L})$, we must have $S^{n-2} = H_x \cap H_y$. Likewise, it may be shown that any j-dimensional subspace $S^j$, $0 \leq j \leq n-2$, can be written as the intersection of two $(j+1)$-dimensional subspaces. Therefore, by induction on $n-j$, every proper subspace of $(E,\mathcal{L})$ is an intersection of members of $\mathcal{H}$, and hence is a flat of M.

(70) By (69), the members of $\mathfrak{L}$ are flats of $M$, and it is clear that they are precisely the 2-flats of $M$. Hence, if $F$ is a flat of $M$ and $L \in \mathfrak{L}$ such that $|L \cap F| \geq 2$, then $L \cap F$ is a 2-flat contained in $L$, so $L \cap F = L$ and $L \subseteq F$. Therefore every flat of $M$ is line-closed.

(71) From (69) and (70) it follows that the subspaces of $(E,\mathfrak{L})$ are precisely the flats of $M$.

(72) It follows easily from (63) and (64) that, for any subspaces $F' \subseteq F''$, $d(F'') = d(F') + 1$ if and only if there are no subspaces $F$ such that $F' \subsetneq F \subsetneq F''$. Therefore, by (71), $r(F'') = r(F') + 1$ for flats $F' \subseteq F''$ of $M$ if and only if $d(F'') = d(F') + 1$. Since for every flat $F$ of a matroid there is a nested chain of flats $\emptyset = F_0 \subset F_1 \subset \ldots \subset F_k = F$ such that $r(F_{i+1}) = r(F_i) + 1$, $0 \leq i \leq k-1$, and since $r(\emptyset) = 0 = d(\emptyset) + 1$, it follows that $r(F) = d(F) + 1$ for every flat (subspace) $F$ of $M$. In particular, $r(M) = r(E) = n+1$.

By (68) and (72), $M$ is a rank $n+1$ matroid whose $h$-flats are the $(h-1)$-dimensional subspaces of $(E,\mathfrak{L})$, and, hence, the t-function of $M$ is given by $t_M(0,1,h) = \frac{s^h - 1}{s-1}$, $1 \leq h \leq n+1$. ∎

In view of (66), we say that a matroid $M = (E,\mathcal{H})$ is a $PG(n,s)$ if $(E,\mathfrak{L})$ is a $PG(n,s)$, where $\mathfrak{L}$ is the family of lines of $M$, and $\mathcal{H}$ is the family of hyperspaces of $(E,\mathfrak{L})$.

(73) It may be proved [5 ] that, for $n \geq 3$, PG(n,s) exists if and only if s is a prime power, and in this case PG(n,s) is essentially unique. A PG(2,s) also exists for every prime power s (although it is not necessarily unique), but it is not known whether s must be a prime power for a PG(2,s) to exist. However, the well-known Bruck-Ryser theorem does give certain necessary conditions on the order of a PG(2,s).

(74) Theorem. (Bruck-Ryser) A necessary condition for the existence of a PG(2,s) is that, for $s \equiv 1,2 \pmod 4$, integers x and y exist such that $s = x^2 + y^2$.

(For a proof of this theorem and related results, see [5 ].)

(75) Where q is a prime power and $n \geq 2$, we may construct a PG(n,q) as follows. Let GF(q) be a finite field of order q, let E' be the set of all non-zero (n+1)-tuples with elements from GF(q), and let J' be the set of all linearly independent subsets of E'. M' = (E',J') is then a rank n+1 matroid design, and every j-flat of M' has cardinality $q^j-1$, for $0 \leq j \leq n+1$. In particular, the points of M' all have cardinality q-1. Any (q-1)-deflation M of M' is then a simple, rank n+1 matroid design whose lines satisfy (PG1) - (PG3), and whose flats are precisely the line-closed subsets of E. Thus, M is a PG(n,q).

(76) For any PG(n,s) $M = (E,\mathcal{H})$, a matroid of form $M' = M \times (E - H_o)$, where $H_o$ is a hyperplane of M, is called an an <u>affine geometry of dimension n and order s</u>, abbreviated by <u>EG(n,s)</u>. If F' is any j-flat of M', $0 \leq j \leq n+1$, then $F = cl_M(F')$ is a j-flat of M, and $F-F' \subseteq H_o$; hence $F' = F-H_o$. Since $F \not\subseteq H_o$, $d(F \cap H_o) = d(F)-1$, so $|F'| = \frac{s^j-1}{s-1} - \frac{s^{j-1}-1}{s-1} = s^{j-1}$. Conversely, for any j-flat F of M, where $F \not\subseteq H_o$, $F' = F-H_o$ is a flat of M' and $|F'| = s^{j-1}$, so F' is a j-flat of M'. Hence M' is a rank n+1 matroid design such that $t_{M'}(0,1,j) = s^{j-1}$, and F' is a j-flat of M' if and only if $F' = F-H_o$ for a j-flat F of M. For any (n-2)-flat F contained in $H_o$, $\mathcal{H}'_F = \{H-F : H \in \mathcal{H}-\{H_o\},\ F \subseteq H\}$ is a collection of hyperplanes that partitions $E-H_o$, and is called a <u>parallel class</u> of M'. Evidently the hyperplanes of M' may be partitioned into $t_{M'}(0,n-2,n-1) = \frac{s^{n-1}-1}{s-1}$ parallel classes, one for each (n-2)-flat in $H_o$.

(77) The results of (65) and (76) show that, for any finite affine or projective geometry M of rank n, any two hyperplanes of M are either disjoint, or they intersect in an (n-2)-flat. In other words, every two distinct intersecting hyperplanes intersect on the same number of elements. This additional regularity condition on the intersection of hyperplanes does not hold for most matroid designs. (For instance, it does not hold for most trivioids.) In fact, this

condition is essentially the characteristic that distinguishes affine and projective geometries from general matroid designs, as the following rephrased theorem of W. Kantor shows.

(78) Theorem. (Kantor [11]) If $M$ is a simple, connected, equicardinal matroid such that $r(M) \geq 5$ and, for some integer $\mu$, every two hyperplanes of $M$ are either disjoint or intersect in $\mu$ points, then $M$ is either a finite affine geometry or a finite projective geometry.

The theorem fails if $r(M) \leq 4$. However, the only known case in which it fails for $r(M) = 4$ is for a 3-(22,6,1) design discovered by Witt [19]. This design has the property that every two blocks are either disjoint, or intersect in exactly two points.

3.8. d-sequences and D-consistency.

The relations (T0)-(T3) impose strong restrictions on the possible parameters for a matroid design. However, when the values $t(0,1,j)$ are given, $0 \leq j \leq n$, it is often quite awkward to verify directly whether the function $t(i,j,k)$ so defined is T-consistent. We shall define an auxiliary set of parameters for a matroid design that is considerably easier to handle, and contains all the information of the associated t-function.

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

(79) $\quad d_i = t_M(0,1,i) - t_M(0,1,i-1)$, $1 \le i \le n$,

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 $M$.

(80) Theorem. Let $t(i,j,k)$ be a positive, integer-valued, T-consistent function on integers $i,j,k$, where $0 \le i \le j \le k \le n$. Let $d_i = t(0,1,i) - t(0,1,i-1)$ for each $i$, $1 \le i \le n$. Then

$$(81)\quad t(i,j,k) = \frac{\prod_{\ell=i+1}^{j} \sum_{m=\ell}^{k} d_m}{\prod_{\ell=i+1}^{j} \sum_{m=\ell}^{j} d_m}, \quad \text{for } 0 \le i \le j \le k \le n,$$

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

Proof. For given $i$, $0 \le i \le n$, the proof of (81) is by induction on the set $S = \{(k,j): i \le j \le k \le n\}$, ordered lexicographically. For $k = j = i$, the products are empty and so $t(i,j,k) = 1$, which agrees with (T0) of (20).

Assume now that (81) holds for all pairs $(k,j) \in S$ such that $(k,j) \le (w,u)$ 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 (81) holds for $i = i$, $j = i$, $k = u+1$. 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 (81) for $(k,j) = (w,u+1)$. Now

$$t(i,u+1,w) = \frac{t(i,u,w)\ t(u,u+1,w)}{t(i,u,u+1)}, \quad \text{by (T2)},$$

$$= \frac{t(i,u,w)}{t(i,u,u+1)} \cdot \frac{t(0,1,w)-t(0,1,u)}{t(0,1,u+1)-t(0,1,u)} \quad , \text{ by (T1)},$$

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

using the defining relation for the $d_i$'s. But

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

and

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

both by the induction hypothesis. Substituting the last two expressions into (82) and simplifying, we obtain

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

$$= \frac{\prod_{\ell=i+1}^{u+1} \sum_{m=\ell}^{w} d_m}{\prod_{\ell=i+1}^{u+1} \sum_{m=\ell}^{u+1} d_m},$$

which is (81) 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 <u>D-consistent</u> if $d_1 = 1$ and the associated function $t(i,j,k)$ given by (81) is T-consistent.

(83) <u>Theorem</u>. A sequence $D = (d_n,d_{n-1},\ldots,d_1)$ is D-consistent if and only if

(D0) $d_1 = 1$ and $d_i \geq 1$, $1 \leq i \leq n$.

(D1) $\dfrac{\prod_{\ell=i+1}^{j} \sum_{m=\ell}^{k} d_m}{\prod_{\ell=i+1}^{j} \sum_{m=\ell}^{j} d_m}$ is integral for $0 \leq i \leq j \leq k \leq n$.

(D2) $d_{i-1} | d_i$, $2 \leq i \leq n$, and $\dfrac{d_{i+1}}{d_i} \geq \dfrac{d_i}{d_{i-1}}$, $2 \leq i \leq n-1$.

<u>Proof</u>. Let $D$ be D-consistent, i.e., let $t(i,j,k)$ as defined

by (81) be positive integer-valued and T-consistent, and let $d_1 = 1$. By (81),

$$t(0,1,i) = \sum_{m=1}^{i} d_m, \quad 1 \leq i \leq n,$$

(84) hence $d_i = t(0,1,i) - t(0,1,i-1)$, $1 \leq i \leq n$,

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

Since $t(0,1,i) > t(0,1,i-1)$ by (T0), $d_i \geq 1$ for all $i$, so (D0) is satisfied.

(D1) follows at once from the expression (81) for $t(i,j,k)$ and the assumption that $t(i,j,k)$ is T-consistent (see (32)), hence integer-valued.

To prove (D2), we note that, for $1 \leq i \leq n-1$,

(85)
$$\frac{d_{i+1}}{d_i} = \frac{t(0,1,i+1) - t(0,1,i)}{t(0,1,i) - t(0,1,i-1)}, \quad \text{by (84)},$$

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

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

(86) Likewise, $\dfrac{d_i}{d_{i-1}} = t(i-2,i-1,i) - 1$ for $2 \leq i \leq n$.

(87) In particular, $d_{i-1} | d_i$ for $2 \leq i \leq n$.

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) of (31), $t(i-2,i,i+1) \geq t(i-2,i-1,i+1)$. Hence

(88) $$t(i-1,i,i+1) \geq t(i-2,i-1,i),$$

because $t(i,j,k)$ is everywhere positive. Substituting (85) and (86) in (88), we find that $\frac{d_{i+1}}{d_i} \geq \frac{d_i}{d_{i-1}}$, $2 \leq i \leq n-1$. Combined with (87), this establishes (D2).

Conversely, let $D$ satisfy (D0), (D1), and (D2); we shall show that the function $t(i,j,k)$ given by (81) is T-consistent.

$t(i,i,k) = 1$ because the products on the right side of (81) are empty when $j = i$. We also have

(89) $$t(0,1,i) = \sum_{m=1}^{i} d_m/d_1 = \sum_{m=1}^{i} d_m, \quad 1 \leq i \leq n.$$

Since $d_i \geq 1$, it follows that $t(0,1,i) > t(0,1,i-1)$ for $2 \leq i \leq n$. Hence $t(i,j,k)$ satisfies (T0).

Using (89) we can write

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

By (81) $$\frac{\sum_{m=i+1}^{k} d_m}{d_{i+1}} = t(i,i+1,k),$$

and (T1) follows.

To prove (T2), we apply (81) to obtain, for integers $0 \le i \le h \le j \le k \le n$,

$$\frac{t(i,h,k)t(h,j,k)}{t(i,h,j)} = \frac{\left(\dfrac{\prod_{\ell=i+1}^{h}\sum_{m=\ell}^{k} d_m}{\prod_{\ell=i+1}^{h}\sum_{m=\ell}^{h} d_m}\right)\cdot\left(\dfrac{\prod_{\ell=h+1}^{j}\sum_{m=\ell}^{k} d_m}{\prod_{\ell=h+1}^{j}\sum_{m=\ell}^{j} d_m}\right)}{\left(\dfrac{\prod_{\ell=i+1}^{h}\sum_{m=\ell}^{j} d_m}{\prod_{\ell=i+1}^{h}\sum_{m=\ell}^{j} d_m}\right)}$$

$$= \frac{\left(\prod_{\ell=i+1}^{h}\sum_{m=\ell}^{k} d_m\right)\left(\prod_{\ell=h+1}^{j}\sum_{m=\ell}^{k} d_m\right)}{\left(\prod_{\ell=i+1}^{h}\sum_{m=\ell}^{j} d_m\right)\left(\prod_{\ell=h+1}^{j}\sum_{m=\ell}^{j} d_m\right)}$$

$$= \frac{\prod_{\ell=i+1}^{j}\sum_{m=\ell}^{k} d_m}{\prod_{\ell=i+1}^{j}\sum_{m=\ell}^{j} d_m}$$

$$= t(i,j,k) .$$

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

$$t(i,j,k) = \frac{\prod_{\ell=i+1}^{j}\sum_{m=\ell}^{k} d_m}{\prod_{\ell=i+1}^{j}\sum_{m=\ell}^{j} d_m}$$

$$(90) \qquad = \frac{\left(\sum_{m=i+1}^{k} d_m\right)}{d_j} \cdot \prod_{\ell=i+2}^{j} \left( \frac{\sum_{m=\ell}^{k} d_m}{\sum_{m=\ell-1}^{j} d_m} \right)$$

(91) By (D2), $d_m \geq d_{m-1} \frac{d_\ell}{d_{\ell-1}}$ for $m \geq \ell$.

Substituting (91) in (90) we obtain

$$(92) \qquad t(i,j,k) \geq \frac{\sum_{m=i+1}^{k} d_m}{d_j} \cdot \prod_{\ell=i+2}^{j} \frac{\left(\frac{d_\ell}{d_{\ell-1}}\right) \sum_{m=\ell}^{k} d_{m-1}}{\sum_{m=\ell-1}^{j} d_m}$$

$$= \frac{\sum_{m=i+1}^{k} d_m}{d_j} \cdot \prod_{\ell=i+2}^{j} \left(\frac{d_\ell}{d_{\ell-1}}\right) \prod_{\ell=i+2}^{j} \frac{\sum_{m=\ell-1}^{k-1} d_m}{\sum_{m=\ell-1}^{j} d_m} \quad .$$

(93) Since $j \geq i+2$, $\prod_{\ell=i+2}^{j} \frac{d_\ell}{d_{\ell-1}} = \frac{d_j}{d_{i+1}}$ ,

(94) and since $k > j$, $\prod_{\ell=i+2}^{j} \left( \frac{\sum_{m=\ell-1}^{k-1} d_m}{\sum_{m=\ell-1}^{j} d_m} \right) \geq 1$ .

From (92), (93), and (94) it follows that

$$t(i,j,k) \geq \frac{\sum_{m=i+1}^{k} d_m}{d_j} \quad .$$

By (81), $\frac{\sum_{m=i+1}^{k} d_m}{d_j} = t(i,i+1,k)$, and thus $t(i,j,k) \geq t(i,i+1,k)$, which is (T3). ∎

(95) Corollary. For any matroid design $M$, $d(M)$ satisfies (D0), (D1), and (D2), and $t_M(i,j,k)$ is given in terms of $d(M)$ by (81).

## 3.9. Unimodality in matroid designs

We shall use the relations (D0), (D1), and (D2) to prove an interesting arithmetic property of matroid designs.

(96) A function $f: \mathbb{R} \to \mathbb{R}$ is said to be unimodal if, whenever $f(x) < f(w)$ for some $x > w$, then $f(z) \leq f(y)$ for all $z \geq y \geq x$.

The following result is conjectured to be true for an arbitrary matroid.

(97) Theorem. For any matroid design $M$, the number of $i$-flats of $M$ is a unimodal function of $i$, $0 \leq i \leq r(M)$.

Proof. Let $r(M) = n$, and let $d(M) = (d_n, d_{n-1}, \cdots, d_1)$. Then $t_M(i,j,k)$, $0 \leq i \leq j \leq k \leq n$, is given by (81). We shall show that $t(0,i,n)$ is a unimodal function of $i$.

For each $i$, $0 \leq i \leq n-1$, let

$$A(i) = \frac{\sum_{m=i+1}^{n} d_m}{\sum_{m=1}^{i+1} d_m} .$$

(98) By (81) $$t(0,i+1,n) = \frac{\prod_{\ell=1}^{i+1} \sum_{m=\ell}^{n} d_m}{\prod_{\ell=1}^{i+1} \sum_{m=\ell}^{i+1} d_m}.$$

$$= \frac{\prod_{\ell=1}^{i} \sum_{m=\ell}^{n} d_m}{\prod_{\ell=2}^{i+1} \sum_{m=\ell}^{i+1} d_m} \cdot A(i).$$

Noting that $\prod_{\ell=1}^{i} \sum_{m=\ell}^{i} d_m = \prod_{\ell=2}^{i+1} \sum_{m=\ell}^{i+1} d_{m-1}$, we may rewrite (98) as follows:

(99) $$t(0,i+1,n) = \frac{\prod_{\ell=1}^{i} \sum_{m=\ell}^{n} d_m}{\prod_{\ell=1}^{i} \sum_{m=\ell}^{i} d_m} \cdot A(i) \prod_{\ell=2}^{i+1} \frac{\sum_{m=\ell}^{i+1} d_{m-1}}{\sum_{m=\ell}^{i+1} d_m}.$$

Using (81), (99) becomes

(100) $$t(0,i+1,n) = t(0,i,n)\, A(i) \prod_{\ell=2}^{i+1} \frac{\sum_{m=\ell}^{i+1} d_{m-1}}{\sum_{m=\ell}^{i+1} d_m}.$$

(101) By (DO),

$$A(i) = \frac{\sum_{m=i+1}^{n} d_m}{\sum_{m=1}^{i+1} d_m}$$ is decreasing as $i$ increases,

and $A(i) > 0$ for all $i$, $0 \leq i \leq n-1$.

(102) By (D2), $B_{i,\ell} = \dfrac{\sum_{m=\ell}^{i+1} d_{m-1}}{\sum_{m=\ell}^{i+1} d_m}$ is nonincreasing as $i$ increases, and $0 < B_{i,\ell} \leq 1$ for all $i$, $\ell$, $2 \leq \ell \leq i+1$.

(103) Let $C(i) = A(i) \prod_{\ell=2}^{i+1} B_{i,\ell}$. By (101) and (102), $C(i)$ decreases as $i$ increases, and $C(i) > 0$, $0 \leq i \leq n-1$.

(104) Applying induction to (100) we find that $t(0,i,n) = \prod_{j=0}^{i-1} C(j)$, and hence (103) implies that $t(0,i,n)$ is unimodal in $i$. ∎

## 3.10. Characterization of matroid designs by d-sequences

We shall now compute the d-sequences for some of the matroid designs discussed earlier.

Let $M$ be a rank $n$ matroid design with d-sequence $d(M) = (d_n, d_{n-1}, \cdots, d_1)$, and t-function $t_M(i,j,k)$, $0 \leq i \leq j \leq k \leq n$.

(105) From paragraph (45) it follows that an $\alpha$-inflation or $\alpha$-deflation of $M$ has the same d-sequence as $M$.

(106) 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 $t(i,j,k) = t_M(i+p,j+p,k+p)$, $0 \leq i \leq j \leq k \leq q-p$, by (42).

Hence, for $1 \leq k \leq q-p$,

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

$$= \frac{\sum_{m=p+1}^{k+p} d_m}{d_{p+1}} - \frac{\sum_{m=p+1}^{k+p-1} d_m}{d_{p+1}}, \quad \text{by (81)},$$

$$= \frac{d_{k+p}}{d_{p+1}} .$$

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

(107) For any integer $h$, $1 \leq h \leq n$, the d-sequence of $M^{(h)}$ (the h-truncation of $M$) is clearly $\left(\sum_{j=h}^{n} d_j, d_{h-1}, \cdots, d_1\right)$.

(108) We note that, if $D = (d_n, d_{n-1}, \cdots, d_1)$ is D-consistent and $d_j = 1$ for some $d_j$, then $d_j = d_{j-1} = \cdots = d_1 = 1$.

Indeed, for $1 \leq i \leq j$, $d_i \geq 1$, by (D0), and $d_i | d_j$, by (D2). Hence $d_j = 1$ implies $d_i = 1$ for $1 \leq i \leq j$.

$(d_n,1,\cdots,1)$, is said to be <u>trivial</u>.

(109) <u>Theorem</u>. Any trivial sequence $(d_n,1,\cdots,1)$ of length $n$ is the d-sequence of an $(\alpha,n-1,d_n+n-1)$-trivioid, and conversely.

<u>Proof</u>. Let $d(M) = (d_n,1,\cdots,1)$ for some rank $n$ matroid design $M = (E,\mathcal{H})$. By (81), $t_M(0,1,j) = j$ for $0 \leq j \leq n-1$, and $t_M(0,1,n) = d_n + n-1$.

Let $\alpha$ be the common cardinality of the points of $M$, and let $M'$ be an $\alpha$-deflation of $M$. By (47), $M'$ is simple and has the same t-function as $M$. Thus, every j-flat of $M$ has cardinality $j$, for $0 \leq j \leq n-1$. 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 $0 \leq j \leq n-1$. 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 $\alpha$, an $(\alpha,n-1,d_n+n-1)$-trivioid certainly exists, and it is straightforward to verify that its d-sequence is $(d_n,1,\cdots,1)$. ∎

(110) We recall from (13) that for any matroid $M = (E,\mathcal{H})$, 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 $\underline{c^*(M)}$ denote the minimum cardinality of the co-circuits of M. If M is an equicardinal matroid, then $c^*(M)$ is the size of every co-circuit of M. In particular, if M is a simple matroid design, then the leading term of d(M), the d-sequence of M, is $c^*(M)$.

(111) Theorem. Every matroid design M with prime co-circuit cardinality $c^*(M)$ is a trivioid.

Proof. Let $c^*(M) = p$ be a prime. Where $\alpha$ is the cardinality of the points of M, $\alpha | c^*(M)$ 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 $(p, \frac{k(M)}{p}, \frac{k(M)}{p} + 1)$ - trivioid. Otherwise, $\alpha = 1$ and M is simple. Therefore $d(M) = (p, d_{n-1}, \cdots, d_1)$. Let j be the greatest integer such that $d_j = 1$. By (D2), $d_{n-1} | p$ and $\frac{p}{d_{n-1}} \geq \frac{d_{j+1}}{d_j} > 1$. Hence $d_{n-1} = 1$, so $d_i = 1$ for $1 \leq i \leq n-1$. Thus, d(M) is trivial, so, by (109), M is a trivioid. ∎

The d-sequence of t-designs with $\lambda = 1$ may be characterized as follows.

(112) Theorem. For any integer $n \geq 3$, $M = (E, \mathcal{H})$ is an $(n-1)$-$(d_n + d_{n-1} + n-2, d_{n-1} + n-2, 1)$ design if and only if M is a simple, rank n matroid design and $d(M) = (d_n, d_{n-1}, 1, \ldots, 1)$.

Proof. This result follows immediately from (55) and the definition (79) of d-sequence. ∎

We point out that for any sequence of the form $(d_n, d_{n-1}, 1, \ldots, 1)$, where $d_n \geq d_{n-1} \geq 1$, the condition (D1) simply reduces to the requirement that the numbers $\lambda_i$ associated (26) with the corresponding (n-1)-design of (112) be integers. Likewise, (D2) is simply a consequence of Fisher's inequality for this (n-1)-design. However, it is well-known from BIBD theory that for given parameters $t,v,k,\lambda$, the integrality of the expressions for $\lambda_i$ 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 matroid design.

A D-consistent sequence that is the d-sequence of some matroid design will be called a realizable D-consistent sequence. In the following paragraphs we shall characterize the d-sequences of the finite projective and affine geometries, and invoke the known existence conditions for these geometries to show that a large class of D-consistent sequences are not realizable. In addition, we shall develop a new criterion for certain types of D-consistent sequences to be realizable.

(113) By (66) the t-function $t(i,j,k)$ of any $PG(n,s)$ satisfies $t(0,1,j) = \frac{s^j-1}{s-1}$, $0 \leq j \leq n+1$. Hence $d_j = \frac{s^j-1}{s-1} - \frac{s^{j-1}-1}{s-1} = s^{j-1}$. Thus, the d-sequence of any $PG(n,s)$ is $(s^n, s^{n-1}, \ldots, s, 1)$.

(114) Likewise, from (76) we conclude that the d-sequence of any $EG(n,s)$ is $(s^{n-1}(s-1), s^{n-2}(s-1), \ldots, s-1, 1)$.

The converses of (113) and (114) also hold. As a preliminary to establishing this result, we shall prove a partial converse to (113).

(115) Theorem. If $M = (E,\mathcal{H})$ is a simple matroid design of rank $n$, $n \geq 3$, and the last three terms of $d(M)$ are $s^2$, $s$, $1$ for some integer $s \geq 2$, then the lines of $M$ are the lines of a $PG(h-1,s)$ for some integer $h$, and $|E| = \frac{s^h-1}{s-1}$.

Proof. Let $F^3$ be any 3-flat of $M$. By (106), $M' = M \times F^3$ has d-sequence $(s^2,s,1)$, and, by (35), the lines and points of $M'$ are precisely the lines and points of $M$ contained in $F^3$. By (81), every line of $M'$ contains precisely $s+1$ points, and every point of $M'$ is contained in precisely $s+1$ lines. Let $L$ be a fixed line and let $x$ be

a fixed point of $M'$. If $x \notin L$, then there is a distinct line $L_{xy}$ containing $x$ and $y$ for each distinct point $y \in L$; since there are $s+1$ such lines, every line containing $x$ must intersect $L$ in a point.

(116) It follows from the above discussion that every two distinct lines of $M$ contained together in a 3-flat intersect in a point.

(117) Let $\mathcal{L}$ be the family of lines of $M$. We shall verify that $(E,\mathcal{L})$ satisfies (PG1) - (PG3). (PG1) follows from the definition of line in a matroid, and (PG3) follows from the assumption that $s \geq 2$. To verify (PG2), let $a,b,c,d$ be any four distinct elements of $E$, and suppose that the lines $L_{ab} = cl(\{a,b\})$ and $L_{cd} = cl(\{c,d\})$ contain a common point $\{e\}$. If $L_{ab} = L_{cd}$, (PG2) is trivially satisfied. If $L_{ab} \neq L_{cd}$, then for any points $f \in L_{ab}-L_{cd}$ and $g \in L_{cd}-L_{ab}$, $r(\{f,e,g\}) = 3$. Since $\{a,b\} \subseteq cl(\{f,e\})$ and $\{c,d\} \subseteq cl(\{g,e\})$, $\{a,b,c,d\} \subseteq F^3 = cl(\{f,e,g\})$, so the lines $L_{ac} = cl(\{a,c\})$ and $L_{bd} = cl(\{b,d\})$ are contained in $F^3$. But then, by (116), $L_{ac}$ and $L_{bd}$ contain a common point. Thus (PG2) holds.

(118) Therefore, for some integer $h$, $(E,\mathcal{L})$ is a $PG(h-1,s)$, and by (64), $|E| = \frac{s^h-1}{s-1}$. ∎

(119) Theorem. (Pointed out to the author by Richard Wilson.) If $D = (d_n, d_{n-1}, \ldots, d_1)$ is a realizable D-consistent sequence, $n \geq 3$, and $d_3 = s^2$, $d_2 = s$ for some integer $s \geq 2$, then $\sum_{i=1}^{n} d_i = \frac{s^h - 1}{s-1}$ for some positive integer $h$.

Proof. Let $M = (E, \mathcal{H})$ be a matroid design such that $d(M) = D$. By (105), we may assume that $M$ is simple. By (115), $|E| = \frac{s^h - 1}{s-1}$ for some positive integer $h$. But $\sum_{i=1}^{n} d_i$ is the number of points of $M$, and $M$ is simple, so $\sum_{i=1}^{n} d_i = \frac{s^h - 1}{s-1}$. ∎

The criterion of (119) 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 $36 + 4 + 2 + 1 = 43 \neq 2^h$ for any integer $h$.

(120) Theorem. For any integers $n \geq 2$ and $s \geq 2$, every simple matroid design with d-sequence of form $(s^n, s^{n-1}, \ldots, s, 1)$ is a PG(n,s), and conversely.

Proof. We have already noted in (113) that any PG(n,s) has a d-sequence of the given type.

Suppose conversely that $M = (E, \mathcal{H})$ is a simple matroid design with d-sequence $(s^n, s^{n-1}, \ldots, s, 1)$. Then $t_M(0,1,h) =$

$\frac{s^h-1}{s-1}$, $1 \leq h \leq n+1$. By (115), the set $\mathfrak{L}$ of lines of $M$ are precisely the lines of a finite projective geometry of order $s$ on the set $E$. Since $|E| = \sum_{j=0}^{n} s^j = \frac{s^{n+1}-1}{s-1}$, $(E,\mathfrak{L})$ is a $PG(n,s)$. Let $\mathcal{H}'$ be the family of hyperspaces of $(E,\mathfrak{L})$. To show that $M$ is a $PG(n,s)$, we must show that $\mathcal{H} = \mathcal{H}'$.

(121) For any flat $F$ of $M$, let $x,y \in F$, $x \neq y$, and let $L_{xy} = cl(\{x,y\})$ be the unique line of $M$ containing $\{x,y\}$. Where $J$ is any basis of $F$ containing $\{x,y\}$, we have $cl(\{x,y\}) \subseteq cl(J) = F$, so $L_{xy} \subseteq F$. Hence $F$ is line-closed. Thus every flat of $M$ is a subspace of $(E,\mathfrak{L})$.

Let $M' = (E,\mathcal{H}')$. By (66), $t_{M'}(0,1,h) = \frac{s^h-1}{s-1}$, $1 \leq h \leq n+1$, hence the t-functions of $M$ and $M'$ are the same. Therefore the total number of flats of $M$ and $M'$ is the same. But, by (121), every flat of $M$ is a flat of $M'$. Hence $M$ and $M'$ have the same flats. In particular, $\mathcal{H} = \mathcal{H}'$, so $M$ is a $PG(n,s)$. ∎

(122) Theorem. If $(d_n,d_{n-1},\ldots,d_1)$ is a realizable D-consistent sequence such that for some $m$, $1 \leq m \leq n-3$, and

positive integer $s$, $\frac{d_{j+1}}{d_j} = s$ for $m \leq j \leq m+2$, then $s$ is a prime power.

Proof. Let $M$ be a matroid design such that $d(M) = (d_n, d_{n-1}, \ldots, d_1)$, and let $F^{m-1}$ and $F^{m+3}$ be an $(m-1)$-flat and an $(m+3)$-flat of $M$, respectively, such that $F^{m-1} \subset F^{m+3}$. Let $M'$ be a simple deflation of $M(F^{m-1}, F^{m+3})$. By (105), (106), and our hypotheses, $d(M') = (s^3, s^2, s, 1)$, so, by (120), $M'$ is a $PG(3,s)$. Hence, by (73), $s$ is a prime power. ∎

(123) Using a similar argument to the above, we may also show that if $(d_n, d_{n-1}, \ldots, d_1)$ is any realizable D-consistent sequence such that $\frac{d_{m+1}}{d_m} = \frac{d_{m+2}}{d_{m+1}} = s$ for some integer $m$, $1 \leq m \leq n-2$, then $s$ satisfies the Bruck-Ryser conditions (74).

(124) It is easily verified that any sequence of the form $(s^n, s^{n-1}, \ldots, s, 1)$ is D-consistent, for any positive integers $n$ and $s$. Hence, by (122), all such sequences with $n \geq 3$, $s \geq 2$, and $s$ not a prime power are D-consistent but not realizable. In analogy with (120), we may derive the following characterization of the d-sequences of finite affine geometries.

(125) Theorem. For any integers $n \geq 3$ and $s \geq 2$, every simple rank $n$ matroid design $M$ with d-sequence of form $(s^{n-2}(s-1), s^{n-3}(s-1), \ldots, (s-1), 1)$ is an $EG(n-1,s)$ and conversely.

Proof. By (114), any $EG(n-1,s)$ has a d-sequence as given.

Conversely, let $M$ be a simple matroid design such that $d(M) = (s^{n-2}(s-1), s^{n-3}(s-1), \ldots, (s-1), 1)$.

(126) First we establish that for any two hyperplanes $H_1$, $H_2$ of $M$, either $H_1 \cap H_2 = \emptyset$ or $H_1 \cap H_2$ is an $(n-2)$-flat. Suppose that $H_1 \cap H_2 \neq \emptyset$, and let $x \in H_1 \cap H_2$. $M' = M \cdot (E-\{x\})$ has rank $n-1$ and d-sequence $(s^{n-2}, \ldots, s, 1)$, by (106). Further, $H_1' = H_1-\{x\}$ and $H_2' = H_2-\{x\}$ are hyperplanes of $M'$. Now (120) implies that $M'$ is an inflation of a $PG(n-2,s)$, so $H_1' \cap H_2'$ is an $(n-3)$-flat of $M'$. Hence $H_1 \cap H_2$ is an $(n-2)$-flat of $M$.

(127) Therefore every two distinct hyperplanes of $M$ are either disjoint, or intersect in precisely $t_M(0,1,n-2)$ elements. If $n \geq 5$, the theorem of Kantor (78) implies that $M$ is either a projective or affine geometry. However, $M$ is not a projective geometry, because the d-sequence of $M$ is not of the form given in (120). Hence $M$ is an affine geometry, and in fact it must be an $EG(n-1),s)$.

In the cases $n = 3$ and $n = 4$, we shall prove the result directly.

(128) Let $n = 3$. Every line of $M$ contains $s$ points, and every point is contained in $s+1$ lines, by (81). Hence, for every line $L$ and point $x$ not in $L$, there is exactly

one line disjoint from $L$ and containing $x$. Thus, the set $\mathcal{N}$ of lines of $M$ may be partitioned into parallel classes. By (81), $|\mathcal{N}| = s(s+1)$, and since there are $\frac{|E|}{s} = s$ lines in each class, there are exactly $s+1$ parallel classes, $P_1,\cdots P_{s+1}$. Choose a set $L_0 = \{y_1,y_2,\cdots,y_{s+1}\}$ of $s+1$ points disjoint from $E$, and for each parallel class $P_i$ of lines, adjoin the point $y_i$ to every line in $P_i$. The set $\mathcal{N}'$ of lines so created, together with $L_0$, are the lines of a rank 3 matroid $M' = (E \cup L_0, \mathcal{N}')$, and $M'$ clearly satisfies (PG1) - (PG3). Hence $M'$ is a PG(2,s). Moreover, $M = M' \times E$, so $M$ is an EG(2,s).

(129) Let $n = 4$. For any 3-flat (hyperplane) $H$ of $M$, $M \times H$ has d-sequence $(s(s-1),s-1,1)$, hence $M \times H$ is an EG(2,s). Further, (126) implies that every two 3-flats of $M$ are either disjoint or intersect in a common line.

(130) Let $\mathcal{L}$ be the set of lines of $M$. For any $L_1,L_2 \in \mathcal{L}$, write $L_1 \, R \, L_2$ if either $L_1 = L_2$, or $L_1 \cap L_2 = \emptyset$ and $L_1$ and $L_2$ are contained in a common 3-flat. We claim that $R$ is an equivalence relation on $\mathcal{L}$. Indeed, let $L_1,L_2,L_3$ be distinct lines such that $L_1 \, R \, L_2$ and $L_2 \, R \, L_3$, and let

$H_1$ be the 3-flat containing $L_1 \cup L_2$, $H_2$ the 3-flat containing $L_2 \cup L_3$.

If $L_3 \cap H_1 \neq \emptyset$, then $L_2 \subsetneq H_1 \cap H_2$, which implies that $r(H_1 \cap H_2) = 3$ and hence $H_1 = H_2$. Then $L_1, L_2$, and $L_3$ are distinct lines of $M \times H_1$, which is an EG(2,s), and $L_1$ and $L_3$ are both parallel to $L_2$. By (76), parallelism between lines is an equivalence relation in an EG(2,s), so $L_1 \cap L_3 = \emptyset$. Thus $L_1 \; R \; L_3$.

If $L_3 \cap H_1 = \emptyset$, choose $x \in L_1$ and let $H_3 = cl(L_3 \cup \{x\})$ be the unique 3-flat containing $x$ and $L_3$. By (129), $H_3 \cap H_1 = L$ is a line. If $L \cap L_2 \neq \emptyset$, then $L_3 \subsetneq H_2 \cap H_3$, so $H_2 = H_3$, which is impossible, because $x \in H_3 - H_2$. Therefore $L$ is parallel to $L_2$ in $H_1$. But then $L$ and $L_1$ both contain $x$ and are parallel to $L_2$, which implies, by (128), that $L_1 = L$. Since $L_3 \cap H_1 = \emptyset$, $L_3 \cap L_1 = \emptyset$, and so $L_1 \; R \; L_3$.

Therefore $R$ is transitive, and it follows at once that it is an equivalence relation. Let $Q_1, Q_2, \ldots, Q_t$ denote the equivalence classes of $R$. For each $L \in \mathcal{L}$ and $x \in E - L$,

$H = c\ell(\{x\} \cup L)$ is a 3-flat, and $M \times H$ is an $EG(2,s)$ whose lines are precisely the lines of $M$ contained in $H$. By (76) there is a line $L'$ containing $x$ and contained in $H$ that is parallel to $L$; that is, $L'$ is a line of $M$ containing $x$ such that $L' \, R \, L$. Thus $\bigcup_{L \in Q_i} L = E$ for each $i$, $1 \leq i \leq t$.

By (81), the lines of $M$ all have cardinality $s$, and $|E| = s^3$, so $|Q_i| = s^2$ for $1 \leq i \leq t$. Further, $M$ contains $s^2(s^2+s+1)$ lines altogether, so $t = \frac{|\mathcal{L}|}{|Q_i|} = s^2+s+1$. Let $H_0 = \{y_1, \ldots, y_{s^2+s+1}\}$ be a set of $s^2+s+1$ elements disjoint from $E$. We define a set of lines $\mathcal{L}'$ on $E' = E \cup H_0$ as follows. For each $i$, $1 \leq i \leq t$, and $L \in Q_i$, let $L \cup \{y_i\} \in \mathcal{L}'$. Further, for any 3-flat $H$ of $M$, let $Q_{H_1}, \ldots, Q_{H_{s+1}}$, for integers $H_1, \ldots, H_{s+1}$, be the $s+1$ equivalence classes from among $\{Q_1, \ldots, Q_t\}$ to which the lines contained in $H$ belong, and let the corresponding set $L_H = \{y_{H_1}, y_{H_2}, \ldots, y_{H_{s+1}}\}$ be contained in $\mathcal{L}'$.

Now it is straightforward to verify that $(E', \mathcal{L}')$ satisfies (PG1) - (PG3). Since $|E'| = |E| + |H_0| = s^3+s^2+s+1 = \frac{s^4-1}{s-1}$, $(E', \mathcal{L}')$ is a $PG(3,s)$. The family of hyperspaces

of $(E',\mathcal{L}')$ is $\mathcal{H}' = \{H_0\} \cup \{H \cup L_H : H \in \mathcal{H}\}$. Clearly, $M = (E',\mathcal{H}') \times E$; hence $M$ is an $EG(3,s)$ by definition. ∎

(131) Theorem. If $D = (d_n, d_{n-1}, \ldots, d_1)$ is a realizable D-consistent sequence such that for some $m$, $1 \leq m \leq n-3$, and positive integer $s$, $\frac{d_{m+1}}{d_m} = s-1$ and $\frac{d_{m+2}}{d_{m+1}} = \frac{d_{m+3}}{d_{m+2}} = s$, then $s$ is a prime power.

Proof. Let $M$ be a simple matroid design such that $d(M) = (d_n, d_{n-1}, \ldots, d_1)$. Let $F^{m-1} \subseteq F^{m+3}$, where $F^{m-1}$ is an $(m-1)$-flat and $F^{m+3}$ is an $(m+3)$-flat, and let $M' = (E',\mathcal{H}')$ be a simple deflation of $M(F^{m-1}, F^{m+3})$. By (105), (106), and our hypotheses, $d(M') = (s^2(s-1), s(s-1), s-1, 1)$. Hence, by (125), $M'$ is an $EG(3,s)$. Therefore by definition there exists a $PG(3,s)$ $M''$ such that $M' = M'' \times E'$. By (73), therefore, $s$ is a prime power. ∎

## 3.11. Computation of D-consistent sequences

In spite of the insufficiency of the conditions (D0), (D1), and (D2) as existence criteria for matroid designs, 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 $\gamma$.

(131a) Let $\gamma$ be given, and let $p_1 p_2 \cdots p_t$ be the prime factorization of $\gamma$ such that $p_1 \leq p_2 \cdots \leq p_t$. Let $D = (d_n, d_{n-1}, \cdots, d_1)$ be a D-consistent sequence such that $d_n = \gamma$, and let $s$ be the largest index for which $d_s = 1$. Then $d_s = d_{s-1} = \cdots = d_1 = 1$, by (108). Let $D'$ be the truncated sequence $(d_n, d_{n-1}, \cdots, d_{s+1})$. $D'$ is called the nontrivial part of $D$. By (D2), $D'$ can have at most $t$ terms.

If $\gamma$ has few prime factors, 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.

(132) To verify (D1) for the sequence $D = (d_n, d_{n-1}, \cdots, d_1)$, it is usually sufficient (if $D$ has a short nontrivial part) to check that, for every lower interval $D' = (d_h, d_{h-1}, \cdots, d_1)$ of $D$, the quotients

$$\frac{d_h + d_{h-1}}{d_{h-1}}, \quad \frac{(d_h + d_{h-1})(d_h + d_{h-1} + d_{h-2})}{d_{h-1}(d_{h-1} + d_{h-2})}, \ldots, \quad \frac{\prod_{\ell=1}^{h-1} \sum_{j=\ell}^{h} d_j}{\prod_{\ell=1}^{h-1} \sum_{j=\ell}^{h-1} d_j}$$

are integers.

(133) Let $D = (d_n, d_{n-1}, \cdots, d_1)$ be a sequence of positive integers. A <u>normalized interval of D</u> having <u>length</u> i is a sequence of form

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

where $1 \leq i \leq n$, $0 \leq h \leq n-i$.

The following fact is sometimes useful in determining D-consistency.

(134) <u>Theorem</u>. If D is D-consistent, then every normalized interval of D is D-consistent.

<u>Proof</u>. Suppose that D is D-consistent, and let $D' = (d'_\ell, d'_{\ell-1}, \cdots, d'_1)$ be a normalized interval of D, where $d'_i = \frac{d_{h+i}}{d_{h+1}}$ for $1 \leq i \leq \ell \leq n$ and some h, $0 \leq h \leq n-i$.

Clearly, D′ satisfies (D0) and (D2) of (83), since D does.

For $0 \leq i \leq j \leq k \leq \ell$ we have

$$\frac{\prod_{q=i+1}^{j} \sum_{m=q}^{k} d'_m}{\prod_{q=i+1}^{j} \sum_{m=q}^{j} d'_m} = \frac{\prod_{q=i+1}^{j} \sum_{m=q}^{k} \frac{d_{h+m}}{d_{h+1}}}{\prod_{q=i+1}^{j} \sum_{m=q}^{j} \frac{d_{h+m}}{d_{h+1}}}$$

$$= \frac{\prod_{q=h+i+1}^{h+j} \sum_{m=q}^{k+h} d_m}{\prod_{q=h+i+1}^{h+j} \sum_{m=q}^{j+h} d_m},$$

which is integral, by (D1) applied to D. ∎

As an application, let us find all D-consistent sequences with leading term 20. By (109), every sequence of form (20,1,...,1) is D-consistent. 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). Using (132), it is easy to check that (20,2,1) and (20,4,2,1) are not D-consistent; hence, by (134), 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 (125), EG(2,5) is the unique matroid design with d-sequence (20,4,1). There is also a matroid design with d-sequence (20,4,1,1), namely, the inversive plane IP(2,5).

In Appendix I we have listed all nontrivial D-consistent sequences with leading terms 1-40, using the methods presented above. Matroid designs corresponding to the sequences are

given, if known. In certain cases (119) implies that a D-consistent sequence is not realizable. In other cases, a D-consistent sequence may not be realizable because it corresponds to a set of parameters for which no BlBD exists. For results concerning the nonexistence of BlBD's the reader is referred to [ 5 ].

## 3.12. Bounds on rank of nontrivial matroid designs with given co-circuit cardinality

Appendix I 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 matroid design with given co-circuit cardinality. As a preliminary, we shall state and prove an interesting number-theoretic result that appears to be new.

(135) For every pair $(n,m)$ of integers, $n \geq m \geq 1$, let

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

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 $0 \leq r \leq t$. (Thus $\beta(m,n) = 0$ if $m \nmid n$).

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

Proof. We begin by proving the following combinatorial identity. For non-negative integers $a,b,t$, $a \geq t$, $b \geq t$,

$$(137) \qquad \binom{a}{t} = \sum_{r=0}^{t} (-1)^r \binom{b}{r}\binom{a+b-r}{t-r}$$

Let $A$ and $B$ be disjoint sets of $a$ and $b$ elements respectively. $\binom{a+b-r}{t-r}$ shall be interpreted as the number of ways of completing an $r$-subset of $B$ to a $t$-subset of $A \cup B$. Let $T$ be any $t$-subset of $A \cup B$, and let $|T \cap B| = s$. Then for each $r$, $0 \leq r \leq s$, $T$ will be counted $(-1)^r \binom{s}{r}$ times by the right side of (137). But $\sum_{r=0}^{s} (-1)^r \binom{s}{r} = 0$ if $s > 0$ and $\sum_{r=0}^{0} (-1)^r \binom{0}{r} = 1$. Hence the right side of (137) counts the number of $t$-subsets of $A \cup B$ disjoint from $B$, which is $\binom{a}{t}$. (This formula is also developed in [14] as a variant of Van der Monde's convolution formula.)

Dividing both sides of (137) by $\binom{b}{t}$, and using the relation $\dfrac{\binom{b}{r}}{\binom{b}{t}} = \dfrac{\binom{t}{r}}{\binom{b-r}{t-r}}$, $0 \leq r \leq t$, we can re-write (137) as follows:

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

For given integers $n > m \geq 2$, let $0 \leq t \leq n-m$, and substitute $a = n-m$, $b = m+t-1$ in (138). Then we obtain

(139) $$\frac{\binom{n-m}{t}}{\binom{m+t-1}{t}} = \sum_{r=0}^{t} (-1)^r \binom{t}{r} \frac{\binom{n+t-1-r}{t-r}}{\binom{m+t-1-r}{t-r}}$$

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

by (135). Hence, if $\pi_{t-r}$ is integral for $0 \leq t-r \leq t$, then $\binom{n-m}{t}/\binom{m+t-1}{t}$ is integral. If $t > 0$, it follows that $m+t-1 \leq n-m$, so $t \leq n-2m+1$. If $t = 0$, this inequality also holds, since $m \leq \frac{n+1}{2}$. Hence $\beta(m,n) \leq n-2m+1$. ∎

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

(141) Theorem. If $M = (E,\mathcal{H})$ is a simple, nontrivial matroid design with hyperplane cardinality $k(M)$, then

(i) $k(M) \leq |E|/2$.

(ii) $c(M) \leq c^*(M)$

(iii) $r(M) \leq c^*(M)$

Proof. Let $d(M) = D = (d_n, d_{n-1}, \cdots, d_1)$ and let $s$ be the greatest index such that $d_s = 1$. $s \leq n-2$ because $M$, and hence $D$, is nontrivial. Hence the interval $(d_{s+2}, d_{s+1}, 1, \cdots, 1)$ exists and is D-consistent, by (134). For each $k$, $1 \leq k \leq s+1$,

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

$$= \frac{\prod_{\ell=s-k+2}^{s+1} \sum_{m=\ell}^{s+2} d_m}{\prod_{\ell=s-k+2}^{s+1} \sum_{m=\ell}^{s+1} d_m},$$

which is integral, by (D1). Since $\frac{d_{s+2}+d_{s+1}+1}{2} \geq d_{s+1} \geq 2$, (136) implies that

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

that is

$$s \leq d_{s+2} - d_{s+1}. \tag{142}$$

Let $\ell = n-s$ and let $D' = (d'_\ell, d'_{\ell-1}, \cdots, d'_1)$, where $d'_j = \frac{d_{s+j}}{d_{s+1}}$, $1 \leq j \leq \ell$. $D'$ is a normalized interval of $D$, so $D'$ is D-consistent. Hence $\frac{d'_{j+1}}{d'_j} \geq \frac{d'_j}{d'_{j-1}}$, $2 \leq j \leq \ell-1$, by (D2), and in particular

$$d'_{j+1} \geq d'_2 d'_j, \quad 1 \leq j \leq \ell-1. \tag{143}$$

We shall prove that

(144) $\sum_{j=1}^{m-1} d'_j \le \frac{d'_m - 1}{d'_2 - 1}$, for $2 \le m \le \ell$. (144) clearly holds when $m = 2$. For $m > 2$, suppose inductively that

$$\sum_{j=1}^{m-2} d'_j \le \frac{d'_{m-1} - 1}{d'_2 - 1} .$$

Then

$$\sum_{j=1}^{m-1} d'_j \le \frac{d'_{m-1} - 1}{d'_2 - 1} + d'_{m-1}$$

$$= \frac{d'_{m-1} - 1 + (d'_2 - 1)d'_{m-1}}{d'_2 - 1}$$

$$\le \frac{d'_m - 1}{d'_2 - 1} ,$$

by (143). (144) follows by induction. In particular,

$$\sum_{j=1}^{\ell-1} d'_j \le \frac{d'_\ell - 1}{d'_2 - 1} ,$$

that is,

$$\sum_{j=s+1}^{n-1} \frac{d_j}{d_{s+1}} \le \frac{\frac{d_n}{d_{s+1}} - 1}{\frac{d_{s+2}}{d_{s+1}} - 1} .$$

Hence

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

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

By (142), $s + \sum_{j=s+1}^{n-1} d_j \leq d_{s+2} - d_{s+1} + \frac{d_{s+1}(d_n - d_{s+1})}{d_{s+2} - d_{s+1}}$,

(146) hence $k(M) \leq d_{s+2} - d_{s+1} + \frac{d_{s+1}(d_n - d_{s+1})}{d_{s+2} - d_{s+1}}$. We claim that

(147) $$d_{s+2} - d_{s+1} + \frac{d_{s+1}(d_n - d_{s+1})}{d_{s+2} - d_{s+1}} \leq d_n.$$

Indeed, this holds if and only if

$$d_{s+2}^2 - 2d_{s+2}d_{s+1} + d_{s+1}^2 + d_{s+1}d_n - d_{s+1}^2 \leq d_{s+2}d_n - d_{s+1}d_n$$

iff $$d_{s+2}^2 - 2d_{s+2}d_{s+1} \leq d_{s+2}d_n - 2d_{s+1}d_n$$

(148) iff $d_{s+2}(d_{s+2} - 2d_{s+1}) \leq d_n(d_{s+2} - 2d_{s+1})$. Now

$\frac{d_{s+2}}{d_{s+1}} \geq \frac{d_{s+1}}{d_s} \Rightarrow d_{s+1} \geq 2$. Hence (148) is deducible from $d_{s+2} \leq d_n$, which is a consequence of (D2).

By (146) and (147), $k(M) \leq d_n$. Since M is simple, $d_n = c^*(M)$, hence $k(M) \leq c^*(M)$. But $k(M) + c^*(M) = |E|$, and so $k(M) \leq \frac{|E|}{2}$, establishing (i).

Since $k(M) = \sum_{j=1}^{n-1} d_j$, $d_j \geq 1$, and $d_{s+1} > 1$, we have that

(149) $$k(M) > n-1.$$

But the rank of any hyperplane is precisely $n-1$, so every hyperplane must contain a circuit. Hence $c(M) \leq k(M) \leq d_n = c^*(M)$, establishing (ii).

(iii) follows from (149): $r(M) = n \leq k(M) \leq c^*(M)$. ∎

There are examples of matroid designs for which (i), (ii) and (iii) of (141) are all satisfied as equalities: for example, the affine geometry $EG(3,2)$, and the Witt design $5\text{-}(12,6,1)$. Therefore, (141) is, in a certain sense, best possible.

## 3.13. The t-designs in a matroid design

We have already observed in (29) that the flats of a given cardinality in a simple matroid design $M$ 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 matroid design form a $t$-design for an appropriate $t$. These results yield a method for deriving new $t$-designs from known ones in certain cases.

(150) Where $c(M)$ is the minimum cardinality of a circuit of the matroid $M = (E,\mathcal{H})$, 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 <u>independence number of $M$</u>, $\beta(M)$.

(151) The independence number $\beta(M)$ of a simple matroid design $M = (E,\mathcal{H})$ is found from the t-function of $M$ as follows. Every subset of $E$ having cardinality $j \leq \beta(M)-1$ is not only independent, but closed. Hence, for $0 \leq j \leq \beta(M)-1$, the $j$-flats of $M$ are precisely the $j$-subsets of $E$, so $t_M(0,1,j) = j$, since $M$ is simple. By definition of $\beta(M)$, there exists a circuit $C$ of $M$ having cardinality $\beta(M)+1$. Hence $cl(C)$ is a $\beta(M)$-flat having cardinality greater than $\beta(M)$. Hence $t_M(0,1,\beta(M)) > \beta(M)$. Thus, in a simple matroid design $M$, $\beta(M)$ is the least integer $j$ such that $t_M(0,1,j) > j$. In terms of the d-sequence of $M$, $\beta(M)$ is therefore the least integer $j$ such that $d_j > 1$. If $M$ is nonsimple, then obviously $\beta(M) = 1$.

(152) <u>Theorem</u>. Let $M = (E,\mathcal{J})$ be a rank $n$ matroid design with independence number $\beta$, where $2 \leq \beta \leq n$, and for each $j$, $\beta \leq j \leq n$, let $\mathcal{J}_j$ be the set of $j$-flats of $M$. Then $(E,\mathcal{J}_j)$ 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 $\beta$-subset of $E$ is independent, every $\beta$ elements are contained in one and only one $\beta$-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 $(E,\mathfrak{I}_j)$ is a $\beta$-$(|E|, t_M(0,1,j), t_M(\beta,j,n))$ design. ∎

(153) Theorem. Let $M = (E,\mathfrak{I})$ be a rank $n$ matroid design with independence number $\beta$, $2 \leq \beta \leq n$. For each $j$, $\beta \leq j \leq n$, the family $\mathfrak{I}_j$ of independent sets of cardinality $j$ in $M$ are the blocks of a $\beta$-$(|E|,j,\mu_j)$ design on the set $E$, where

$$(154) \qquad \mu_j = \frac{\prod_{\ell=\beta}^{j-1}(t_M(0,1,n) - t_M(0,1,\ell))}{(j-\beta)!} \quad \text{for } j > \beta,$$

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

Proof.

(155) Let $j$ be given, $\beta \leq j \leq n$, and let $E_\beta$ be a fixed $\beta$-subset of $E$. If $j = \beta$, we take $\mu_j = 1$ and the theorem obviously holds. Thus we may assume that $j > \beta$ in what follows.

By the definition of $\beta$, $E_\beta$ is independent, $F_0 = c\ell(E_\beta)$ is a $\beta$-flat of $M$, and $E_\beta$ is a basis of $F_0$. Since $\beta \geq 2$, $M$ is simple, and hence $|F_0| = t_M(0,1,\beta)$. For any

element $x_1 \in E-F_0$, $E_\beta \cup \{x_1\}$ is independent (because $F_0$ is closed), and clearly any independent $(\beta+1)$ - set $J$ containing $E_\beta$ has form $E_\beta \cup \{x\}$ for some $x \in E-F_0$. Thus $E_\beta$ is contained in precisely $|E|-|F_0| = t_M(0,1,n) - t_M(0,1,\beta)$ independent sets of cardinality $\beta+1$.

(156) In general, let $J$ be any independent $j$-subset of $E$ containing $E_\beta$, and let us write $J-E_\beta = \{x_1,\ldots,x_{j-\beta}\}$. (Recall that $j > \beta$.) Let $F_0 = cl(E_\beta)$ and $F_i = cl(F_0 \cup \{x_1,\ldots,x_i\})$ for each $i$, $1 \leq i \leq j-\beta$. Clearly, for each $i < j-\beta$, $x_{i+1} \in E-F_i$ and $F_{i+1} = cl(F_i \cup \{x_{i+1}\})$. Thus, with each independent $j$-set $J$ containing $E_\beta$, we may associate a sequence $\mathfrak{F}: F_0 \subset F_1 \subset \ldots \subset F_{j-\beta}$ of nested flats and an ordering $J' = (x_1,\ldots,x_{j-\beta})$ of $J-E_\beta$ such that $x_{i+1} \in E-F_i$ and $F_{i+1} = cl(F_i \cup \{x_i\})$ for $0 \leq i < j-\beta$. Moreover, this association may be made in precisely $(j-\beta)!$ ways.

(157) Conversely, for any sequence of flats $F_0 \subset F_1 \ldots \subset F_{j-\beta}$, where $F_0 = cl(E_\beta)$, 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 $j$. Indeed, let $k$ be the least integer such that $E_\beta \cup \{x_1,\ldots,x_k\}$ is dependent. Using (7), it follows that $F_{k-1} = cl(E_\beta \cup \{x_1,\ldots,x_{k-1}\})$,

and hence, by (6), that $x_k \in F_{k-1}$, which is contrary to assumption. Therefore $J$ is an independent set of rank $j$ containing $E_\beta$.

A sequence of flats as in (157) can be chosen in precisely $\prod_{\ell=\beta}^{j-1} (t_M(0,1,n) - t_M(0,1,\ell))$ distinct ways, and each corresponding independent $j$-set containing $E_\beta$ is thereby counted $(j-\beta)!$ times, by (156). Thus $E_\beta$ is contained in precisely

$$\mu_j = \frac{\prod_{\ell=\beta}^{j-1}(t_M(0,1,n) - t_M(0,1,\ell))}{(j-\beta)!} \text{ independent } j\text{-sets.} \blacksquare$$

(158) With $M = (E,\mathcal{I})$ as in (153), an argument similar to the above proof shows that, for $0 \le i \le \beta \le j \le n$, every $i$-subset of $E$ is contained in precisely

$$(159)\quad (\mu_j)_i = \frac{\prod_{\ell=i}^{j-1}(t_M(0,1,n) - t_M(0,1,\ell))}{(j-i)!} \text{ independent}$$

$j$-sets of $M$.

To prove that the circuits of a given cardinality in a matroid design form a t-design, we shall use the following basic result.

(160) Theorem. For any matroid $M = (E,\mathcal{I})$ and basis $B$ of $M$ and $x \in E-B$, $\{x\} \cup B$ contains a unique circuit, which

contains $x$.

Proof. Any basis $B$ of $M$ is a maximal independent subset of $E$, so $A = \{x\} \cup B$ is dependent for any $x \in E-B$, and every circuit contained in $A$ obviously contains $x$. If $C_1$ and $C_2$ are two such circuits, then by axiom (C2) there is a circuit $C$ such that $C \subseteq C_1 \cup C_2 - \{x\} \subseteq B$. But the latter is impossible, since $B$ is independent. ∎

(161) Theorem. Let $M = (E, \mathcal{H})$ be a simple, rank $n$ matroid design with independence number $\beta$. For each $j$, $\beta < j \leq n+1$, the family $\mathcal{C}_j$ of cardinality-$j$ circuits of $M$ are the blocks of a $\beta$-$(|E|, j, \eta_j)$ design on the set $E$, where

$$\eta_j = \mu_{j-1} \left\lfloor \frac{t_M(0,1,n) + \sum_{i=1}^{j-2} (-1)^{j-i-1} \binom{j-1}{i} t_M(0,1,i)}{j-\beta} \right\rfloor - \mu_j, \tag{162}$$

and $\mu_j$ is as defined in (153) for $\beta < j \leq n$, and $\mu_{n+1} = 0$.

Proof.

(163) 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 (161) for the case $j = n+1$.

(164) 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, $1 \leq i \leq n$.

(165) 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 $(-1)^{n-i}$. Then, by (165), $f(n+1)$ 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

$$(166) \qquad F(x) = \sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i-1} = 0 \quad \text{for} \quad x \in J.$$

(167) If $x \in E-J$, let $C_x$ be the unique circuit such that $x \in C_x \subseteq J \cup \{x\}$, by (160), and 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 $i-j+1 = \ell$, we have that

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

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 (153), every $\beta$-subset of $E$ is contained in exactly $\mu_n$ bases of $M$, where $\mu_n$ is as in (154). Further, every circuit $C$ of cardinality $n+1$ contains $n+1-\beta$ bases of $M$ containing a given $\beta$ subset of $C$. Hence the number of cardinality - $(n+1)$ circuits of $M$ containing any given $\beta$-subset of $E$ is exactly

$$(168)\quad \eta_{n+1} = \frac{f(n+1)}{n+1-\beta} = \mu_n\left[\frac{t_M(0,1,n) + \sum_{i=1}^{n-1}(-1)^{n-i}\binom{n}{i}t_M(0,1,i)}{n+1-\beta}\right].$$

(169) For an arbitrary $j$, $\beta < j \leq n+1$, we consider $M^{(j-1)}$, the $(j-1)$-truncation of $M$. The circuits of $M^{(j-1)}$ 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 (43), $M^{(j-1)}$ has rank $j-1$ and its t-function $t(i,j,k)$ is determined by

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

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

Hence (168) applied to $M^{(j-1)}$ implies that every $\beta$-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, $\mu_j$ of these circuits are cardinality-$j$ independent sets of $M$, by (169). Thus every $\beta$-subset of $E$ is contained in precisely

$$\eta_j = \frac{\mu_{j-1}f(j)}{j-\beta} - \mu_j$$ cardinality-$j$ circuits of $M$. ∎

(170) Let us observe that we may have $\eta_j = 0$ for some integers $j$ in (162); in this case $C_j = \emptyset$ and $(E,C_j)$ is said to be a <u>vacuous</u> $\beta$-design.

(171) With $M$, $n$, and $\beta$ as in (161), it follows from (160) and the proof of (161) that, for $0 \le i \le \beta$ and $\beta < j \le n+1$, every $i$-subset of $E$ is contained in precisely

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

cardinality-$j$ circuits of $M$.

## 3.14. Some new t-designs

Before applying the results of (153) and (161) to the construction of new t-designs, we shall point out several very natural ways of obtaining new t-designs from given ones.

(172) Theorem. Let $(E,\mathcal{H})$ be a $t$-$(v,k,\lambda)$ design, and let $\mathcal{H}' = \{E-H: H\in\mathcal{H}\}$. Then $(E,\mathcal{H}')$ is a $t$-$(v,v-k,\lambda')$ design, called the complementary design to M, and $\lambda' = \lambda\frac{\binom{v-k}{t}}{\binom{k}{t}}$.

Proof. As in (26), let $\lambda_j$ be the number of members of $\mathcal{H}$ containing any given $i$-subset of $E$, for each $j$, $0 \le j \le t$. Further, let $E_t$ be a fixed $t$-subset of $E$, and for each $j$-subset $S$ of $E_t$, let $\eta_j$ be the number of members of $\mathcal{H}$ intersecting $E_t$ in precisely the set $S$. Then $\eta_t = \lambda$ by hypothesis, so $\eta_t$ is well-defined.

(173) In general, $\eta_j = \lambda_j - \sum_{i=1}^{t-j}\binom{t-j}{i}\eta_{j+i}$. Using downwards induction on $j$, it follows that $\eta_j$ is well-defined for all $j$ such that $0 \le j \le t$. In particular, $\eta_0$ is well-defined, and represents the number of members of $\mathcal{H}$ disjoint from $E_t$. By (173) and the inductive argument, $\eta_0$ does not depend on the particular $t$-subset $E_t$ chosen. Hence $\eta_0$ is precisely the number of members of $\mathcal{H}'$ containing any $t$-subset

of E. Letting $\eta_0 = \lambda'$, it follows that $(E,\mathcal{B}')$ is a $t\text{-}(v,v-k,\lambda')$ design.

Finally,

$$|\mathcal{B}| = \lambda \frac{\binom{v}{t}}{\binom{k}{t}},$$

and likewise

$$|\mathcal{B}'| = \lambda' \frac{\binom{v}{t}}{\binom{v-k}{t}} .$$

But

$$|\mathcal{B}| = |\mathcal{B}'|,$$

and so

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

This result is also noted in [ 1 ].

(174) Let $(E,\mathcal{B})$ be a $t\text{-}(v,k,\lambda)$ design, and let $\mathcal{B}'$ be the family of k-subsets of E not contained in $\mathcal{B}$. Clearly, $(E,\mathcal{B}')$ is a $t\text{-}(v,k,\lambda')$ design, where $\lambda' = \binom{v-t}{k-t} - \lambda$. $(E,\mathcal{B}')$ will be called the <u>opposite design to M</u>. This obvious construction seems to have passed unnoticed in the literature on t-designs.

(175) Let $(E,\mathcal{B})$ be a $t\text{-}(v,k,\lambda)$ design such that $|H_1 \cap H_2| \leq m$ for any distinct $H_1, H_2 \in \mathcal{B}$. Suppose also that for some integers $\ell \leq m$ and $\lambda'$ there exists a $t\text{-}(k,\ell,\lambda')$ design $(E',\mathcal{B}')$. For each $H \in \mathcal{B}$, let $(H,\mathcal{B}'_H)$ be any design on

the set $H$ that is isomorphic to $(E',\mathcal{H}')$, and let $\mathcal{H}'' = \bigcup_{H \in \mathcal{H}} \mathcal{H}'_H$. Then it is straightforward to verify that $(E,\mathcal{H}'')$ is a $t$-$(v,k,\lambda\lambda')$ design, called a <u>composition of $(E,\mathcal{H})$ with $(E',\mathcal{H}')$</u>. (This construction has already been pointed out by Hanani [7 ] in the context of BIBD's, but it seems appropriate to generalize it to arbitrary t-designs and give a name to it.)

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

(176) By (55), $r(M) = t+1$ and $\beta(M) = t$. Hence every circuit of $M$ has cardinality $t+1$ or $t+2$. In this case, (153) and (161) have particularly simple interpretations.

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

(178) The family $\mathcal{B}$ of bases of $M$ is evidently precisely

the collection of (t+1)-subsets of E that are not contained in $C_{t+1}$. Thus (E,$\mathcal{B}$) is a t-(v,t+1,v-k) design, the opposite to $(E,C_{t+1})$.

(179) Finally, the family $C_{t+2}$ 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 $(E,C_{t+2})$ is a $t\text{-}(v,t+2,\frac{(v-k)(v-(t+1)(k-t+1))}{2})$ design, which we shall call the <u>circuit design</u> of M.

The construction of (179) 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,
($t \geq 3$) 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. | $3 - (q^n+1, 5, \frac{(q^n-q)(q^n-4q+5)}{2})$ |
| $4 - (11, 5, 1)$ | $4 - (11, 6, 3)$ |
| $4 - (23, 7, 1)$ | $4 - (23, 6, 24)$ |
| $5 - (12, 6, 1)$ | vacuous, $\lambda = 0$ |
| $5 - (24, 8, 1)$ | vacuous, $\lambda = 0$ |

## 3.15. Self-dual matroid designs

We close the chapter on matroid designs by developing an intriguing unsolved problem in the theory of t-designs.

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

(180) 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 $r(M) = \frac{|E|}{2}$.

(181) Theorem. If $M$ is a simple, nontrivial, self-dual matroid design and $k(M) = k$, then $M$ is a $(k-1)$ - $(2k,k,1)$ design and $k+1$ is an odd prime.

Conversely, every $(k-1)$ - $(2k,k,1)$ design $M$ is a simple, self-dual matroid design with hyperplane cardinality $k$, and $M$ is nontrivial if $k > 2$, in which case $k+1$ is an odd prime.

Proof. Let $M = (E,\mathcal{H})$ be a simple, nontrivial, self-dual matroid design and let $k(M) = k$. By (141), $k \leq \frac{|E|}{2}$. Further, $\frac{|E|}{2} = r(M)$, by (180). But $k = |H| \geq r(H) = r(M)-1$ for every $H \in \mathcal{H}$, so $\frac{|E|}{2} - 1 \leq k \leq \frac{|E|}{2}$. If $k = \frac{|E|}{2} - 1$, then evidently every hyperplane consists of $r(M)-1$ independent elements. Therefore every subset of $r(M)$ elements of $E$ is independent, 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 $0 \leq j \leq k-2$, the $j$-flats of $M$ are all simple. Since the $(k-1)$-flats (hyperplanes)

have cardinality $k$, and $|E| = 2k$, $M$ is a matroid design with d-sequence $(k,2,1,1,\ldots,1)$ containing $k-2$ '1's. It follows from (55) that $M$ is a $(k-1)$-$(2k,k,1)$ design.

Suppose that $k+1$ is not a prime, and let $p$ be a prime divisor of $k+1$, where $1 < p < k+1$. By (81),

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

$$= \frac{(k+p)(k+p-1)\cdots(k+2)}{p \quad (p-1) \cdots 2} \tag{187}$$

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 (187), which gives a contradiction. Therefore $k+1$ is a prime. If $(k+1) = 2$, then $k = 1$ and $M$ is a rank 1 matroid design on a set of two elements. Hence $M$ is not simple, contrary to hypothesis. Thus, $k+1$ is an odd prime., and the first part of the theorem is proved.

(188) Suppose, conversely, that $M = (E,\mathcal{H})$ is a $(k-1)$-$(2k,k,1)$ design. It is easy to see that a 0-$(2,1,1)$ design does not exist; hence $k \geq 2$. If $k = 2$, then $M$ is the trivial rank 2 matroid consisting of two 2-points. If $k > 2$, then, by (151), $\beta(M) = k-1 \geq 2$, and hence $M$ is simple. $M$ is clearly nontrivial,

since every (k-1)-subset is contained in more than one K-subset of E when $|E| = 2k \geq 6$. Finally, it has been observed by Mendelsohn [12] that for every (k-1)-(2k,k,1) design (V,$\mathfrak{b}$), W $\in \mathfrak{b}$ implies E-W $\in \mathfrak{b}$. Therefore, M is a simple, nontrivial, self-dual matroid design, and, by the first part of the proof, k+1 is a prime. ∎

The following is a conjecture.

(189) For every odd prime p there exists a unique simple self-dual matroid design (unique up to isomorphism) having rank p-1.

For the primes 3,5, and 7, the conjecture of (189) is true. Indeed, for p = 3 there exists a $D_1(4,2,1)$, which is just a rank 2 matroid consisting of two disjoint 2-points. For p = 5, there exists a $D_3(8,4,1)$, namely, an EG(3,2), which is known to be the unique $D_3(8,4,1)$ [19]. For p = 7, there exists a $D_5(12,6,1)$, which was discovered and proved to be unique by Witt [19].

The next case (p = 11) involves finding a $D_9(20,10,1)$. A search for such a matroid design is presently being conducted.

# CHAPTER IV

# EQUICARDINAL MATROIDS

## 4.1 Equicardinal matroids that are not matroid designs

We turn our attention to the study of the more general class of equicardinal matroids. In an equicardinal matroid M, we only demand that all the hyperplanes have the same cardinality, which we denote as before by k(M). In particular, the points of an equicardinal matroid may have different cardinalities, which allows more structural freedom than is possible in matroid designs. However, simple equicardinal matroids are virtually as difficult to construct as matroid designs. Even more difficult is the construction of equicardinal matroids whose hyperplanes form a t-design, but which are not matroid designs. As an introduction to the theory of equicardinal matroids, we shall now provide several examples of such matroids, based on the existence of a 5-(24,8,1) design due to Witt [19].

In [19], Witt proved that there exists a unique 5-(24,8,1) design (up to isomorphism). We shall denote it by $W_{24} = (E,\mathcal{H})$.

By (112), $W_{24}$ is a rank 6 matroid design with hyperplane family $\mathcal{H}$, and its d-sequence is (16,4,1,1,1,1).

(190) Theorem. The family of circuits $C$ of $W_{24} = (E,\mathcal{H})$ is precisely the set of 6-subsets of members of $\mathcal{H}$, and $(E,C)$ is a 5-(24,6,3) design.

Proof. By (176) every circuit of $W_{24}$ has cardinality 6 or 7. Let $C_7$ be the set of circuits of cardinality 7. Then, substituting $v = 24$, $k = 8$, and $t = 5$ into the formula of (179), we have that $(E,C_7)$ is a 5-(24,7,0) design; i.e., $C_7 = \emptyset$. Hence every circuit of $W_{24}$ has cardinality 6, and it follows from (177) that the circuits of $W_{24}$ are precisely the 6-subsets of members of $\mathcal{H}$. Therefore $(E,C)$ is the composition of $(E,\mathcal{H})$ with a $\sigma(1,6,8)$, so $(E,C)$ is a 5-(24,6,3) design. ∎

(191) Theorem. The dual of $W_{24}$, $W_{24}^*$, is a simple rank 18 equicardinal matroid that is a 5-design but not a matroid design.

Proof. Let $W_{24} = (E,\mathcal{H})$, with circuit family $C$. By (13), the set $\mathcal{H}^*$ of hyperplanes of $W_{24}^*$ is precisely the set of complements in $E$ of the circuits of $W_{24}$; i.e., $(E,\mathcal{H}^*)$ is the complementary design to $(E,C)$. By (190), $(E,C)$ is a 5-(24,6,3) design, so it follows from (172) that $(E,\mathcal{H}^*)$ is a 5-$(24,18,\binom{18}{5}/2)$ design. In particular, $W_{24}^*$ is an equicardinal matroid, and $k(W_{24}^*) = 18$. Further, by definition of the dual

(12), $r(W_{24}^*) = |E| - r(W_{24}) = 18$. 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 equicardinal matroid that is a 5-design.

If $W_{24}^*$ were a matroid design, then by (141) it would either be a trivioid (which is clearly not the case), or it would satisfy $k(W_{24}^*) \leq |E|/2$, which is false because $k(W_{24}^*) = 18$ and $|E| = 24$. ∎

Using (191) and the basic properties of matroid flats, we can describe the flats of $W_{24}^*$ exactly.

(192) Theorem. (i) For $0 \leq j \leq 14$, the j-flats of $W_{24}^* = (E, \mathcal{H}^*)$ 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 of $W_{24}^*$ are just the j-subsets of E, and (i) is proved.

(193) 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 $15 \leq |F^{15}| \leq 16$. If $|F^{15}| = 16$, $F^{15}$ must be dependent, so $F^{15}$ is a circuit. If $|F^{15}| = 15$, then 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 (193), we may show that

(194) $$16 \leq |F^{16}| \leq 17.$$

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 (194), $C \cup \{x\}$ 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 (190) and the fact that the hyperplanes and circuits of $W_{24}^*$ are the complements, respectively, of the circuits and hyperplanes of $W_{24}$. ∎

(195) Theorem. For every integer $j$, $0 \leq j \leq 15$, there is a $j$-flat $F$ of $W_{24}^*$ such that $M = W_{24}^* \cdot (E-F)$ is a rank $18-j$ equicardinal matroid that is not a matroid design.

(196) Proof. Choose a hyperplane $H$ of $W_{24}^*$, where, by (192), $H = C \cup \{x,y\}$ for some circuit $C$ of $W_{24}^*$ and $x, y \in E-C$, $x \neq y$. Let $s, t \in C$ such that $s \neq t$. Suppose the set $F = (C-\{s,t\}) \cup \{x\}$ is contained in a circuit $C'$. $C' \subseteq H$ because $H$ is closed and $|C'-H| \leq 1$. If $y \in C'$, then $C-(C' \cup \{s\}) = \{t\}$, so $C \subseteq cl(C' \cup \{s\})$. But then $cl(C' \cup \{s\}) = H$, which is impossible, since by (192) $C' \cup \{s\}$ is a 16-flat. Therefore $y \notin C'$. Since $C' \subseteq H$, we must have either $s \in C'$ or $t \in C'$ (but not both). If, say, $s \in C'$, then $C'-C = \{x\}$ and so $x \in cl(C)$. But then $|cl(C)| \geq 17$, which is impossible by (192), because $cl(C)$ is a 15-flat. Therefore $s$, and likewise $t$, are not members of $C'$, and we conclude

that there is no circuit $C'$ containing $F$. Thus, $F$ is a simple 15-flat of $W_{24}^*$.

(197) Let $G_1 = (C-\{s,t\}) \cup \{x,y\} = F \cup \{y\}$. By (196), $r(G_1) = 16$. If $G_1$ is not a 16-flat, then some 15-subset $S$ of $G_1$ must be contained in a circuit. The only 15-subsets of $G_1$ are $(C-\{s,t\}) \cup \{x\} = F$, $(C-\{s,t\}) \cup \{y\}$, and $(C-\{s,t,u\}) \cup \{x,y\}$ where $u \in C$. By the argument of (196), neither of the first two are contained in a circuit. Suppose then that $S = (C-\{s,t,u\}) \cup \{x,y\}$ is contained in a circuit $C'$. If $|C'-C| = 3$, then $C'-C = \{x,y,z\}$ for some $z$ and

$$C' \cup C \subseteq cl(C \cup \{x,y\}) \subseteq cl((C-\{s\}) \cup \{x,y\}).$$

But

$$r((C-\{s\}) \cup \{x,y\}) \leq 17,$$

so

$$r(C' \cup C) \leq 17 \quad \text{while} \quad |C' \cup C| = 19,$$

which contradicts (192). The only other possibility is that $C'-C = \{x,y\}$. Then

$$C' \cup C \subseteq cl((C-\{s\}) \cup \{x\}),$$

so

$$r(C' \cup C) \leq 16 \quad \text{while} \quad |C' \cup C| = 18,$$

which again contradicts (192). Therefore $G_1$ is a simple 16-flat.

Let $G_2 = C \cup \{x\}$. $F \subseteq G_2$, and, by (192), $G_2$ is a

nonsimple 16-flat.

(198) For any $j$, $0 \leq j \leq 15$, let $F'$ be a $j$-subset of $F$, i.e., a $j$-flat contained in $F$. Then $M' = W_{24}^* \cdot (E-F')$ is a rank $18-j$ equicardinal matroid, by (38) and (39), and $G_1-F'$ and $G_2-F'$ are two $(16-j)$-flats of $M'$ having distinct cardinalities. Hence $M'$ is a rank $18-j$ equicardinal matroid that is not a matroid design.

In (195), suppose that $|F| = j \leq 3$. Since $W_{24}^*$ is a $5-(24,18,\lambda)$ design for some $\lambda$, every $5-j$ elements of $E-F$ are contained in exactly $\lambda$ hyperplanes of $W_{24}^*$ containing $F$. Hence $M = W_{24}^* \cdot (E-F)$ is a $(5-j) - (24-j, 18-j, \lambda)$ design. Therefore, for every $t$, $2 \leq t \leq 5$, there exists an equicardinal matroid that is a $t$-design, but not a matroid design.

Using matroid theory alone, the possible structures of the contractions $M = W_{24}^* \cdot (E-F)$, where $F$ is a flat of $W_{24}^*$, can be completely identified. As a way of introducing both concrete examples and general constructions of new equicardinal matroids, we shall analyze all the possible structures of $M$ if $r(M) = 3$ or $4$. (If $r(M) \leq 2$, $M$ is necessarily a trivioid.)

(199) We begin by describing a general matroid construction. Let $M = (E,\mathcal{H})$ be a rank $n$ matroid (not necessarily equicardinal), and let $\mathcal{F}_{n-2}$ 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 $\mathcal{H}' = \mathcal{H} \cup \{P(m) \cup F : F \in \mathcal{F}_{n-2}\}$ satisfies (H1) and (H2); hence $\mathcal{H}'$ is the family of hyperplanes of a matroid on the set $E' = E \cup P(m)$. $(E', \mathcal{H}')$ is called the <u>one-point extension of $M$ by $P(m)$</u>, and denoted by $M \oplus P(m)$.

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

(201) <u>Theorem</u>. 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 $PG(2,2) \oplus P(2)$, or an $EG(2,3)$.

(202) Proof. Let $F$ be a 15-flat of $W_{24}^*$, and let $M = W_{24}^* \cdot (E-F)$. By (38), $M$ has rank $r(W_{24}^*) - r(F) = 3$, and by (39) the hyperplanes of $M$ are precisely the sets of form $H-F$, where $H \in \mathcal{H}^*$ and $F \subseteq H$.

If $F$ is a circuit of $W_{24}^*$, then by (192) the hyperplanes of $W_{24}^*$ containing $F$ are precisely the sets of form $F \cup \{x,y\}$, where $x,y \in E-F$ and $x \neq y$. Hence every two distinct elements of $E-F$ are a hyperplane of $M$, and $|E-F| = 8$, so $M$ is a $\sigma(1,2,8)$.

If $F$ is not a circuit, $F$ must be a 15-subset of $E$ contained in no circuit, by (192). Hence (202) implies that $k(M) = 3$.

Suppose that $F-\{x\} \subseteq C$ for some circuit $C$ and $x \in F$. $C \cup \{x\}$ is then a 16-flat containing $F$, and hence, by (39), $P(2) = (C \cup \{x\})-F$ is a 2-point of $M$. Since $k(M) = 3$, and every two points are contained in a line (hyperplane) of $M$, all other points of $M$ are simple. It is easy to see then that the family $\mathcal{L}'$ of lines of $M$ not meeting $P(2)$ are the lines of a simple rank 3 matroid $M'$ on the set $E-(F \cup P(2))$. Since $|E-(F \cup P(2))| = 7$, $M'$ is a matroid design with d-sequence $(4,2,1)$ and hence, by (120), $M'$ is a $PG(2,2)$. It follows that $M$ is a $PG(2,2) \oplus P(2)$.

If $F-\{x\}$ is not contained in a circuit for any $x \in F$, then, by (192), every 16-flat $F^{16}$ containing $F$ must have cardinality 16. Since the points of $M$ are precisely the sets of form $F^{16}-F$, $M$ is simple. Since $r(M) = 3$, $k(M) = 3$, and $M$ contains $|E-F| = 9$ points, it follows that $M$ is a rank 3 matroid design with d-sequence $(6,2,1)$. Therefore, by (125), $M$ is an $EG(2,3)$. ∎

(203) $PG(2,2) \oplus P(2)$ is shown in Fig. 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.

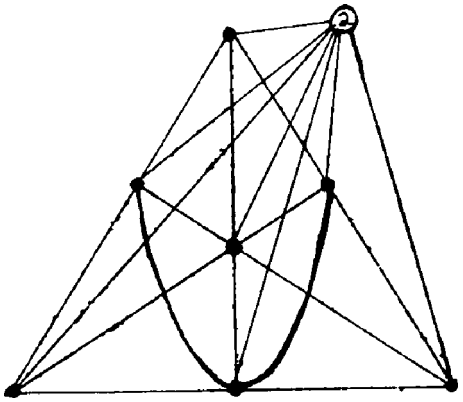


Fig. 1-- The equicardinal matroid $PG(2,2) \oplus P(2)$

As a preliminary to studying the higher rank contractions of $W_{24}^*$, we shall give a special construction of a simple rank 4 equicardinal matroid that is not a matroid design. This is the simplest example of such a matroid known to us.

(204) 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 $P_i$ are mutually disjoint for each $i$, $1 \leq i \leq 3$. 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

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

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

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

and

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

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

Representative lines and planes of $\mathcal{V}$ are shown in Fig. 2.

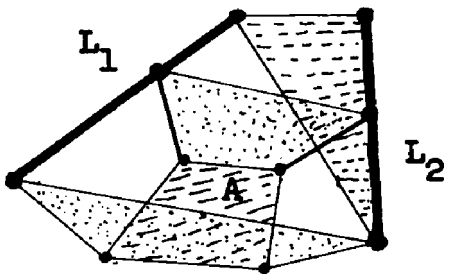



Fig. 2-- The equicardinal matroid $\mathcal{V}$

(205) Theorem. $\Psi$ is the unique simple equicardinal matroid with 10 points and hyperplane cardinality 4 that is not a matroid design.

Proof. Let $M = (E,\mathcal{H})$ be a simple equicardinal matroid such that $|E| = 10$ and $k(M) = 4$.

The rank of the hyperplanes of $M$ cannot exceed 4, since $k(M) = 4$. If the hyperplanes of $M$ had rank 4, then for $0 \leq j \leq 4$ all the $j$-flats would have cardinality $j$, and $M$ would be a matroid design. If the hyperplanes of $M$ had rank 2 or less, then, because $M$ is simple, $M$ would again be a matroid design. Therefore the rank of the hyperplanes is 3, and $r(M) = 4$.

Clearly, the lines of $M$ cannot have cardinality greater than 3. Since, by assumption, $M$ is not a matroid design, it follows that some of the lines of $M$, say $L_1, L_2, \cdots, L_t$ have cardinality 3, and the rest have cardinality 2 (i.e., are simple).

Suppose that two lines of cardinality 3, $L_i$ and $L_j$, have a nonempty intersection. Then $r(L_i \cup L_j) = 3$ and $cl(L_i \cup L_j)$ is a hyperplane. But this is impossible, because $|cl(L_i \cup L_j)| \geq |L_i \cup L_j| = 5 > k(M)$. Hence the lines $L_1, L_2, \cdots, L_t$ are disjoint, and, since $|E| = 10$, we must have $t \leq 3$.

Suppose that $t = 3$. Let $E = \{x\} \cup (L_1 \cup L_2 \cup L_3)$,

and $L_i = \{e_1^i, e_2^i, e_3^i\}$, $i = 1,2,3$, where $L_i \cap L_j = \emptyset$ if $i \neq j$. The sets $\{e_1^1, e_1^2, e_1^3\}$, $\{e_1^1, e_1^2, e_2^3\}$, $\{e_1^1, e_1^2, e_3^3\}$ have rank 3, and hence each determines a hyperplane; call them $H_1$, $H_2$, and $H_3$. For each $i$ and $j$, $1 \leq i,j \leq 3$, $|H_j \cap L_i| \geq 1$ by construction, but if $|H_j \cap L_i| \geq 2$ we would have $L_i \subseteq H_j$ and $|H_j| \geq 5$, a contradiction to the hypothesis that $k(M) = 4$. Hence $|H_j \cap L_i| = 1$ for $1 \leq i,j \leq 3$. But then $|H_1| = |H_2| = |H_3| = 4$ implies that $x \in H_j$ for each $j$, $1 \leq j \leq 3$. Therefore $\{x, e_1^1, e_1^2\} \subseteq H_1 \cap H_2 \cap H_3$, and so

$$r(\{x, e_1^1, e_1^2\}) \leq r(H_1 \cap H_2 \cap H_3) < r(H_1) = 3,$$

which implies that $\{x, e_1^1, e_1^2\}$ is contained in a line of cardinality 3. Since $L_1$, $L_2$, and $L_3$ are the only lines of cardinality 3, we have reached a contradiction. Hence $t \leq 2$.

(206) Suppose that $t = 1$. Let $L_1 = \{e_1, e_2, e_3\}$ be the unique line of cardinality 3, and let $A = E - L_1$. For any $x \in A$, the lines containing $x$ are all simple, and the hyperplanes all have cardinality 4. Hence $M_x = M \cdot (E-\{x\})$ is a rank 3 matroid design with d-sequence (6,2,1). Therefore, by (125), $M_x$ is an EG(2,3) for each $x \in A$. Further, since

$L_1 \cup \{x\} \in \mathcal{H}$ for each $x \in A$, $L_1$ is a line of $M_x$. Let $L_2^x$, $L_3^x$ be the lines of $M_x$ parallel to $L_1$. Then $L_2^x \cup \{x\}$ and $L_3^x \cup \{x\}$ are precisely the hyperplanes of $M$ containing $x$ and wholly contained in $A$. Since this argument holds for any $x \in A$, we conclude that each element of $A$ is contained in exactly two hyperplanes of $M$ that are subsets of $A$. Therefore $A$ contains $\frac{2 \cdot 7}{4}$ hyperplanes of $M$, which is no integer, and a contradiction has been reached.

(207) Thus $M$ contains exactly two disjoint lines of cardinality 3; call them $L_1$ and $L_2$. Let $A = E-(L_1 \cup L_2)$, and let $x \in A$. Then, as in (206), $M_x = M \cdot (E-\{x\})$ is an $EG(2,3)$, and $L_1$ and $L_2$ are lines of $M_x$. Since $L_1 \cap L_2 = \emptyset$, $L_1$ and $L_2$ determine a parallel class of $M_x$, and $A-\{x\}$ must be the third member of this class. Thus $A-\{x\}$ is a hyperplane (line) of $M_x$, so $A$ is a hyperplane of $M$.

(208) Consider any two disjoint pairs $\{a_1, a_2\} = p_1$ and $\{a_3, a_4\} = p_2$ of elements of $A$; they are, in particular, lines of $M$. For each $i$, $i = 1,2$, let $H_1^i$, $H_2^i$, $H_3^i$ be the hyperplanes of $M$ distinct from $A$ containing $p_i$. For given $i$, the sets $q_1^i = H_1^i - p_i$, $q_2^i = H_2^i - p_i$, $q_3^i = H_3^i - p_i$ are

disjoint, by (15), and $|q_j^i| = 2$ for each $q_j^i$. Further, no $q_j^i$ is a subset of $L_1$ or $L_2$. Otherwise, if (say) $q_j^i \subseteq L_1$, then $|H_j^i \cap L_1| \geq 2$ and $L_1 \subseteq H_j^i$. But then $|H_j^i| \geq |L_1 \cup p_i| = 5$, a contradiction. It follows that, for each $i$, $i = 1,2$, the pairs $q_1^i$, $q_2^i$, $q_3^i$ are disjoint and of the form $\{x,y\}$, where $x \in L_1$, $y \in L_2$.

(209) Let $P^i = \{q_1^i, q_2^i, q_3^i\}$, $i = 1,2$. We claim that $P^1 = P^2$. Suppose not; then we may assume that, say, $|q_1^1 \cap q_1^2| = 1$ Let $\{x\} = q_1^1 \cap q_1^2$. Choose $y \in p_1$, and let $H = c\ell(\{y\} \cup q_1^2)$. Since $|H| = 4$ and $H$ meets each of $L_1$, $L_2$, and $A$, $H$ cannot contain either $L_1$ or $L_2$. Hence $H \cap (L_1 \cup L_2) = q_1^2$. Since $y \in H - H_1^2$, $H \neq H_1^2$, so $H \cap H_1^2 = q_1^2$. Thus $H - q_1^2$ and $H_1^2 - q_1^2 = p_2$ are disjoint, which implies that $H - q_1^2 = p_1$. But then $H \cap H_1^1 \supseteq \{x\} \cup p_1$ and $H \neq H_1^1$ a contradiction, since $\{x\} \cup p_1$ is not a line. Thus, $P^1 = P^2$.

From (208) and (209) it follows that for every pair $\{p_1, p_2\}$ of disjoint lines contained in $A$, there is a triple $\{q_1, q_2, q_3\}$ of disjoint simple lines of form $\{x,y\}$, $x \in L_1$, $y \in L_2$, such that $p_i \cup q_j$ is a hyperplane, for every pair $i$ and $j$, $i = 1,2$, $j = 1,2,3$. Further, it is easy to see that

for disjoint pairs $\{p_1, p_2\}$ and $\{p_1', p_2'\}$ of lines in A, the corresponding triples $\{q_1, q_2, q_3\}$ and $\{q_1', q_2', q_3'\}$ are disjoint. Hence M is isomorphic to $\mathfrak{V}$ as defined in (204).∎

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

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

or (ii) $\mathfrak{V}$

or (iii) IP(3).

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

Proof.

(211) Let F be a 14-subset of some circuit C of $W_{24}^*$. $M = W_{24}^* \cdot (E-F)$ is then a rank 4 equicardinal matroid and $k(M) = 4$. Further, $C-F = P(2)$ is a 2-point of M. Let $A = E-C$, and let $\mathfrak{L}'$ denote the lines of M contained in A, $\mathfrak{H}'$ the hyperplanes of M contained in A. Every line of M is properly contained in a hyperplane of M, hence every line has cardinality 3 or less. Thus, if x and y are distinct points of A, then $L_{xy} \cap P(2) = \emptyset$; i.e., $L_{xy} \subseteq A$. In fact, $L_{xy} = \{x,y\}$. Otherwise, we would have $|L_{xy}| \geq 3$ and $|cl(L_{xy} \cup P(2))| \geq 5$, which is impossible, because $cl(L_{xy} \cup P(2))$

is a hyperplane of M. In summary, the members of $\mathfrak{L}'$ are all simple lines, and every two distinct points of A are contained in a unique member of $\mathfrak{L}'$.

(212) For any $L \in \mathfrak{L}'$ and $x \in A-L$, $cl(L \cup \{x\}) = H \in \mathcal{H}$ and $H \cap P(2) = \emptyset$ (since $|H| = 4$); hence $H \in \mathcal{H}'$.

It follows easily from (211) and (212) that $(A,\mathcal{H}')$ satisfies (H1) and (H2), and hence is a matroid -- in fact, it is a matroid design. Let $M' = (A,\mathcal{H}')$. All points and lines of $M'$ are simple, the hyperplanes have cardinality 4, and $|A| = 8$. Therefore $d(M') = (4,2,1,1)$. By (125), $M'$ must be an $EG(3,2)$. But $M = M' \oplus P(2)$; hence M is an $EG(3,2) \oplus P(2)$.

(213) For any 14-flat F of $W_{24}^*$, $M_F = W_{24}^* \cdot (E-F)$ is a rank 4 equicardinal matroid on a set of $|E-F| = 10$ elements, with hyperplane cardinality $k(M_F) = k(M)-|F| = 4$. Hence $c^*(M_F) = 6$. If $M_F$ is a simple matroid design, then

$$d(M_F) = (6, d_3, d_2, 1), \text{ where } 6 + d_3 + d_2 + 1 = 10.$$

Further, (D2) implies that $\frac{6}{d_3} \geq \frac{d_3}{d_2}$. Hence $d(M_F)$ can only be (6,2,1,1). It follows from (55) that $M_F$ is a 3-(10,4,1) design. Moreover, it has been shown by Witt [19] that the inversive plane IP(3) of the type described in (58) is the unique matroid design with this d-sequence.

(214) Now let C be a circuit of $W_{24}^*$, let $x \in E-C$, and

let $S$ be a 13-subset of $C$. Put $F = S \cup \{x\}$, and $M = W_{24}^* \cdot (E-F)$. If $F$ is contained in some circuit $C'$, then $C' \neq C$ (since $F \not\subseteq C$) and $r(C' \cup C) \leq 17$. But then $cl(C' \cup C)$ is a proper flat of $W_{24}^*$ containing two distinct circuits, which is impossible by (192). Therefore $F$ is contained in no circuits, so the 15-flats of $W_{24}^*$ that contain $F$ must be simple. Since the points of $M$ are just the subsets of form $F^{15}-F$, where $F^{15}$ is a 15-flat of $W_{24}^*$ containing $F$, it follows that $M$ is simple.

(215) By (192), $F^{16} = C \cup \{x\}$ is a 16-flat of $W_{24}^*$ containing $F$; hence $F^{16} - F = L$ is a line of $M$, and $|L| = 3$. If $M$ were a matroid design, then, by (213), it would be IP(3), every line of which has cardinality 4. Therefore $M$ is not a matroid design, so, by (205), $M$ is $\Upsilon$.

Finally, we shall show the existence of a 14-flat $F$ of $W_{24}^*$ such that $W_{24}^* \cdot (E-F)$ is IP(3). The easiest proof is somewhat indirect.

Suppose that every 13-subset of $E$ is contained in a circuit. There are $\binom{24}{13}$ 13-subsets of $E$, and each circuit contains $\binom{16}{13}$ 13-subsets, so under our hypothesis there must be at least $\gamma = \frac{\binom{24}{13}}{\binom{16}{13}}$ circuits. But the number of circuits of

$W_{24}^*$ is precisely the number $\delta$ of hyperplanes of $W_{24}$. Since every hyperplane has cardinality 8, and every 5-subset of E is contained in exactly one hyperplane $\delta = \frac{\binom{24}{5}}{\binom{8}{5}}$. A simple computation shows that $\delta < \gamma$, a contradiction.

Therefore let T be a 13-subset of E contained in no circuit. Let $M = W_{24}^* \cdot (E-T)$, and for each $x \in E-T$, let $M_x = W_{24}^* \cdot (E-(TU\{x\}))$. By assumption, $TU\{x\}$ is contained in no circuits, that is, the 15-flats containing $TU\{x\}$ are simple. Hence $M_x$ is simple for every $x \in E-T$. Since $TU\{x\}$ is a 14-flat of $W_{24}^*$, it follows from (211) - (215) that $M_x$ is $\Upsilon$ or IP(3) for every $x \in E-T$.

Suppose that $M_x$ is $\Upsilon$ for every $x \in E-T$. Then for every given x, $M_x$ contains exactly two lines $L_1$ and $L_2$ of cardinality 3. Equivalently, by (39), $TU\{x\}$ is contained in exactly two 16-flats of $W_{24}^*$ having cardinality 17; or, equivalently, x is contained in exactly two 3-flats <u>of</u> <u>M</u> having cardinality 4. Since this holds for every $x \in E-T$, and $|E-T| = 11$, M must contain exactly $\frac{2 \cdot 11}{4}$ 3-flats having cardinality 4, which is no integer. This is a contradiction; hence for some $x' \in E-T$, $M_{x'} = W_{24}^* \cdot (E-TU\{x'\})$ is IP(3), and $TU\{x'\}$ is the required 14-flat. ∎

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 equicardinal matroids, we shall present one example of a simple rank 5 equicardinal matroid 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 $\Phi = (E', \mathcal{H}')$, and we describe it as follows.

(216) $|E'| = 11$, and all points of $\Phi$ are simple. $\Phi$ has one line of cardinality 3, $L = \{a,b,c\}$, and all other lines are simple. The remaining eight points of $\Phi$ are divided into two disjoint 3-flats having 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.

(217) $k(\Phi) = 5$. In particular, $\mathcal{H}_1' = \{\{x\} \cup F_i^3 : i=1 \text{ or } i=2 \text{ and } x \in E'-F_i^3\}$ is the collection of hyperplanes containing $F_1^3$ and $F_2^3$. Likewise, $\mathcal{H}_2' = \{\{x,y\} \cup L : x,y \in E'-L \text{ and } x \neq y\}$ is the collection of hyperplanes containing $L$.

(218) 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 $\mathcal{H}_x'$ of hyperplanes containing $x$ but not $L$, when

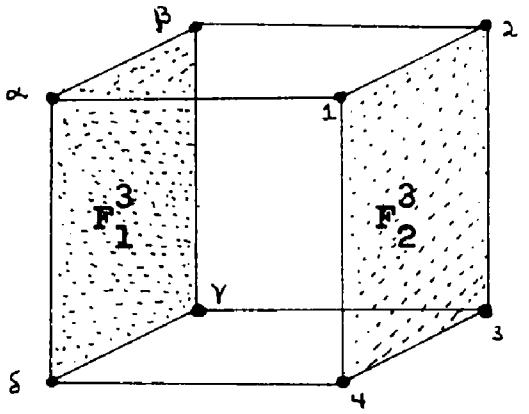
restricted to the set E-L, form an EG(3,2) on E-L. In particular, $F_i^3 \cup \{x\} \in \mathcal{H}'_x$ for $i = 1,2$ and each $x \in L$.

Let $\mathcal{H}''_x = \{H-\{x\}: H \in \mathcal{H}'_x\}$ for each $x \in L$ $x = a,b,c$. By (218), $F_i^3 \in H''_x$ 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 $\mathcal{H}''_x$, because they are the only 3-flats of $\mathcal{H}$ having cardinality 4 and contained in E-L.

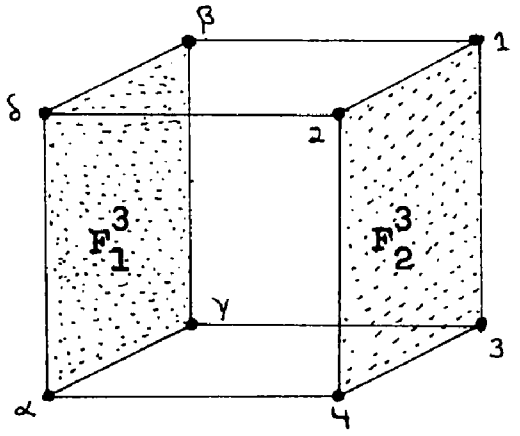
Thus, for $x = a,b,c$, the pairs $(E-L, \mathcal{H}''_x)$ constitute three copies of EG(3,2) on the set E-L, each containing $F_1^3 = \{\alpha,\beta,\gamma,\delta\}$ and $F_2^3 = \{1,2,3,4\}$ as their only common hyperplanes. Up to isomorphism there is only one way in which three sets of hyperplanes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

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

(a)




(b)




(c)

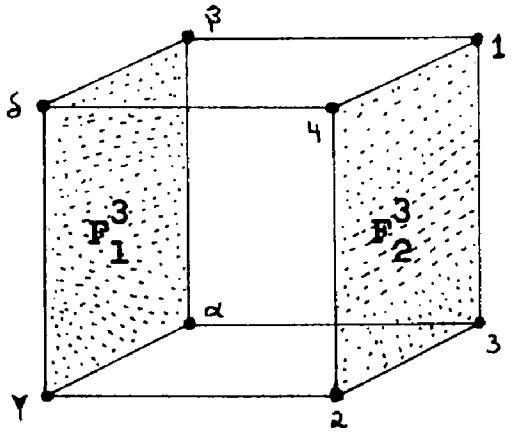



Fig. 3-- Three copies of EG(3,2) containing exactly two parallel hyperplanes in common.

For each $x$, $x = a,b,c$, adjoin the elements $x$ to each of the sets in list $(x)$, and let $\mathcal{H}_3'$ be the resulting collection of 5-subsets of $E'$. We claim that $\mathcal{H}' = \mathcal{H}_1' \cup \mathcal{H}_2' \cup \mathcal{H}_3'$ is the hyperplane - family of the matroid $\Phi$ having points, lines and 3-flats as described in (216). To show that $(E',\mathcal{H}')$ 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 $j \leq 3$; and (ii) that for $0 \leq j \leq 3$ 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.

## 4.2 The characterization problem

The preceding examples were presented in some detail to suggest the variety of equicardinal matroids that are not matroid designs. However, equicardinal matroids are still such highly regular objects that it is often possible to completely describe the structure of an equicardinal matroid with given rank and co-circuit cardinality. This problem in its generality will be called the characterization problem for equicardinal matroids.

We shall first observe that to describe the possible structures of equicardinal matroids, we will not sacrifice any substantial results by restricting our attention to connected equicardinal matroids. Indeed, by (52), every component of an equicardinal matroid is equicardinal, and it was observed

in (51) that the components of a matroid determine the matroid completely. Thus we define $\underline{\mathfrak{m}_n(\gamma)}$ for positive integers $n$ and $\gamma$ to be the family of all connected equicardinal matroids $M$ such that $r(M) = n$ and $c^*(M) = \gamma$. We shall seek to characterize $\mathfrak{m}_n(\gamma)$ for various values of $n$ and $\gamma$.

(219) Theorem. Let $M = (E, \mathcal{H})$ be a matroid with co-circuit family $C$. Then $M$ is connected if and only if for every distinct $x,y \in E$ there exists $C \in C$ such that $x,y \in C$.

Proof. Let $R$ be the relation on the set $E$ defined such that $x\ R\ y$ if and only if $x = y$ or there exists $C \in C$ such that $x,y \in C$. We shall show that $R$ is an equivalence relation. It is obvious that $R$ is reflexive and symmetric. Suppose that $R$ is not transitive; that is, suppose that for some $\{x,y\} \subseteq C_1$ and $\{z,y\} \subseteq C_2$ there is no $C \in C$ such that $\{x,z\} \subseteq C$. Let $|C_1 \cup C_2|$ be a minimum among all circuit pairs $(C_1,C_2)$ such that for any $\{x,y\} \subseteq C_1$ and $\{y,z\} \subseteq C_2$ $\{x,z\}$ is contained in no member of $C$. By the Circuit Axiom (C2) of (14), there exists $C_3 \in C$ such that $x \in C_3 \subseteq C_1 \cup C_2 - \{y\}$, and, by (C1), there exists $w \in C_3 \cap (C_2 - C_1)$. Likewise, there exists $C_4 \in C$ such that $z \in C_4 \subseteq C_1 \cup C_2 - \{y\}$ and there exists $v \in C_4 - C_2$.

Now $C_3 \cup C_4 \subseteq C_1 \cup C_2 - \{y\}$, and so $|C_3 \cup C_4| < |C_1 \cup C_2|$. Hence $C_3 \cap C_4 = \emptyset$, by the choice of $C_1$ and $C_2$. In particular, $v \in C_1 - (C_3 \cup C_2)$, and hence $C_3 \cup C_2 \subseteq C_1 \cup C_2 - \{v\}$;

that is, $|C_3 \cup C_2| < |C_1 \cup C_2|$. But $\{x,w\} \subseteq C_3$ and $\{w,z\} \subseteq C_2$, so by the minimality hypothesis on $|C_1 \cup C_2|$, there exists $C \in \mathcal{C}$ such that $\{x,z\} \subseteq C$. This contradicts the choice of $C_1$ and $C_2$, and hence $R$ is transitive.

Clearly, every equivalence class of $R$ is a separator of $M$, and every nonempty separator of $M$ contains an equivalence class of $R$. Hence $R$ contains only one equivalence class if and only if $M$ is connected, and the theorem follows.∎

We shall sometimes use (219) in the equivalent formulation: $M = (E,\mathcal{H})$ is connected if and only if for every distinct $x,y \in E$, there exists $H \in \mathcal{H}$ such that $x,y \notin H$.

(220) By (39), for any subset $A$ of $E$, the hyperplanes of $M \cdot (E-A)$ are precisely the sets of form $H-A$ where $H$ is a hyperplane of $M$ containing $A$. Therefore, the co-circuits of $M \cdot (E-A)$ are precisely the co-circuits of $M$ not meeting $A$. In particular, $c^*(M) = c^*(M \cdot (E-A))$. We also recall from (110) that every co-circuit is partitioned by the points that meet it.

The following theorem expresses a special property of connected equicardinal matroids, and provides a very useful tool for characterizing equicardinal matroids having a given co-circuit cardinality.

(221) Theorem. If $M$ is a connected equicardinal matroid and $F$ is a $j$-flat of $M$ $(0 \leq j \leq n)$, then $M \cdot (E-F)$ is a connected equicardinal matroid.

Proof. That $M \cdot (E-F)$ is an equicardinal matroid follows at once from (220). The essence of the theorem is that connectivity is preserved under the contraction of an equicardinal matroid to the complement of a flat.

(222) Suppose that (221) has been proved whenever $r(F) < j$, where $2 \leq j \leq n$, and let $F^j$ be a $j$-flat of $M$. Where $F^{j-1}$ is a $(j-1)$-flat contained in $F^j$, we have

$$M \cdot (E-F^j) = (M \cdot (E-F^{j-1})) \cdot (E-F^j),$$
$$= (M \cdot (E-F^{j-1})) \cdot ((E-F^{j-1}) - (F^j-F^{j-1})).$$

(223) Now $M \cdot (E-F^{j-1})$ is connected, by the induction hypothesis (222), and $F^j-F^{j-1}$ is a point of $M \cdot (E-F^{j-1})$. Hence $M \cdot (E-F^j)$ is connected, again by (222).

(224) Therefore, it suffices to prove (221) when $F$ is a point of $M$. (If $F$ is a 0-flat there is nothing to prove.)

(225) Let $F$, then, be a point of $M$, and let $c^*(M) = \gamma$. We shall show that for every $x,y \in E-F$, $x \neq y$, there is a cocircuit $C$ such that $\{x,y\} \subseteq C$ and $C \cap F = \emptyset$. It will follow then, by (219) and (220), that $M \cdot (E-F)$ is connected.

With $x,y$, and $F$ as above, $2 \leq r(F \cup \{x,y\}) \leq 3$, since $F$ is closed and $r(F) = 1$. If $r(F \cup \{x,y\}) = 2$, then

for any $w \in F$, $\{w,x\}$ is a basis of $FU\{x,y\}$. Where $B$ is any basis of $M$ containing $\{w,x\}$, $cl(B-\{x\}) = H$ is a hyperplane containing $F$, but $y \notin H$ because $x$ depends on $\{w,y\}$ and $x \notin H$. Therefore $E-H$ is a co-circuit as required by (225).

We may suppose then that $r(FU\{x,y\}) = 3$, i.e., that $\{w,x,y\}$ is independent for any $w \in F$. We shall show the existence of two co-circuits $C_1$ and $C_2$ such that $\{x,y\} \subseteq C_1 \cup C_2 - C_1 \cap C_2$ and $F \subseteq C_1 \cap C_2$. If $x,y$, and $F$ are contained in some common co-circuit, $C_1$, choose $w \in F$, and let $B$ be a basis of $M$ extending $\{w,x,y\}$. Then we take $H = cl(B-\{w\})$ and $C_2 = E-H$. If $x,y$, and $F$ are contained in no common co-circuit, we let $C_1$ and $C_2$ be co-circuits containing $\{x\} \cup F$ and $\{y\} \cup F$ respectively (using (219), (220), and the hypothesis that $M$ is connected).

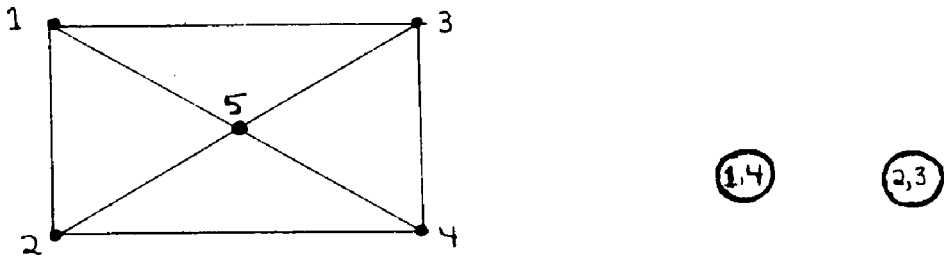
With $C_1$ and $C_2$ as above, there exist, by (C2), co-circuits $C_x$ and $C_y$ such that $x \in C_x \subseteq C_1 \cup C_2 - F$ and $y \in C_y \subseteq C_1 \cup C_2 - F$. Thus $C_x \cup C_y \subseteq C_1 \cup C_2 - F$; since $|C_x| = |C_y| = |C_1| = |C_2| = \gamma$ and $F \neq \emptyset$, we must have $C_x \cap C_y \neq \emptyset$. But then $M' = M \cdot (C_x \cup C_y)$ is connected. Thus, by (219), there is a co-circuit $C$ of $M'$ containing $x$ and $y$, and, by (220), $C$ is a co-circuit of $M$ disjoint from $F$. ∎

(226) Corollary. If $M \in \mathfrak{M}_n(\gamma)$ and $F$ is a $j$-flat of $M$, then $M \cdot (E-F) \in \mathfrak{M}_{n-j}(\gamma)$.

This result follows at once from (38), (220), and (221).

The contraction, $M \cdot (E-F)$, of a matroid $M$ to the complement in $E$ of a flat $F$ will be called the contraction of $M$ at $F$. We shall sometimes abbreviate $M \cdot (E-F)$ to $M_F$ in this case.

In general, it is not true that the contraction at a flat of a connected matroid is again connected. In Fig. 4 we show a connected rank 3 matroid $M$ on five points, and the contraction of $M$ at $\{5\}$, which is not connected.




M  M · {1,2,3,4}

Fig. 4-- A connected matroid having a disconnected contraction

The trivioids of a given rank and co-circuit cardinality are particularly easy to characterize, as we shall now show.

(227) Theorem. For any positive integers $n$ and $\gamma$, the trivioids in $\mathfrak{M}_n(\gamma)$ are precisely the trivioids of form $\sigma(\alpha, n-1, \frac{\gamma}{\alpha} + n-1)$, where $\alpha | \gamma$ and $\alpha < \gamma$.

Proof. Let $M = (E,\mathcal{H})$ be a trivioid contained in $\mathbb{m}_n(\gamma)$, and let $\alpha$ be the common cardinality of the points of $M$. Every $n-1$ distinct points of $M$ constitute a hyperplane of $M$. Further, every co-circuit is partitioned by the points that meet it, so $\alpha | c^*(M) = \gamma$. Thus $M$ contains $\frac{\gamma}{\alpha} + n - \gamma$ points in all, so $M$ is a $\sigma(\alpha, n-1, \frac{\gamma}{\alpha} + n - 1)$.

If $\alpha = \gamma$, then the complement of every hyperplane is a point, so, by (49), $M$ would be disconnected, which is contrary to hypothesis. Thus $\alpha < \gamma$.

Conversely, if $\alpha | \gamma$ and $\alpha < \gamma$, it is easily seen that every $\sigma(\alpha, n-1, \frac{\gamma}{\alpha} + n - 1)$ is in $\mathbb{m}_n(\gamma)$. ∎

Our next two theorems establish conditions under which an equicardinal matroid is a trivioid.

(228) For any matroid $M = (E,\mathcal{H})$ we let $\underline{P(M)}$ denote the set of points of $M$. Where $A \subseteq E$, $\underline{P(A)}$ shall denote the set of points of $M$ contained in $A$.

(229) Theorem. Let $M = (E,\mathcal{H})$ be a connected equicardinal matroid. If for some point $b$ of $M$, $M \cdot (E-b)$ is a $(|b|, -, -)$-trivioid and $P(M \cdot (E-b)) \subseteq P(M)$, then $M$ is a $(|b|, -, -)$-trivioid.

Proof. Let $M \cdot (E-b)$ be a $(|b|, k', v')$-trivioid. We shall show that for every set $W$ of $k' + 1$ distinct points of $M$,

$$\bigcup_{X \subseteq W} X \in \mathcal{H}.$$

(230) If $b \in W$, then $W-\{b\}$ is a set of $k'$ points of $M \cdot (E-b)$, so $\bigcup_{X \in W-\{b\}} X$ is a hyperplane of $M \cdot (E-b)$, and thus $\bigcup_{X \in W} X$ is a hyperplane of $M$.

(231) If $b \notin W$, let $H$ be a hyperplane of $M$ not containing $b$ such that $|P(H) \cap W|$ is a maximum. There is such a hyperplane because $b$ is not a separator of $M$ (unless $r(M) = 1$, in which case $E = b$ and $M$ is a $(|b|,0,1)$-trivioid).

(232) Suppose that $c \in W-P(H)$ for some point $c$. Since $|P(H)| = |W| = k' + 1$, there is a point $d \in P(H)-W$, and thus $W' = P(H) \cup \{b\} - \{d\}$ has cardinality $k' + 1$. Then $H' = \bigcup_{X \in W'} X$ is a hyperplane of $M$, by (230). From $(H2)'$ we conclude that there is a hyperplane $H''$ of $M$ such that $H'' \supseteq c \cup (H' \cap H)$ and $b \cap H'' = \emptyset$. But then $|W \cap P(H'')| > |W \cap P(H)|$, contradicting the choice of $H$. Therefore $W-P(H) = \emptyset$; that is, $H = \bigcup_{X \in W} X$. ∎

(233) In (44) we defined a simple $j$-flat of a matroid to be a $j$-flat having cardinality $j$. We say that a $j$-flat is <u>elementary</u> if it contains precisely $j$ points of the matroid.

(234) <u>Theorem</u>. Let $M = (E,\mathcal{H})$ be a connected, nontrivial equicardinal matroid. If there exist two distinct points

$a_1$ and $a_2$ of $M$ such that $M \cdot (E-a_1)$ and $M \cdot (E-a_2)$ are trivial, then $r(M) = 3$. Conversely, if $r(M) = 3$ then $M \cdot (E-a)$ is trivial for every point $a$ of $M$.

Proof. Let $M = (E,\mathcal{H})$ be a connected, equicardinal matroid and suppose that $r(M) = 3$. Let $a$ be any point of $M$ and let $M' = M \cdot (E-a)$. Then $r(M') = 2$, so the hyperplanes of $M'$ are its points, and each has cardinality $\alpha = k(M) - |a|$. Thus $M'$ is an $(\alpha, 1, |\underline{E-a}|)$-trivioid.
$\alpha$

Conversely, suppose that $M$ is a nontrivial connected equicardinal matroid such that $k(M) = k$, and $M_i = M \cdot (E-a_i)$ is a trivioid for distinct points $a_i$ of $M$, $i = 1,2$. Let the points of $M_i$ have cardinality $s_i$. $r(M) = n \geq 3$, since every equicardinal matroid of rank less than 3 is trivial. (235) Let $\mathcal{L}_i$ be the set of lines of $M$ containing $a_i$, for $i = 1,2$, and let $L_{12}$ be the unique line containing $a_1 \cup a_2$. By (39), the points of $M_i$ are precisely the sets of form $L-a_i$, where $L \in \mathcal{L}_i$. Hence $|L-a_i| = s_i$ for every $L \in \mathcal{L}_i$, and the union of every $n-2$ distinct sets of the form $L-a_i$ is a hyperplane of $M_i$. Therefore, by (39), the union of every $(n-2)$ distinct members of $\mathcal{L}_i$ is a hyperplane of $M$, so

(236) $(n-2)\, s_1 + |a_1| = (n-2)\, s_2 + |a_2| = k$.

(237) Further, since the hyperplanes are proper subsets of E, each $\mathfrak{L}_i$ contains at least (n-1) lines, and the members of $\mathfrak{L}_i$ are themselves proper subsets of E.

(238) Let us now assume, contrary to the theorem, that $r(M) = n \geq 4$. Suppose in addition that for some line $L_o \in \mathfrak{L}_2$ different from $L_{12}$, $L_o$ contains three distinct points $a_2$, b, and c. Since $L_o \neq L_{12}$, $a_1 \not\subseteq L_o$, so every point a of $L_o$ is the intersection of $L_o$ with a unique line $L_a \in \mathfrak{L}_1$. Let $L_b$ and $L_c$ be the lines of $\mathfrak{L}_1$ corresponding to b and c in this way. Then, by (237), there exists on (n-2)-subset $\mathfrak{L}'$ of $\mathfrak{L}_1$ containing $L_b$ and $L_c$ and omitting $L_{12}$. Hence $H = \bigcup_{L \in \mathfrak{L}'} L \in \mathfrak{H}$ and H contains $b \cup c$, but $H \cap a_2 = \emptyset$, so H does not contain $L_o = c\ell(b \cup c)$, which is absurd. Hence, if $n \geq 4$, every line in $\mathfrak{L}_2 - \{L_{12}\}$ is elementary. Likewise, every line in $\mathfrak{L}_1 - \{L_{12}\}$ is elementary.

(238a) Where b is any point of M not contained in $L_{12}$, (238) implies that $a_1 \cup b$ and $a_2 \cup b$ are lines of M contained in $\mathfrak{L}_1$ and $\mathfrak{L}_2$, respectively. Hence b is a point of $M_1$ and of $M_2$. Therefore $s_1 = s_2 = |b|$, so (236) implies that $|a_1| = |a_2|$. Let $s_1 = s_2 = s$, $|a_1| = |a_2| = \alpha$.

Since every hyperplane of M contains at least n-1 points, and since, by (220) and the assumption that M is

connected, there exists a hyperplane of $M$ disjoint from $a_1 \cup a_2$, it follows from (238a) that $(n-1)s \leq k$. By (236), $(n-2)\,s + \alpha = k$, and so $s \leq \alpha$. On the other hand, $a_2 \subseteq L_{12} - a_1$, and so $\alpha = |a_2| \leq |L_{12} - a_1| = s$. Therefore $\alpha = s$, and $L_{12} = a_1 \cup a_2$. Hence $M \cdot (E-a_1)$ is an $(|a_1|,-,-)$-trivioid whose points are points of $M$, so $M$ is an $(|a_1|,-,-)$-trivioid, by (229), (contrary to our hypothesis on $M$. Therefore $r(M) = 3$. ∎

(239) Theorem. If, for some $n \geq 1$ and $\gamma \geq 1$, there exists a nontrivial matroid $M \in \mathfrak{m}_n(\gamma)$, then for every $m$, $3 \leq m \leq n$, there exists a nontrivial matroid $M_m \in \mathfrak{m}_m(\gamma)$.

Proof. Let $m$ be the greatest integer such that $m \leq n$ and $\mathfrak{m}_m(\gamma)$ contains a nontrivial member $M_m = (E_m, \mathcal{H}_m)$ and every member of $\mathfrak{m}_{m-1}(\gamma)$ is trivial. By (226), $M_m \cdot (E_m - a) \in \mathfrak{m}_{m-1}(\gamma)$ for every point $a$ of $M_m$. Hence, by (234), $r(M_m) = 3$, that is, $m = 3$. ∎

## 4.3 A diophantine analysis of rank 3 equicardinal matroids

(240) Every connected rank 1 equicardinal matroid is a trivioid, since $\emptyset$ is the only hyperplane. Likewise every connected rank 2 equicardinal matroid is a trivioid, for the hyperplanes are identical with the points. Therefore, for every

$\gamma$, $\mathfrak{m}_1(\gamma) \cup \mathfrak{m}_2(\gamma)$ contains only trivial matroids.

(241) From (239) and (240) it follows that if, for some $\gamma$, $\mathfrak{m}_3(\gamma)$ contains only trivioids, then $\bigcup_{n=1}^{\infty} \mathfrak{m}_n(\gamma)$ contains only trivioids. More generally, if $\mathfrak{m}_3(\gamma)$ contains only a few non-isomorphic matroid structures, then it is frequently possible to describe completely all members of $\mathfrak{m}_n(\gamma)$ for $n \geq 3$. We therefore turn our attention to the analysis of rank 3 connected equicardinal matroids.

For a given co-circuit cardinality $\gamma$, let $M = (E,\mathfrak{H})$ $\in \mathfrak{m}_3(\gamma)$, and let $k(M) = k$.

(242) For any point $a$ of $M$, let $\mathfrak{H}_a$ denote the set of lines (i.e., hyperplanes) of $M$ containing $a$. By (15), the sets $H-a$ such that $H \in \mathfrak{H}_a$ partition $E-a$, and hence $(k-|a|) \mid (|E|-|a|)$, or, noting that $|E|-k = \gamma$, $(k-|a|) \mid \gamma$.

(243) Suppose that $k-|a| = \gamma$ for some point $a$. Then $\frac{|E|-|a|}{k-|a|} = 2$, so $a$ is contained in precisely two lines of $M$, say $H_1$ and $H_2$. Let $P(H_1) = \{a,a_1,\cdots,a_u\}$ and $P(H_2) = \{a,b_1,\cdots,b_u\}$. $H_1$ and $H_2$ are lines whose union is $E$, and since every two points are contained in a unique line, $a_i \cup b_j$ is a line for every $i$ and $j$. Thus

(244) $k = |a| + \sum_{i=1}^{u} |a_i| = |a| + \sum_{j=1}^{v} |b_j| = |a_i| + |b_j|,$

for $1 \leq i \leq u$, $1 \leq j \leq v$.

From (244) it follows readily that $|a_1| = |a_2| = \ldots = |a_u|$ and $|b_1| = |b_2| = \ldots = |b_v|$. Let $\alpha$ be the cardinality of the $a_i$'s and $\beta$ the cardinality of the $b_i$'s. Then

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

Thus

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

so

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

and

$$u\alpha > v(u-1)\alpha,$$

which implies

$$v = 1.$$

A symmetric analysis shows that $u = 1$. Therefore $M$ contains only the three points $a$, $a_1$, and $b_1$, and $a$ is therefore a separator of $M$, contrary to the hypothesis that $M \in \mathfrak{M}_3(\gamma)$, i.e., that $M$ is connected.

(245) Hence $(k-|a|)|\gamma$ and $k-|a| \neq \gamma$ for every point $a$ of $M$.

For every $H \in \mathfrak{H}$ and $d$, $1 \leq d \leq k$, let $x_d^H$ denote the number of $(k-d)$-points contained in $H$, and let $\langle x_d^H \rangle$ denote the corresponding $k$-tuple. From (245) it follows that

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

If $a_1$ and $a_2$ are distinct points of $M$, then (245) implies that $k-|a_1| = d_1$ and $k-|a_2| = d_2$ are proper divisors of $\gamma$. Since $cl(a_1 \cup a_2) \in \mathcal{H}$, $|a_1| + |a_2| \leq k$; hence $|a_2| < d_1$ and

(247) $$k = |a_2| + d_2 \leq d_1 + d_2 \leq 2d,$$

where $d$ is the largest proper divisor of $\gamma$. This proves (248).

(248) Theorem. If $M \in \mathfrak{M}_3(\gamma)$, $k(M) = k$, then:

(i) For every hyperplane $H$ of $M$ there is a solution $\langle x^H \rangle$ to the diophantine equation $k = \sum_{\substack{d|\gamma \\ d\neq\gamma}} (k-d)x_d$, such that $x_d^H$ is the number of $(k-d)$-points contained in $H$.

(ii) $k \leq 2d$ where $d$ is the largest divisor of $\gamma$ less than $\gamma$.

## 4.4. Rank 3 equicardinal matroids with co-circuit cardinality a prime or prime squared

The following theorem generalizes (111).

(249) Theorem. Where $p$ is a prime and $n \geq 0$, every member of $\mathfrak{M}_n(p)$ is trivial.

Proof. By (124), it suffices to prove (249) when $n = 3$. Let $M \in \mathfrak{M}_3(p)$, $k(M) = k$. By (248) (ii), $k \leq 2$; hence $k = 2$ (since every line contains two points). Therefore $M$ is a $(1,2,-)$-trivioid. ∎

It is tempting to speculate that for $n \geq 3$, $\mathfrak{M}_n(\gamma)$ contains only trivioids if and only if $\gamma$ is a prime. However, this conjecture is false, as we shall subsequently show (313).

Another class of rank 3 equicardinal matroids that admits of relatively easy characterization is $\mathfrak{M}_3(p^2)$, where $p$ is a prime.

(250) Theorem. Where $p$ is a prime, every member of $\mathfrak{M}_3(p^2)$ is either

(i) a $\sigma(1,2,p^2+2)$

or (ii) a $\sigma(p,2,p+2)$

or (iii) a $PG(2,p)$.

Proof. Let $M = (E,\mathcal{H}) \in \mathfrak{M}_3(p^2)$, and let $k(M) = k$. The only proper divisors of $p^2$ are 1 and $p$. Hence, by (248), to every line $H$ of $M$ there corresponds a solution $(x^H, y^H)$ to the diophantine equation

(251) $$k = (k-1)x + (k-p)y$$

such that $x^H$ and $y^H$ are the number of $(k-1)$-points and

the number of (k-p)-points in $H$, respectively.

(252) Suppose that for some $H$, $x^H > 0$. If $x^H = 1$, then (251) becomes

$$k = (k-1) + (k-p)y^H.$$

Hence we must have $k = p+1$, $y^H = 1$, and $|E| = v+k = p^2 + p+1$. With $k = p+1$, the only solutions to (251) are $(x,y) = (1,1)$ and $(x,y) = (0,p+1)$; hence every line consists of either one p-point and one simple point, or $p+1$ simple points. Since every two points are contained in some line, $M$ contains <u>at most</u> one p-point, but, since $x^H = 1$, $M$ contains exactly one p-point. Call it $a$. $E' = E-a$ is then a union of $p^2 + 1$ simple points. Since every pair of simple points is contained in a unique line $H$, $H$ must contain only simple points, and hence $H \subseteq E'$. Where $\mathcal{H}' = \{H \in \mathcal{H}: H \subseteq E'\}$ it follows that $(E',\mathcal{H}')$ is a $2\text{-}(p^2+1, p+1, 1)$ design. But then $|\mathcal{H}'| = \frac{(p^2+1)p^2}{(p+1)p}$, which is no integer.

(253) Therefore, if $x^H > 0$ for some $H$, then $x^H \geq 2$. Then, by (251), $k \geq (k-1)\, x^H \geq 2(k-1)$, which is only possible if $x^H = 2$ and $k = 2$. In this case, $(x,y) = (2,0)$ is the only meaningful solution to (251), and hence every line of

M is the union of two simple points. Since $|E| = \gamma+k = p^2 + 2$, it follows that M is a $\sigma(1,2,p^2+2)$, which is (i).

(254) Let us therefore assume that $x^H = 0$ for every H. Then from (248) we have

$$k = (k-p)y^H,$$

(255)

$$(k-p) + p = (k-p)y^H$$

and

$$p = (k-p)\ (y^H-1).$$

Since p is a prime, the only solutions to (255) are: (I) $y^H = 2$, $k = 2p$; and (II) $y^H = p+1$, $k = p+1$. In case (I) every line H is the union of two p-points, and $|E| = 2p + \gamma = 2p + p^2 = p(p+2)$; hence M is a $\sigma(p,2,p+2)$, which is (ii).

(256) In case (II), every line H is the union of (p+1) simple points and $|E| = p^2 + p+1$. Thus M is a simple matroid design with d-sequence $(p^2,p,1)$, so, by (120), M is a PG(2,p), which is case (iii). ∎

## 4.5 Affine Extension

Our next main object will be to determine $m_3(pq)$ completely for certain pairs of distinct primes p and q. To do so, however, we need to introduce a new class of matroids.

A matroid $M = (E,\mathcal{H})$ is said to be <u>affine resolvable</u> if there exists a partition of $\mathcal{H}$ into classes $\{\rho_i,\ 1 \leq i \leq t\}$ such that each $\rho_i$ partitions $E$. The sets $\rho_i$ are called <u>parallel classes</u> of $M$.

(257) Let $M$ be a rank 3 affine resolvable matroid with parallel classes $\rho_i$, $1 \leq i \leq t$, $P(M)$ the set of points of $M$, and let $M' = (E',\mathcal{H}')$ be a rank 2 or rank 3 matroid with point set $P(M') = \{a_1', a_2', \cdots a_t', a_{t+1}', \cdots a_u'\}$, such that $u \geq t$ and $E \cap E' = \phi$. We define

$$X_i = \{a_i' \cup H\colon H \in \rho_i\},\ 1 \leq i \leq t,$$

$$X = \bigcup_{i=1}^{t} X_i,$$

$$Y = \{a_i' \cup a\colon a \in P(M),\ t+1 \leq i \leq u\},$$

and let

$$\mathcal{H}'' = X \cup Y \cup \mathcal{H}' \quad \text{if} \quad r(M') = 3,$$

$$\mathcal{H}'' = X \cup Y \cup \{E'\} \quad \text{if} \quad r(M') = 2.$$

In either case $(E \cup E',\mathcal{H}'')$ is called the <u>affine extension of $M$ by $M'$</u>, and denoted by $M \oplus M'$.

(258) <u>Theorem</u>. $M \oplus M'$ is a connected rank 3 matroid whenever $M \oplus M'$ is defined.

Proof. Let $M$, $M'$, and $M \oplus M' = (E \cup E',\mathcal{H}'')$ be as defined in (257), and let $P'' = P(M) \cup P(M')$ and $E'' = E \cup E'$. To

verify (H1) and (H2) for $(E'',\mathcal{H}'')$, it clearly suffices to show that every two members of $P''$ are contained in a unique member of $\mathcal{H}''$. It then follows easily that $P''$ is precisely the set of points of $M \oplus M'$, and that $r(M \oplus M') = 3$.

Let $a,b \in P''$, $a \neq b$. If $a,b \in P(M)$, then $cl_M(a \cup b) = H \in \mathcal{H}$, and $H \in \mathcal{P}_i$ for some $i$, so $a \cup b \subseteq H \cup a_i' \in \mathcal{H}''$. If $a,b \in P(M')$ and $r(M') = 2$, then $a \cup b \subseteq E' \in \mathcal{H}''$. If $a,b \in P(M')$ and $r(M') = 3$, then $cl_{M'}(a \cup b) = H' \in \mathcal{H}' \subseteq \mathcal{H}''$. Lastly, suppose that $a \in P(M)$ and $b \in P(M')$, say $b = a_j'$. If $t < j \leq u$, then $a \cup b \in \mathcal{H}''$. If $1 \leq j \leq t$, let $H_a$ be the unique hyperplane in $\mathcal{P}_j$ containing $a$; then $a \cup b \subseteq H_a \cup b \in \mathcal{H}''$. Thus, in any case, there is a unique member of $\mathcal{H}''$ containing $a \cup b$, and so $M \oplus M'$ is a rank 3 matroid.

Finally, let $S$ be a minimal nonempty separator of $M$. (259) If $S \cap E' \neq \emptyset$ and $E'-S \neq \emptyset$, let $a_i'$ and $a_j'$ meet $S \cap E'$ and $E'-S$, respectively. Further, let $H = cl_{M'}(a_i' \cup a_j') \in \mathcal{H}' \subseteq \mathcal{H}''$. Since $H \subseteq E'$ and $S$ is a separator, either $S \subseteq E'$ or $E \subseteq S$. In the former case, the hyperplane $a_j' \cup H_j$, where $H_j \in \mathcal{P}_j$, contains neither $S$ nor $E''-S$ (since $H_j \not\supseteq E$), and is therefore impossible. In the latter case,

the hyperplane $a_i' \cup H_i$, where $H_i \in \rho_i$, contains neither $S$ (since $H_i \not\supseteq E$), nor $E''-S$. Hence either case is impossible.

(260) Therefore, if $S \cap E' \neq \emptyset$, then $E' \subseteq S$. The parallel class $\rho_1$ contains at least two elements, $H_1$ and $H_2$, since the members of $\mathcal{H}$ are proper subsets of $E$. Further, $r(M') \geq 2$ implies $M'$ contains at least two points $a_1'$ and $a_2'$. Therefore neither $a_1' \cup H_1$ nor $a_1' \cup H_2$ contains $S$. Hence $E''-S \subseteq a_1' \cup H_i$, $i=1,2$. Since $H_1 \cap H_2 = \emptyset$, $E''-S \subseteq a_1'$, which implies $E'' = S$ (since $a_1' \subseteq E' \subseteq S$). But then $(E'', \mathcal{H}'')$ is connected.

(261) The only other alternative is that $S \subseteq E$, in which case the hyperplane $a_1' \cup H_1$, $H_1 \in \rho_1$, contains neither $S$ nor $E''-S$, which is a contradiction.

Therefore $S = E''$, and $M \ominus M'$ is a connected rank 3 matroid. ∎

If, in (257), the cardinalities of the points and lines of $M$ and $M'$ are appropriately related, then $M \ominus M'$ will be an equicardinal matroid.

The construction (257) generalizes the way in which a $PG(2,s)$ is derived from an $EG(2,s)$. Indeed, a $PG(2,s)$ is just an $EG(2,s) \ominus \sigma(1,1,s+1)$, as may easily be verified.

However, there are many more possibilities. In Fig. 5 we show two easy examples of affine extension that are not projective geometries.

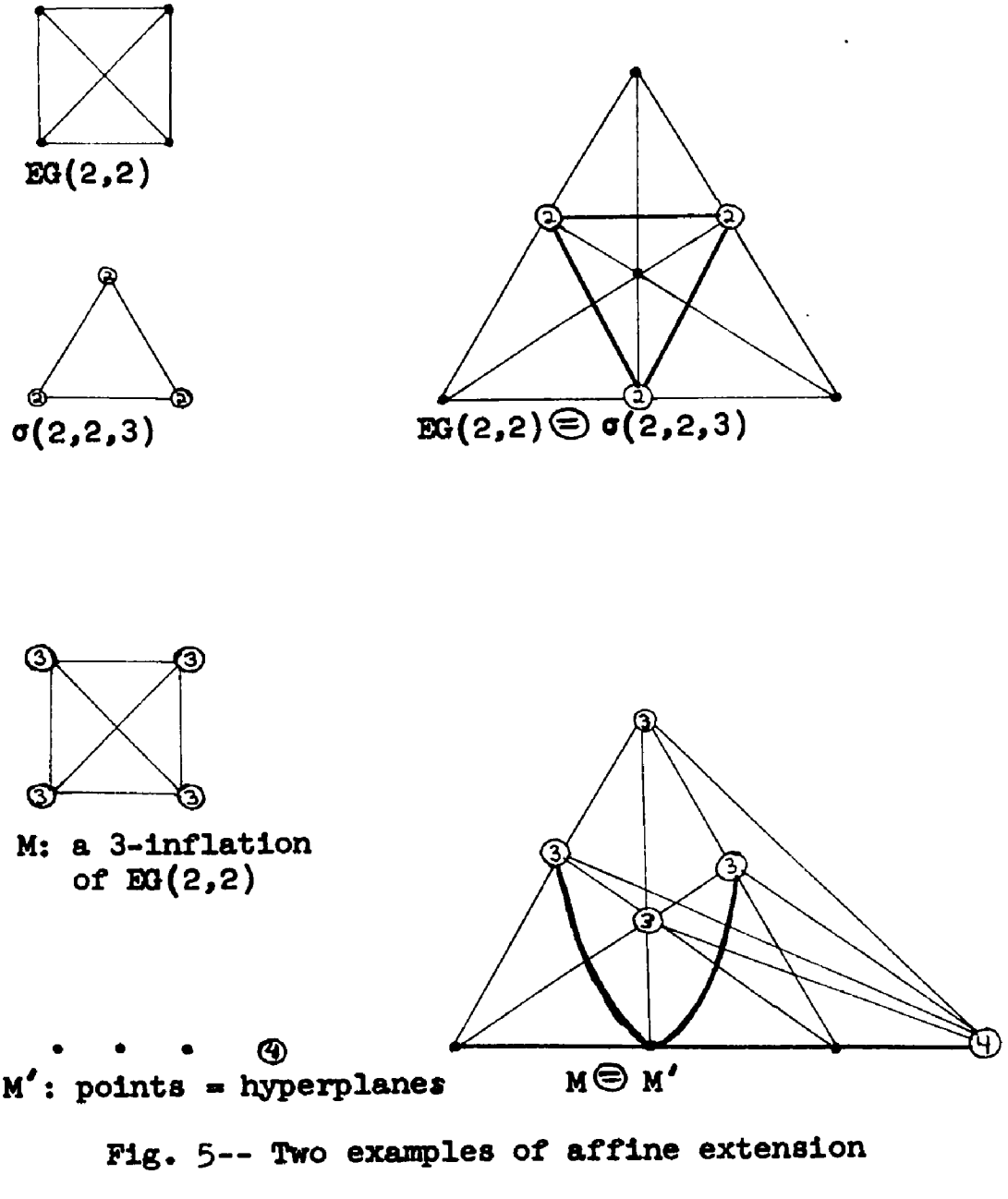
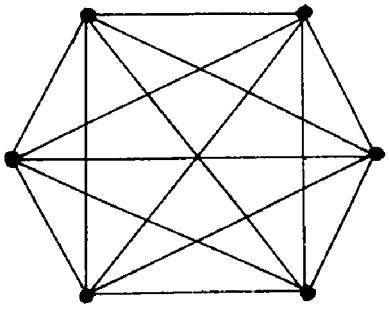
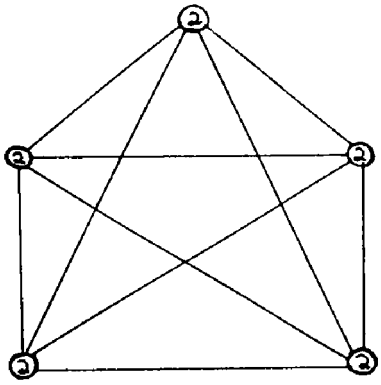



Fig. 5-- Two examples of affine extension

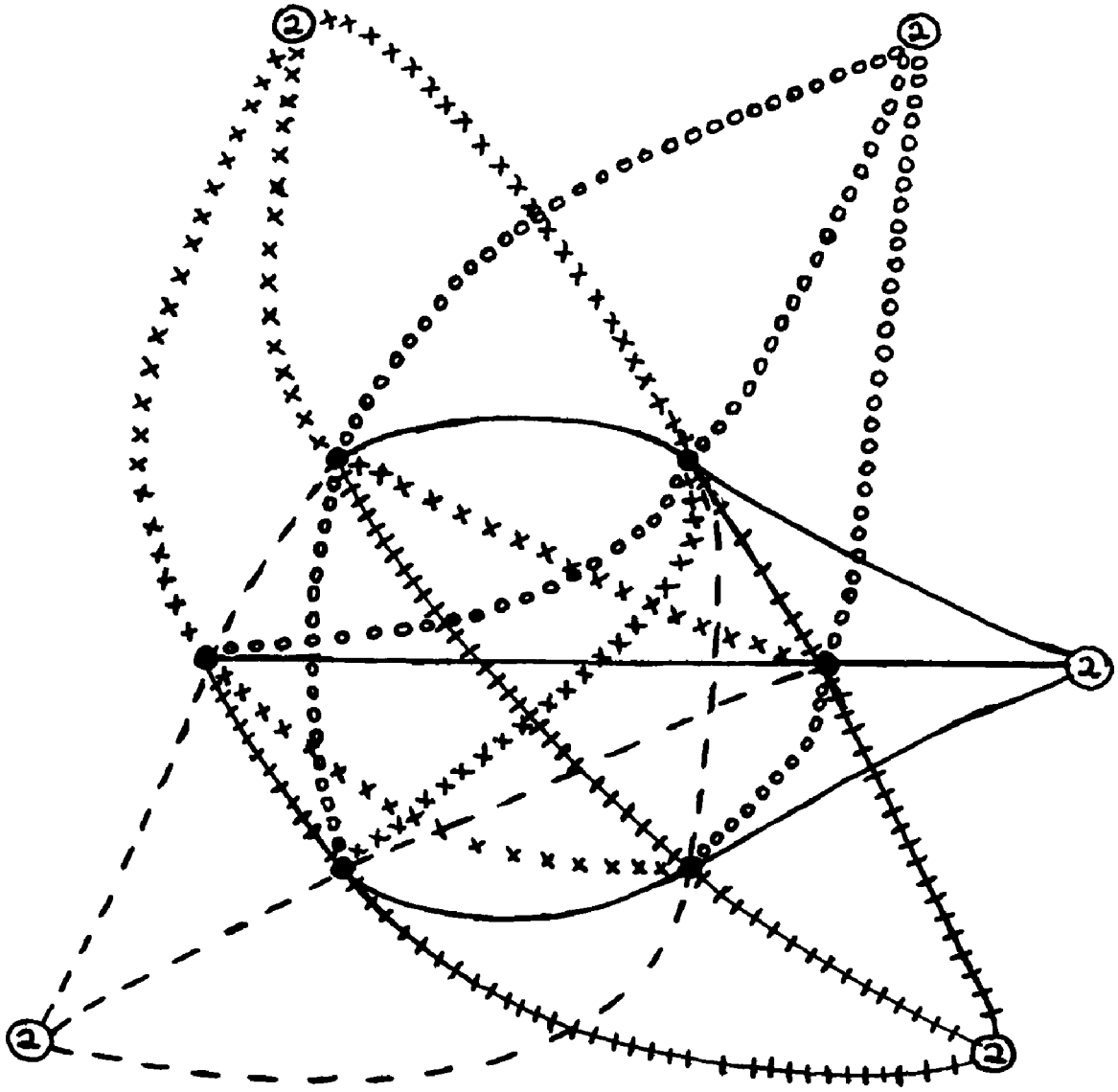
(262) A very general class of affine extensions arises from certain complete subgraphs. In our terminology, a <u>complete subgraph of order n</u> is just a $\sigma(1,2,n)$; in graph terminology the points are called <u>vertices</u> and the hyperplanes are called <u>edges</u>. It is proved in graph theory (see, for example, [ 9]) that for every positive integer m, $\sigma(1,2,2m)$ is affine resolvable into 2m-1 parallel classes. For any such m, $\sigma(1,2,2m)$ and $\sigma(2,2,2m-1)$ are both rank 3 matroids, and the latter has 2m-1 points, each of cardinality 2. By (258), it follows that $\sigma(1,2,2m) \oplus \sigma(2,2,2m-1)$ is a connected rank 3 matroid, called the <u>complete graph extension of order m</u>, CGE(m). Fig. 6 shows $\sigma(1,2,6)$, $\sigma(2,2,5)$, and $\sigma(1,2,6) \oplus \sigma(2,2,5)$.



$\sigma(1,2,6)$



$\sigma(2,2,5)$




$\sigma(1,2,6) \ominus \sigma(2,2,5)$

Fig. 6-- The complete graph extension of order 3

(The elementary lines in $\sigma(1,2,6) \ominus \sigma(2,2,5)$ joining each pair of 2-points have here been omitted for simplicity.)

## 4.6 Rank 3 equicardinal matroids with co-circuit cardinality pq, p and q distinct primes

(263) Theorem. Let p and q be distinct primes such that either $p < \frac{2}{3}q+1$, or $\frac{2}{3}q+1 \leq p \leq \frac{3}{4}q+1$ and the polynomial

$$\Theta_{p,q}(x) = (q+1)x^2 - (12pq-2q^2-6p^2+6p+3q+5)x + 6(p+1)(pq+q+1)$$

has no positive integral root. Then for every nontrivial matroid $M \in \mathfrak{M}_3(pq)$ exactly one of the following holds.

(i) $(p+1)|q(q+1)$ and M is a $D_2(pq+p+1,p+1,1)$.

(ii) $(p+1)|q(pq+1)$ and M is a $D_2(pq+1,p+1,1) \oplus P(p)$.

(iii) $q = 2p-1$ and M is an $EG(2,p) \oplus \sigma(p,2,p+1)$.

Proof. (264) Let p, q, and $M = (E,\mathcal{H})$ satisfy the hypothesis of (263). Since $r(M) = 3$, $\mathcal{H}$ is the family of lines of M. By (234), $M_a = M \cdot (E-a)$ is a trivioid for every point a of M, and the points of $M_a$ are its hyperplanes. Let $\delta = k(M_a)$. Since the points of $M_a$ are disjoint, $\delta | c^*(M_a) = pq$, and hence $\delta = 1$, p, q, or pq.

(265) If $\delta = 1$, $M_a$ is a $\sigma(1,1,pq+1)$;

if $\delta = p$, $M_a$ is a $\sigma(p,1,q+1)$;

if $\delta = q$, $M_a$ is a $\sigma(q,1,p+1)$;

if $\delta = pq$, $M_a$ is a $\sigma(pq,1,2)$.

We abbreviate these rank 2 trivioids by $\sigma_1$, $\sigma_p$, $\sigma_q$, and $\sigma_{pq}$, respectively.

(266) Now $M_a \neq \sigma_{pq}$, because $\sigma_{pq}$ is just the union of two disjoint hyperplanes (points), and hence is not connected, which contradicts (221) and the assumption that M is connected.

(267) Suppose that all points of M have cardinality $\alpha$.

If a is any point of M, the points of $M_a$ are partitioned by points of M, and hence $\alpha | \delta$; i.e., $\alpha = 1, p$, or q. If $\alpha = p$, then $\delta = p$ and hence $M_a = \sigma_p$ and $P(M_a) \subseteq P(M)$. But then, by (229), M is a trivioid, contrary to hypothesis. A similar conclusion holds if $\alpha = q$. Hence $\alpha = 1$, and since M is nontrivial, the same argument used above shows that $M_a \neq \sigma_1$.

(268) If $M_a = \sigma_p$ for some point a of M, $|a| = 1$, then the cardinality of every line containing a is p+1, and there are q+1 such lines. Therefore $|E| = pq + p+1$. Likewise, if $M_a = \sigma_q$ for some point a of M, then $|E| = pq + q+1$. Since $pq + p+1 \neq pq + q+1$, it must be that either $M_a = \sigma_p$ for every $a \in P(M)$, or $M_a = \sigma_q$ for every $a \in P(M)$.

(269) If $M_a = \sigma_q$ for every $a \in P(M)$, then every line of M contains q+1 points and every two (simple) points of M are contained in a unique line. Therefore, since $|E| = pq + q+1$,

$M$ is a $D_2(pq + q+1, q+1,1)$ (i.e., a 2-$(pq + q+1, q+1,1)$ design) and $d(M) = (pq,q,1)$. But $d(M)$ does not satisfy (D2), because $\frac{pq}{q} < \frac{q}{1}$ (by our hypotheses, $p < q$). Therefore $d(M)$ is not D-consistent, a contradiction.

(270) If $M_a = \sigma_p$ for all $a \in P(M)$, then, reasoning as in (269), we find that $M$ is a $D_2(pq + p+1, p+1,1)$ with d-sequence $(pq,p,1)$. In particular, the number of lines of $M$ is $|\mathfrak{B}| = t_M(0,2,3) = \frac{(pq+p)(pq+p+1)}{p(p+1)}$, which must be an integer. Since $\frac{(pq+p)(pq+p+1)}{p(p+1)} = \frac{(q+1)(pq+p+1)}{p+1} = \frac{(q+1)pq}{p+1} + q+1$, and since $p+1$ and $p$ are relatively prime, $(p+1)$ must divide $q(q+1)$. This is precisely statement (i).

(271) Let us assume then that the hypothesis of (267) does not hold, and that $M$ contains two points of unequal cardinality.

(272) Suppose that $M_a = \sigma_1$ for some point $a$. Since every point of $M_a$ contains a point of $M$, it follows that $P(M_a) \subseteq P(M)$, and hence all points of $M$ except $a$ are simple. ($a$ is nonsimple, by our hypothesis (271).) By (39), $a \cup b$ is a line of $M$ for every $b \in P(M)-\{a\}$. Therefore, for $b \in P(M)-\{a\}$, $a$ is a point of $M_b$, and so we must have $|a| = p$ or $|a| = q$. Let us also note that $M_a = \sigma_1$ implies $|E| = pq + 1 + |a|$. If $|a| = q$, then the lines of $M$ all

have cardinality $q+1$. Let $\overline{H}_a$ be the set of lines not containing $a$. Clearly, $M' = (E-a, \overline{H}_a)$ is a simple rank 3 equicardinal matroid and $k(M') = q+1$. Therefore $M'$ is a $D_2(pq+1, q+1, 1)$ design and $d(M') = (pq-q, q, 1)$. However, $\frac{pq-q}{q} < \frac{q}{1}$, so $d(M')$ does not satisfy (D2), which is a contradiction.

Hence $|a| = p$. A similar argument to the above shows then that $M' = (E-a, \overline{H}_a)$ is a $D_2(pq+1, p+1, 1)$, and $d(M') = (p(q-1), p, 1)$. Since $a \cup b$ is a line of $M$ for every $b \in P(M_a)$, $M = M' \oplus a$, which gives (ii).

(273) By (271) and (272), we may therefore suppose that $M$ contains two points of unequal cardinality, and that for every point $a$ of $M$, $M_a = \sigma_p$ or $M_a = \sigma_q$. Further, if $M_a = \sigma_p$, then $|H-a| = p$ for every line $H$ containing $a$, and hence $|a| = k-p$. Conversely, if $|a| = k-p$, then clearly $M_a \neq \sigma_q$, so $M_a = \sigma_p$. Thus $M_a = \sigma_p$ if and only if $|a| = k-p$, and, similarly, $M_a = \sigma_q$ if and only if $|a| = k-q$. In particular, every point has cardinality $k-p$ or $k-q$, and each of these cardinalities is assumed by some point.

(274) By (248) and (273), to each line $H$ of $M$ there corresponds a solution $(\alpha^H, \beta^H)$ to the diophantine equation

(275) $$(k-q)\,\alpha + (k-p)\,\beta = k,$$

where $\alpha^H$ is the number of $(k-q)$-points in $H$ and $\beta^H$ is the number of $(k-p)$-points in $H$.

We shall show that $0 \leq \beta^H \leq 3$ for every $H \in \mathfrak{H}$.

(276) By (273) there is a point $a$ of $M$ such that $|a| = k-q$; hence $k \geq q+1$.

(277) Suppose that $\beta^H \geq 4$ for some $H \in \mathfrak{H}$. If $\alpha^H = 0$, then, by (275),

$$\beta^H(k-p) = k = p + (k-p),$$

so

$$(\beta^H-1)(k-p) = p.$$

Since $\beta^H \geq 4$ and $p$ is a prime, it follows that $\beta^H = p+1$ and $k-p = 1$. But then $p < q$ implies $k-q \leq 0$, which contradicts (276). Therefore $\alpha^H \geq 1$. Thus we have

$$k = \alpha^H(k-q) + \beta^H(k-p) \geq 1 + 4(k-p),$$

whence

$$4p \geq 3k + 1.$$

Since $k \geq q+1$, it follows that

$$4p \geq 3q + 4,$$

$$p \geq \tfrac{3q}{4} + 1.$$

Hence $p > \frac{3}{4}q+1$, since $q$ is a prime and $p$ is an integer. This contradicts our hypotheses on $p$ and $q$, and proves that

(278) $0 \leq \beta^H \leq 3$ for every $H \in \mathfrak{H}$.

(279) Suppose now that $k-q > 1$, and we shall derive a contradiction.

(280) If there exists a line $H$ such that $\beta^H = 0$, then from (275) we have

$$(k-q)\,\alpha^H + 0 = k = q + (k-q),$$

whence

$$(\alpha^H - 1)(k-q) = q.$$

Since $q$ is a prime and by hypothesis $k > q+1$, we must have $\alpha^H = 2$ and $k = 2q$. By (273), let $a$ and $b$ be a $(k-q)$-point and $(k-p)$-point of $M$, respectively. Then $|a| = q$, $|b| = 2q-p$, and the line $H' = c\ell(a \cup b)$ has cardinality $|H'| \geq 2q-p+q > 2q = k$, a contradiction. Therefore under hypothesis (279), $\beta^H \geq 1$ for every $H \in \mathfrak{H}$.

(281) If $\beta^H = 1$ for some line $H$ of $M$, then (275) becomes

$$\alpha^H(k-q) + (k-p) = k = p + k-p,$$

that is,

$$\alpha^H(k-q) = p.$$

Therefore, since $k-q > 1$, $k = p+q$ and $\alpha^H = 1$. But then, by (273), every point of $M$ is a $p$-point or a $q$-point, and therefore $k = p+q$ implies that every line of $M$ is of the form $a \cup b$, where $a$ is a $p$-point, $b$ is a $q$-point. Since

$M$ contains at least three points, it contains two distinct points $c$ and $c'$ of equal cardinality, and hence the line $c\ell(c \cup c')$ is not of the above form. Thus we have a contradiction.

(282) By (278), we may therefore assume that, if $k-q > 1$, then $\beta^H = 2$ or $\beta^H = 3$ for every line $H$ of $M$. Suppose that $(\alpha^H, \beta^H)$ and $(\alpha^{H'}, \beta^{H'})$ represent two distinct solutions to (275). Clearly, both $\alpha^{H'} \neq \alpha^H$ and $\beta^{H'} \neq \beta^H$. With no loss of generality we may therefore assume that $\beta^H = 2$ and $\beta^{H'} = 3$. Hence

$$\alpha^H(k-q) + 2(k-p) = k,$$

and

$$\alpha^{H'}(k-q) + 3(k-p) = k,$$

that is,

$$\alpha^H(k-q) + k = 2p$$

and

$$\alpha^{H'}(k-q) + 2k = 3p,$$

whence

$$(2\alpha^H - \alpha^{H'})(k-q) = p.$$

Since $k-q > 1$, we must have $k-q = p$, which leads to a contradiction just as in (281). Therefore the solution $(\alpha^H, \beta^H)$ to (275) is the same for every $H \in \mathcal{H}$, and either $\beta^H = 2$ or $\beta^H = 3$. If $\beta^H = 2$, every line $H$ contains exactly two $(k-p)$-points. Let $P_{k-p}(M)$ be the set of $(k-p)$-points of $M$,

and let a be a (k-q)-point. Then $M_a = \sigma_q$, and since $|P(M_a)| = p+1$, there are exactly p+1 lines H containing a, and the sets H-a partition E-a. Hence $|P_{k-p}(M)| = 2(p+1)$. On the other hand, if b is a (k-p)-point, then $M_b = \sigma_p$, and so the q+1 lines containing b each contain one (k-p)-point other than b. Hence $|P_{k-p}(M)| = q+2$. Thus $2(p+1) = q+2$, so $2p = q$, which is impossible. If $\beta^H = 3$, a similar argument shows that

$$2(q+1) + 1 = 3(p+1),$$

whence

$$2q = 3p.$$

Since p and q are primes, this expression implies that $p = 2$ and $q = 3$. However, in that case (275) becomes

$$\alpha^H(k-3) + 3(k-2) = k,$$

or equivalently,

$$(\alpha^H+2)\, k = 3(\alpha^H+2),$$

and thus

$$k = 3 .$$

But then $k-q = 0$, which contradicts (279).

(283) It follows from (280), (281) and (282) that $k-q > 1$ is impossible. Hence, by (276), $k = q+1$.

(284) By (273) and (283), M contains only simple points and u-points, where $u = q-p+1$. Further, $M_a = \sigma_q$ for every

simple point $a$, so every simple point is contained in exactly $p+1$ lines of $M$. Similarly, every u-point is contained in exactly $q+1$ lines of $M$.

(285) Suppose that some line $H$ contains only simple points. Then, by (283), $H$ contains $q+1$ points. Let $a \in P(H)$, and let $H'$ be a line distinct from $H$ containing $a$. Because $|H'-a| = q$ and $u \nmid q$, $H'-a$ must contain a simple point $a'$. Clearly $a' \cap H = \emptyset$. But for each $b \in P(H)$, there is a unique line containing $b$ and $a'$. Hence altogether $a$ is contained in at least $q+1$ distinct lines, contradicting (284).

(286) By (284) and (285) it follows that every line of $M$ contains at least one u-point.

(287) Now let us consider the special case $q = 2p-1$. In this case $k = q+1 = 2p$ and $u = p$. For every line $H$, $(\alpha^H, \beta^H)$ therefore satisfies

(288) $$\alpha^H + \beta^H p = 2p, \quad \beta^H \geq 1.$$

It is easy to check that $(\alpha^H, \beta^H) = (0,2)$ and $(\alpha^H, \beta^H) = (p,1)$ are the only non-negative integral solutions to (288); i.e., every line of $M$ consists of either two p-points, or one p-point and $p$ simple points. By (284), every simple point $a$ is contained in exactly $p+1$ lines; since each of these lines contains exactly one p-point, $M$ contains exactly

(p+1) p-points. Let $P_1(M)$ be the set of simple points of M, $P_p(M)$ the set of p-points of M, and let $A = \bigcup_{a \in P_1(M)} a$, $\mathcal{H}_A = \{H \cap A: H \in \mathcal{H} \text{ and } (\alpha^H, \beta^H) = (p,1)\}$. Every two distinct elements $x,y \in A$ are contained in a unique member of $\mathcal{H}_A$, namely $c\ell\{x,y\}-b$, where b is the unique p-point contained in $c\ell\{x,y\}$. Further, every member of $\mathcal{H}_A$ has cardinality k-p = p. Finally,

$$\begin{aligned} |A| &= |E| - p\,|P_p(M)| = k + pq - p(p+1) \\ &= 2p + p(2p-1) - p^2-p \\ &= p^2. \end{aligned}$$

Therefore $(A,\mathcal{H}_A)$ is a rank 3 matroid design with d-sequence (p(p-1), p-1,1), and so $(A,\mathcal{H}_A)$ is an EG(2,p), by (125). Since k = 2p, the union of every two distinct p-points is a line of M. Thus, where $B = \bigcup_{b \in P_p(M)} b$, and $\mathcal{H}_B$ is the set of lines of M contained in B, $(B,\mathcal{H}_B)$ is a $\sigma(p,2,p+1)$. Finally, the set of lines containing any fixed p-point of M and meeting A form a parallel class of $(A,\mathcal{H}_A)$ when restricted to A. It follows that M is an EG(2,p) $\ominus$ $\sigma(p,2,p+1)$. This is precisely case (iii).

(289) It remains to show that if $q \neq 2p-1$ and (283), (284), and (286) are satisfied, M cannot exist.

(290) Every line of $M$ contains a simple point. Suppose to the contrary that some line is a union of u-points. Then $u|k$, that is, $(q-p+1) \mid q+1$. But then $(q-p+1) \mid p$, which implies that $q-p+1 = p$ (since $q > p$), and hence $q = 2p-1$, contrary to our current hypothesis.

(291) Every line of $M$ contains at least two u-points. Indeed, by (286), every line of $M$ contains at least one u-point. Suppose that $H_0$ is a line containing exactly one u-point. Then $H_0$ contains $p$ simple points and $p+1$ points in all. Let $E' = E-H_0$, and $\mathcal{H}' = \{H \in \mathcal{H}: H \subseteq E'\}$. For a given simple point $a$ contained in $E'$ and each point $b$ in $H_0$ there is a unique line containing $a$ and $b$, and it intersects $H_0$ only in $b$. Hence there are $p+1$ such lines. But, by (284), $a$ is contained in a total of $p+1$ lines; hence every line containing $a$ meets $H_0$. Therefore, every line $H' \in \mathcal{H}'$ is a union of u-points, which we have shown in (290) to be impossible. Thus $\mathcal{H}'$ must be empty. However, let $a$ be a simple point in $H_0$ and let $H_1$ be a line distinct from $H_0$ containing $a$. By (286), $H_1$ contains a u-point $b$, and $b \subseteq E'$. There are exactly $(p+1)$ lines containing $b$ and meeting $H_0$, and hence, by (284), exactly $(q+1)-(p+1) = q-p \geq 1$ lines of $\mathcal{H}'$

containing b. Thus $\mathcal{H}'$ is nonempty, which is a contradiction.

(292) (278) and (291) together imply that, for every line H, $\beta^H = 2$ or $\beta^H = 3$. Using the fact that $k = q+1$, we obtain, from (275),

$$\beta^H = 2 \text{ implies } \alpha^H = 2p-q-1 \text{ for every } H \in \mathcal{H},$$

$$\text{and } \beta^H = 3 \text{ implies } \alpha^H = 3p-2q-2, \text{ for every } H \in \mathcal{H}.$$

Let $\mathcal{H}_1$ be the set of lines (type-1 lines) containing (2p-q-1) simple points and 2 u-points, and let $\mathcal{H}_2$ be the set of lines (type-2 lines) containing 3p-2q-2 simple points and 3 u-points.

(293) Let x be the number of u-points in M, and let $r_1$ be the number of type-i lines containing any simple point of M, i = 1,2. We must show that $r_1$ and $r_2$ are well-defined. This follows by observing that $r_1 + r_2 = p+1$, and $r_1 = 3(p+1) - x$. The last relationship follows from the fact that every simple point a lies on (p+1) lines, each containing at most three and at least two u-points. Hence $3(p+1) \geq x \geq 2(p+1)$, and $3(p+1) - x$ is the number of lines containing a that contain precisely two u-points.

(294) Let $R_i$ be the number of type-i lines containing any u-point, i = 1,2. Reasoning as in (293), we find that

$$R_1 + R_2 = (q+1)$$

and

$$R_1 = (2(q+1) + 1)-x,$$

and hence $R_1$ and $R_2$ are well-defined.

(295) Let $y$ denote the number of simple points in $M$. Since $|E| = \gamma + k = pq + q+1$, we have that $(q-p+1)\,x + y = pq + q+1$. Moreover, $x > 0$ and $y > 0$, since not all points of $M$ have the same cardinality.

(296) Let $h_i$ denote the number of type-i lines in $M$, $i = 1,2$. Since every type-1 line contains $2p-q-1$ simple points, and since every simple point is contained in $r_1$ type-1 lines, we have, using (293) and (295),

(297) $(2p-q-1)\,h_1 = r_1 y = (3(p+1)-x)(pq+q+1-(q-p+1)x)$.

Using similar arguments we obtain the following equations.

(298) $$2h_1 = R_1 x = [2(q+1) + 1-x]x$$

(299) $$(3p-2q-2)\,h_2 = r_2 y = [x-2(p+1)][pq+q+1-(q-p+1)x]$$

(300) $$3h_2 = R_2 x = [x-(q+2)]x.$$

These four equations in $h_1$, $h_2$, and $x$ must have a positive integral solution for $M$ to exist. The equations are consistent, as may be verified by eliminating $h_1$ and $h_2$.

(301) Suppose that for some solution to this system, $h_2 = 0$.

From (300) it then follows that $x = 0$ or $x = q+2$. But $x > 0$, by (295), and so $x = q+2$. Substituting $h_2 = 0$ and $x = q+2$ in (299), we have that either

$$q+2 - 2(p+1) = 0$$

or

$$(pq+q+1) - (q-p+1)(q+2) = 0.$$

The first implies that $2p = q$, which is absurd. The second yields

$$pq + q+1 = q^2-pq + 3q-2p+2,$$

$$2pq + 2p = q^2 + 2q+1,$$

$$2p(q+1) = (q+1)^2,$$

so $2p = q+1$, which is contrary to our present hypothesis (289).

Therefore we may assume that $h_2 > 0$. Now $r_2 > 0$ and $y > 0$, so it follows by (299) that

$$3p-2q-2 > 0,$$

(302) and hence $$p \geq \frac{2q}{3} + 1.$$

Eliminating $h_1$ from (297) and (298), we obtain the following quadratic in $x$:

(303) $$(2p-q-1)\,\frac{[2(q+1) + 1-x]x}{2} = [3(p+1)-x][pq+q+1-(q-p+1)x]$$

Collecting terms, (303) becomes

(304) $$(q+1)x^2 - (12pq-2q^2-6p^2+6p+3q+5)x + 6(p+1)(pq+q+1) = 0\ .$$

But $p \geq \frac{2}{3} q+1$, by (302), so by our hypothesis the polynomial of (304), $\theta_{p,q}(x)$, has no positive integral root. Therefore there is no positive integral solution to the equations (297)-(300), so M does not exist. Thus (289) is proved, and likewise the theorem. ∎

The proof of (263) is valid for any pair of distinct primes p and q for which $p \leq \frac{3}{4} q+1$ and the associated equations (297)-(300) have no positive integral solution in x. The pairs (p,q) as above for which such solutions do exist, or even those pairs for which only $\theta_{p,q}(x)$ has a positive integral root, appear to be very rare. In fact, the pair (17,23) is the only one known to this author.

The problem of constructing a rank 3, nontrivial, connected, equicardinal matroid with co-circuit cardinality $17 \cdot 23 = 391$ is therefore of considerable interest. If such a matroid $M = (E,\mathcal{H})$ does exist, the proof of (263) provides a very substantial degree of information about its structure. With $p = 17$ and $q = 23$, we know from (284) that M contains only simple points and u-points, where $u = 23-17+1 = 7$. Where x is the number of 7-points in M, x must be a root of $\theta_{17,23}(x)$, which in this case becomes

$$24x^2 - 2076x + 44820 = 0 \tag{305}$$

The only positive integral solution to (305) is $x = 45$, so $M$ must contain precisely 45 7-points. From (295) it follows that $|E| = 415$, and the number of simple points of $M$ is $y = 415 - 7 \cdot 45 = 100$. By definition (292), the type-1 lines each contain 10 simple points and 2 7-points, and the type-2 lines each contain 3 simple points and 3 7-points. Using the expressions for $r_1$, $r_2$, $R_1$, and $R_2$ in (293) and (294), we find that every simple point is contained in 18 lines, 9 or each type. Every 7-point is contained in 24 lines, 4 of type 1 and 20 of type 2.

Let $E'$ be the union of the simple points in $E$, and let $\mathcal{H}'$ be the type-1 lines restricted to $E'$. By the above, $|E'| = 100$, $\mathcal{H}'$ is a set of lines in $E'$ each containing 10 points, and every point of $E'$ is contained in precisely 9 members of $\mathcal{H}'$. Apparently, then, $(E', \mathcal{H}')$ is closely related to the affine geometry $EG(2,10)$, the existence of which is still undetermined. Unfortunately, it appears that the determination of $M$ would be at least as difficult as the construction of an $EG(2,10)$, and therefore we leave the question of its existence as an unsolved problem.

We have the following two important consequences of Theorem (263).

(306) Theorem. If $p$ and $q$ are distinct primes such that $\frac{2}{3}q+1 \leq p \leq \frac{3}{4}q+1$ and $\theta_{p,q}(x)$ has no positive integral root, then every member of $\mathfrak{m}_3(pq)$ is trivial.

Proof. Let $M$ be a nontrivial member of $\mathfrak{m}_3(pq)$. Then, by (263), exactly one of the following holds:

(i) $(p+1)|q(q+1)$

(ii) $(p+1)|q(pq+1)$

(iii) $q = 2p-1$.

If $q = 2p-1$, then $p = \frac{q+1}{2} < \frac{2}{3}q+1$, contrary to hypothesis. Therefore (iii) is impossible.

If $p+1 = q$, then, since $p$ and $q$ are primes, $(p,q) = (2,3)$. But $2 < \frac{2}{3} \cdot 3 + 1 = 3$, contrary to our assumption. Hence $p+1 \neq q$, so (i) holds if and only if $(p+1)|(q+1)$, and (ii) holds if and only if $(p+1)|(pq+1)$.

If $(p+1)|(q+1)$, then either $p+1 = q+1$, or $p+1 \leq \frac{q+1}{2}$, both of which are contrary to assumption. Hence (i) is impossible.

If $(p+1)|(pq+1)$, then $(p+1)|[(p+1)q+1-q]$, so $(p+1)|(q-1)$. Hence, either $p+1 = q-1$, or $p+1 \leq \frac{q-1}{2}$.

The latter case clearly violates $p \geq \frac{2}{3} q+1$. In the former case, $q = p+2$, so we have $p \leq \frac{3}{4}(p+2) + 1$, that is, $p \leq 10$. Therefore either $(p,q) = (3,5)$ or $(p,q) = (5,7)$. But neither of these satisfies the inequality $p \geq \frac{2}{3} q+1$, and hence (ii) is also impossible. Therefore every member of $\mathfrak{M}_3(pq)$ is trivial. ∎

(307) Corollary. If $p$ and $q$ are distinct primes such that $\frac{2}{3} q+1 \leq p \leq \frac{3}{4} q+1$ and $\Theta_{p,q}(x)$ has no positive integral root, then every connected equicardinal matroid with co-circuit cardinality $pq$ is trivial.

This result follows at once from (241).

(308) Theorem. Let $p$ and $q$ be distinct primes such that $p < \frac{2}{3} q+1$ and $(p,q) \neq (2,3), (3,5)$.

(i) If $(p+1)|(q+1)$, then every nontrivial member of $\mathfrak{M}_3(pq)$ is a $D_2(pq+p+1,p+1,1)$.

(ii) If $(p+1)|(pq+1)$, then every nontrivial member of $\mathfrak{M}_3(pq)$ is a $D_2(pq+1,p+1,1) \oplus P(p)$.

(iii) If $q = 2p-1$, then every nontrivial member of $\mathfrak{M}_3(pq)$ is an $EG(2,p) \cong \sigma(p,2,p+1)$.

(iv) If $(p+1) \nmid (q+1)$, $(p+1) \nmid (pq+1)$, and $q \neq 2p-1$, then every connected equicardinal matroid with cocircuit cardinality $pq$ is trivial.

Proof. We shall show first that, under our hypotheses, at most one of the following conditions holds.

(i′) $(p+1) \mid q(q+1)$

(ii′) $(p+1) \mid q(pq+1)$

(iii′) $q = 2p-1$.

(309) Since $(p,q) \neq (2,3)$, it follows that $q \neq p+1$. Therefore, (i′) and (ii′) are respectively equivalent to

(i″) $(p+1) \mid (q+1)$

(ii″) $(p+1) \mid (pq+1)$.

(310) We write

$$pq + 1 = pq + p - p+1 = p(q+1) - (p-1),$$

and it follows that if $(p+1) \mid (pq+1)$ and $(p+1) \mid (q+1)$, then $(p+1) \mid (p-1)$, which is absurd. Thus, at most one of (i″) and (ii″) holds.

(311) If $q = 2p-1$, then (ii″) becomes

$$(p+1) \mid 2p^2-p+1$$

or

$$(p+1) \mid (2p-3)(p+1) + 4,$$

which holds if and only if

$$(p+1) \mid 4,$$

that is, if and only if

$$p = 3 \text{ and } q = 2\cdot 3-1 = 5,$$

a case we excluded. Thus, at most one of (ii′) and (iii′) holds.

(312) Finally, if $q = 2p-1$, then (i′) becomes $(p+1) \mid 2p$, which is absurd, so at most one of (i′) and (iii′) holds.

By (310) - (312), at most one of (i′), (ii′), and (iii′) holds, so, by (309), at most one of (i′), (ii′) and (iii′) holds. Conclusions (i) - (iii) of the corollary now follow from (263). It also follows from (263) and the above that if $(p+1) \nmid (q+1)$, $(p+1) \nmid (pq+1)$, and $q \neq 2p-1$, then every member of $\mathfrak{M}_3(pq)$ is trivial, so, by (241), every connected equicardinal matroid with co-circuit cardinality $pq$ is trivial. ∎

(313) As may be checked directly, the pair of primes (7,11) satisfies (308) (iv); hence every connected equicardinal matroid with co-circuit cardinality 77 is trivial. The pair (5,7) satisfies (308) (ii), hence every nontrivial member of $\mathfrak{M}_3(35)$ is a $D_2(36,6,1) \oplus P(5)$; that is, an $EG(2,6) \oplus P(5)$. But $EG(2,6)$ does not exist, by (74). Thus every member of $\mathfrak{M}_3(35)$ is trivial; hence all connected equicardinal matroids with co-circuit cardinality $\gamma$ are trivial.

(314) As may be seen from Appendix II, 35 and 77 are the only integers $\gamma$ between 1 and 100, other than primes, for which

every connected equicardinal matroid with co-circuit cardinality $\gamma$ is known to be trivial. Every pair of distinct primes $(p,q)$ such that $1 \leq pq \leq 100$, except the pair $(7,11)$, satisfies the condition $p < \frac{2}{3}q+1$ and at least one of the divisibility conditions of (263). In some of these cases, however, it is not known whether or not the corresponding BIBD's prescribed by (263) exist.

## 4.7. Characterization of higher rank equicardinal matroids

We turn our attention now to the problem of determining $\mathfrak{m}_n(\gamma)$ when $n > 3$ and $\gamma$ is the product of two primes.

(315) Theorem.

(i) Where $p$ is an odd prime, every member of $\bigcup_{n=4}^{\infty} \mathfrak{m}_n(p^2)$ is trivial.

(ii) The only nontrivial member of $\bigcup_{n=4}^{\infty} \mathfrak{m}_n(2^2)$ is the rank 4 matroid $EG(3,2)$.

Proof. Let $p$ be a prime (either odd or even), and let $M = (E,\mathcal{H})$ be a nontrivial member of $\mathfrak{m}_4(p^2)$.

(316) By (234), $M_a = M \cdot (E-a)$ is nontrivial for some point $a$ of $M$, and hence $M_a$ is a $PG(2,p)$, by (250). In particular, $M_a$ is simple; hence $P(M_a) \cup \{a\} = P(M)$. By (234) and (250), $M_b$ is a $PG(2,p)$ for some $b \in P(M_a)$,

and since $a \subseteq a'$ for some point $a'$ of $M_b$, $a$ is also simple. Therefore, $M$ is simple, and

(317) $$|E| = |P(M_a)| + |a| = p^2+p+q.$$

(318) Suppose that $M_b$ is trivial for some point $b$; by (250), $M_b$ is a $\sigma(1,2,p^2+2)$ or a $\sigma(p,2,p+2)$. If $M_b$ is a $\sigma(1,2,p^2+2)$, then $|E-b| = p^2 + 2$, so $|E| = p^2+2 + |b| = p^2+3$, contrary to (317). If $M_b$ is a $\sigma(p,2,p+2)$, then $|E-b| = p(p+2)$ and $|E| = p^2 + 2p + |b| = p^2 + 2p+1$, again contrary to (317). Therefore $M_b$ is nontrivial for every $b \in P(M)$.

(319) Hence $M_b$ is a $PG(2,p)$ for every $b \in P(M)$. Thus all points and lines of $M$ are simple, and $k(M) = p+2$. Using (317), it follows that $M$ is a matroid design with d-sequence $d(M) = (p^2,p,1,1)$.

(320) If $p \neq 2$, then $d(M) = (4,2,1,1)$, so $M$ is an $EG(3,2)$, by (125).

(321) If $p \neq 2$, consider the number $t_M(0,3,4)$ of hyperplanes in $M$. By (81),

$$t_M(0,3,4) = \frac{(p^2+p)(p^2+p+1)(p^2+p+2)}{p \quad (p+1) \quad (p+2)}$$

$$= \frac{(p^2+p+1)p^2}{p+2} + p^2 + p+1 .$$

Now, since $p > 2$, $p^2$ and $p+2$ are relatively prime, so $\frac{p^2+p+1}{p+2} = p-1 + \frac{3}{p+2}$ must be an integer, which is absurd. Hence, for $p \neq 2$, every member of $\mathfrak{M}_4(p^2)$ is trivial, and thus every member of $\bigcup_{n=4}^{\infty} \mathfrak{M}_n(p^2)$ is trivial, by (239). Thus (i) is proved.

To complete the proof of (ii), we shall show that if $M = (E,\mathcal{I}) \in \mathfrak{M}_5(2^2)$, then $M$ is trivial. If $M$ is non-trivial, then $M_a = M \cdot (E-a)$ is an $EG(3,2)$ for some point $a$ of $M$, by (234) and (320). Using the fact that an $EG(3,2)$ is simple, an argument similar to that of (316)-(318) shows that $M_a$ is an $EG(3,2)$ for every point $a$ of $M$. It follows that $M$ is a matroid design with d-sequence $d(M) = (4,2,1,1,1)$. But then,

$$t_M(0,4,5) = \frac{(4+2)(4+2+1)(4+2+1+1)(4+2+1+1+1)}{2 \cdot 3 \cdot 4 \cdot 5}$$

$$= \frac{6 \cdot 7 \cdot 8 \cdot 9}{2 \cdot 3 \cdot 4 \cdot 5},$$

which is no integer, and therefore no such $M$ exists. Thus every member of $\mathfrak{M}_5(2^2)$ is trivial, which implies, by (239), that every member of $\bigcup_{n=5}^{\infty} \mathfrak{M}_n(2^2)$ is trivial. This, together with (320), proves (ii). ∎

When $p$ and $q$ are distinct primes such that $p < \frac{2}{3}q+1$, the problem of determining $\mathfrak{m}_n(pq)$ for $n \geq 4$ is considerably more difficult in certain cases. For example, we know from the analysis of $W_{24}^*$ in section 4.1 that $\mathfrak{m}_n(6)$ contains nontrivial matroids for every $n$, $3 \leq n \leq 18$. Likewise, $\mathfrak{m}_n(15)$ contains a variety of structures for $n \geq 4$. Excluding these cases, however, we can state some rather general results. In what follows, we shall treat the various cases corresponding to (i), (ii), and (iii) of (308) separately.

(322) Theorem. If $p$ and $q$ are distinct primes such that $q = 2p-1$ and $(p,q) \neq (2,3), (3,5)$, then every member of $\bigcup_{n=4}^{\infty} \mathfrak{m}_n(pq)$ is trivial.

Proof. By (239), it suffices to prove that every member of $\mathfrak{m}_4(pq)$ is trivial. Let $M = (E,\mathcal{H}) \in \mathfrak{m}_4(pq)$ and suppose that $M$ is nontrivial. By (234), $M_a$ is nontrivial for some point $a$ of $M$. Now $M_a \in \mathfrak{m}_3(pq)$, and under our hypotheses the conditions of (308) (iii) are satisfied, so $M_a$ is an $EG(2,p) \ominus \sigma(p,2,p+1)$. The simple points of $M_a$ are certainly simple points of $M$, and since $M_a$ contains at least two such points, (234) and (308) imply that there exists a simple point $b$ of $M$, $b \neq a$, such that $M_b$ is an $EG(2,p) \ominus \sigma(p,2,p+1)$. In

particular,

$$|E-b| = p^2 + p(p+1) = 2p^2+p,$$

(323) so $$|E| = 2p^2 + p+1.$$

(324) Let $d_1,d_2,\ldots,d_{p+1}$ be the $p+1$ $p$-points of $M_b$. $L_i = d_i \cup b$ is then a line of $M$ for each $i$, $1 \leq i \leq p+1$. Suppose that for some $i$, $d_i$ is also a point of $M$. Then $M_{d_i} \in \mathbb{M}_3(pq)$. Since $|E-d_i| = 2p^2 + 1$, $M_{d_i}$ is not an $EG(2,p) \ominus \sigma(p,2,p+1)$, so, by (308), $M_{d_i}$ must be trivial. Since $L_i-d_i$ is a simple point of $M_{d_i}$, $M_{d_i}$ must be a $\sigma(1,2,pq+2)$, the underlying set of which contains $p(2p-1) + 2 = 2p^2-p+2$ elements, contradicting the statement that $|E-d_i| = 2p^2 + 1$. Therefore $d_i$ is not a point of $M$ for $1 \leq i \leq p+1$. In particular, each line $L_i$, $1 \leq i \leq p+1$, contains three distinct points of $M$, $b$, $e_1^i$, $e_2^i$.

(325) Suppose now that $M_c$ is trivial for some point $c$ of $M$. Since $r(M_c) = 3$, this is equivalent to the statement that the union of every two lines of $M$ containing $c$ is a hyperplane of $M$. Let $L_i$ be distinct from $cl(b \cup c)$. Then $c \cap L_i = \emptyset$, and $cl(c \cup e_1^i)$ and $cl(c \cup e_2^i)$ are distinct lines containing $c$ and disjoint from $b$, so $H = cl(c \cup e_1^i) \cup cl(c \cup e_2^i)$

is a hyperplane of $M$ disjoint from $b$. But $L_i = cl(\{e_1^i, e_2^i\})$ and $H$ is closed, so $b \subseteq L_i \subseteq H$, a contradiction. Therefore $M_c$ is nontrivial for every $c \in P(M)$.

By (308) it follows that $M_c$ is an $EG(2,p) \ominus \sigma(p,2,p+1)$ for every $c \in P(M)$. In particular, by (323), every point of $M$ is simple. Now an $EG(2,p)$ contains exactly $p^2+p$ lines, and a $\sigma(p,2,p+1)$ contains $\binom{p+1}{2} = \frac{p^2+p}{2}$ lines. Thus, by construction, an $EG(2,p) \ominus \sigma(p,2,p+1)$ contains exactly $p^2 + p + \frac{p^2+p}{2} = \frac{3(p^2+p)}{2}$ lines, and further, each line has cardinality $2p$. Therefore every point of $M = (E,\mathcal{H})$ is contained in exactly $\frac{3}{2}(p^2+p)$ hyperplanes of cardinality $2p+1$, so

$$|\mathcal{H}| = \frac{3(p^2+p)}{2} \cdot \frac{(2p^2+p+1)}{2p+1} .$$

Now

$$\frac{3}{2}(p^2+p) \cdot \frac{2p^2+p+1}{2p+1} = \frac{3p}{2}(p^2+p) + \frac{3(p^2+p)}{2(2p+1)} ,$$

and $\frac{3p(p^2+p)}{2}$ is an integer, so $2(2p+1) \mid 3(p^2+p)$. Since $p$ is a prime and $p \neq 2$ by hypothesis, we must have $2(2p+1) \mid 3(p+1)$, and so $4p+2 \leq 3p+3$, which is absurd. Therefore every member of $\mathfrak{M}_4(pq)$, and hence of $\bigcup_{n=4}^{\infty} \mathfrak{M}_n(pq)$, is trivial. ∎

Preparatory to considering $\bigcup_{n=4}^{\infty} \mathfrak{m}_n(pq)$ for cases (i) and (ii) of (263), we shall establish a general result concerning the independence number, $\beta(M)$, of an equicardinal matroid $M$.

(326) Theorem. If, for some integers $\gamma \geq 1$, $n \geq 3$, and $m \geq 2$, every nontrivial matroid $M \in \mathfrak{m}_n(\gamma)$ satisfies $\beta(M) \geq m$, then for every integer $n' \geq n$ and every nontrivial matroid $M' \in \mathfrak{m}_{n'}(\gamma)$, $\beta(M') \geq m + (n'-n)$.

Proof.

(327) First, if every member of $\mathfrak{m}_n(\gamma)$ is trivial, then every member of $\mathfrak{m}_{n'}(\gamma)$ is trivial for $n' \geq n$, by (239), and the theorem is vacuously true.

(328) Second, let us observe that $m \leq n$, since for any $M \in \mathfrak{m}_n(\gamma)$, $\beta(M) \leq r(M)$.

(329) Now let us assume that the theorem holds for all integers $n'$, $n \leq n' < N$, and we shall prove it for $n' = N$. (The theorem obviously holds if $n' = n$.) Let $M = (E,\mathcal{H})$ be a nontrivial member of $\mathfrak{m}_N(\gamma)$.

If $M$ is nonsimple, let $a \in P(M)$, $|a| > 1$. Let $b$ and $c$ be points of $M$ distinct from $a$. Then $M_b$, $M_c \in \mathfrak{m}_{N-1}(\gamma)$, but neither of $M_b$ and $M_c$ is simple, so $\beta(M_b) = \beta(M_c) = 1$.

But, by (234), at least one of $M_b$ and $M_c$ is nontrivial, and, by the induction hypothesis, every nontrivial $M' \in \mathfrak{M}_{N-1}(\gamma)$ satisfies $\beta(M') \geq m \geq 2$. This contradiction proves that $M$ is simple.

(330) Suppose that $M$ contains a line $L$ such that $|L| \geq 3$. Let $a_1, a_2, a_3$ be distinct elements of $L$. For each $i$, $L-a_i$ is a point of $M_{a_i} = M \cdot (E-a_i)$, so $M_{a_i}$ is nonsimple, and therefore a trivioid, by the induction hypothesis. But then $M$ is a trivioid, contrary to hypothesis. Hence every line of $M$ is simple.

(331) Let $S$ be any subset of $E$ having cardinality $m + N-n$ and let $x \in S$. Then $M_{(x)} \in \mathfrak{M}_{N-1}(\gamma)$. If $M_{(x)}$ is a nontrivial, then by the induction hypothesis the $(m+N-n-1)$-subset $S-(x)$ is independent in $M_{(x)}$, so $S$ is independent in $M$, by the definition of contraction (36). If $M_{(x)}$ is trivial, then, since every line of $M$ is simple, it must be the simple trivioid $\sigma(1,k(M)-1,|E|-1)$. Since $r(M_{(x)}) = N-1$, every $(N-1)$-subset of $E-(x)$ is independent in $M_{(x)}$. Finally by (328), $m \leq n$, so $m+N-n-1 \leq N-1$. Thus $S-(x)$ is independent in $M_{(x)}$, from which it follows that $S$ is independnet in $M$. ∎

(332) Corollary. If, for some $\gamma \geq 1$, every nontrivial member of $\mathfrak{M}_3(\gamma)$ is simple, then, for $n \geq 3$, every nontrivial $M = (E,\mathfrak{N}) \in \mathfrak{M}_n(\gamma)$ is a $D_{n-1}(|E|, k(M),1)$.

Proof. A matroid $M_0$ is simple if and only if $\beta(M_0) \geq 2$. Hence, for any nontrivial $M = (E,\mathfrak{N}) \in \mathfrak{M}_n(\gamma)$, (326) implies that $\beta(M) \geq 2 + n-3 = n-1$. Thus $d(M) = (\gamma, k(M)-n+2,1,\cdots,1)$, and so $M$ is a $D_{n-1}(|E|, k(M),1)$, by (112). ∎

(333) Theorem. If $p$ and $q$ are distinct primes such that $(p+1) \mid (q+1)$, then, for $n \geq 3$, every nontrivial member of $\mathfrak{M}_n(pq)$ is a $D_{n-1}(pq+p+n-2, p+n-2,1)$.

Proof. If $p$ and $q$ are distinct primes such that $(p+1) \mid (q+1)$, then certainly $p < \frac{2}{3} q+1$, and, further, $(p,q) \neq (2,3), (3,5)$.

Hence, by (308) (i), every nontrivial member of $\mathfrak{M}_3(pq)$ is a $D_2(pq+p+1,p+1,1)$, and is therefore simple. By (332), any nontrivial $M = (E,\mathfrak{N}) \in \mathfrak{M}_n(pq)$ is, therefore, a $D_{n-1}(|E|, k(M),1)$. By (112), $d(M) = (pq,\alpha,1,\cdots,1)$, a sequence with $n$ terms. Since $d(M)$ is D-consistent, $\frac{pq}{\alpha} \geq \frac{\alpha}{1}$ and $\alpha \mid pq$, so $\alpha = p$. Therefore $d(M) = (pq,p,1,\cdots,1)$, so, by (81),

$$|E| = pq+p+n-2$$

and

$$k(M) = p+n-q.$$

Thus, $M$ is a $D_{n-1}(pq+p+n-2, p+n-2,1)$. ∎

In the final case, where $p$ and $q$ are distinct primes satisfying $p < \frac{2}{3}q+1$ and $(p+1) \mid (pq+1)$, the variety of structures possible in $\mathfrak{M}_n(pq)$, $n \geq 4$, is considerable. We shall, therefore, restrict our attention to the analysis of $\mathfrak{M}_4(pq)$ in this instance.

As a preliminary, we are going to introduce a generalization of t-designs that has a considerable theoretical interest in its own right, and also provides us with a method for constructing an infinite class of simple rank 4 equicardinal matroids that are not matroid designs.

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

(334) A triple $(E,\mathcal{S},\mathcal{J})$ is a <u>transversal design</u> with parameters $t,v,s,k,\lambda$, where $v \geq k \geq t \geq 2$, $s \geq 1$, $\lambda \geq 1$, if:

(i) $\mathcal{S}$ is a family of $v$ nonempty disjoint subsets that partition the finite set $E$ and $|S| = s$ for every $S \in \mathcal{S}$;

(ii) $\mathcal{J}$ is a family of PT's of $\mathcal{S}$ such that $|T| = k$ for every $T \in \mathcal{J}$;

(iii) every PT of length $t$ is contained in exactly $\lambda$ members of $\mathcal{J}$.

For short we refer to any such triple $(E,\mathcal{S},\mathcal{J})$ as a $\underline{TD_t(v,s,k,\lambda)}$.

For a given $TD_t(v,s,k,\lambda)$, $\mathcal{D} = (E,\mathcal{S},\mathcal{J})$, let $\lambda_i$, $0 \leq i \leq t$, be the number of members of $\mathcal{J}$ containing a given PT of $\mathcal{S}$ having length $i$. Where $T_i$ is any PT of $\mathcal{S}$ having length $i$, there are $\binom{v-i}{t-i}s^{t-i}$ PT's of length $t$ containing $T_i$, and $\lambda$ members of $\mathcal{J}$ containing each such PT of length $t$. Further, each PT of length $k$ containing $T_i$ contains $\binom{k-i}{t-i}$ PT's of length $t$ containing $T_i$. Thus $\lambda_i$ is well-defined and

$$\lambda_i = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} s^{t-i}, \quad 0 \leq i \leq t. \tag{335}$$

In particular, $\lambda_t = \lambda$, and $\lambda_0 = |\mathcal{J}|$. The parameters $t,v,s,k,\lambda$ are said to be $\underline{\text{consistent}}$ if the numbers $\lambda_i$ of (335) are integers.

Transversal designs are a generalization of t-designs, for it is clear that a $TD_t(v,1,k,\lambda)$ is the same as a $D_t(v,k,\lambda)$. One may think of a TD as a t-design with an "extra dimension". As we have already observed, the integrality of the numbers $\lambda_i$ is not sufficient to guarantee the existence of a BlBD; hence this observation holds more

generally for TD's. It is conceivable, however, that because of the "extra dimension" of a TD for which $s > 1$, the integrality of the $\lambda_i$'s are more nearly sufficient conditions for existence than they are in the case of BIBD's.

We remark that TD's for which $t = 2$, $v = k$, and $\lambda = 1$ have been used by Hanani in [7 ], under the name "T-systems", to construct certain BIBD's. To the author's knowledge, this is the only place in which these objects have previously been singled out for attention. Some of the results of section 4.8 will generalize on those of Hanani.

Now we shall see how certain TD's may be used to construct simple rank 4 equicardinal matroids.

(336) Theorem. Let $(E,\mathcal{S},\mathcal{J})$ be a $TD_3(v,s,s+1,1)$ for some integer $s \geq 2$, and let $\mathcal{H}$ be the family $\mathcal{J} \cup \{S \cup \{x\}: S \in \mathcal{S}$ and $x \in E-S\}$ of $(s+1)$-subsets of $E$. Then $(E,\mathcal{H})$ is simple rank 4 equicardinal matroid, called an EM(v,s), and, if $s \geq 3$, $(E,\mathcal{H})$ is not a matroid design.

Proof. Let $(E,\mathcal{S},\mathcal{J})$ and $M = (E,\mathcal{H})$ be as above, and let $\mathcal{S} = \{S_1,S_2,\ldots,S_v\}$. The members of $\mathcal{H}$ all have cardinality $s+1$, by construction.

(337) Let $H_1$ and $H_2$ be distinct members of $\mathcal{H}$. Then either $H_1 \cap H_2 = S_j$ for some $j$, $1 \leq j \leq v$, or else $|(H_1 \cap H_2) \cap S_i| \leq 1$

for $1 \leq i \leq v$. In the latter cases, $H_1 \cap H_2$ is a PT of $\mathcal{S}$. If $|H_1 \cap H_2| > 2$, then not both $H_1, H_2 \in \mathfrak{I}$; hence one, say $H_1$, may be written as $S_i \cup \{x\}$ for some $S_i \in \mathcal{S}$ and $x \in E-S_i$. Since $H_1 \cap H_2 \neq S_i$, it follows that $|H_1 \cap (S_i \cup \{x\})| \leq 2$, contrary to assumption. Therefore, either $H_1 \cap H_2 \in \mathcal{S}$, or $H_1 \cap H_2$ is a PT of length 2 or less.

(338) Conversely, since $s \geq 2$, every $S_i$ may be written as $S_i = (S_i \cup \{x\}) \cap (S_i \cup \{y\})$, where $x$ and $y$ are distinct members of $S_j$ for some $j \neq i$. Likewise, every $PT\{x,y\}$ of $\mathcal{S}$ of length 2, where $x \in S_i$ and $y \in S_j$, may be written as $\{x,y\} = (S_i \cup \{y\}) \cap (S_j \cup \{x\})$. Hence the members of $\mathcal{S}$, and the length-2 PT's of $\mathcal{S}$, may each be represented as an intersection of members of $\mathcal{H}$.

(339) Let $\mathfrak{I}_2$ be the set of length-2 PT's of $\mathcal{S}$, and let $\mathfrak{L} = \mathfrak{I}_2 \cup \mathcal{S}$. Then, clearly, every two distinct elements in $E$ are contained in a unique member of $\mathfrak{L}$.

We shall show that for every $L \in \mathfrak{L}$ and $x \in E-L$, $L \cup \{x\}$ is contained in a member of $\mathcal{H}$, and it will follow from (337)-(339) that $M$ is a simple matroid with line-family $\mathfrak{L}$ and hyperplane-family $\mathcal{H}$. Thus we shall have $r(M) = 4$,

and $M$ will be a matroid design if and only if the lines are equicardinal, that is, if and only if $s = 2$.

(340) Let $L \in \mathfrak{L}$ and $x \in E-L$. If $L = S_i$ for some $i$, then $L \cup \{x\} \in \mathfrak{H}$ by construction. Otherwise, $L = \{a,b\}$ for some $a \in S_i$ and $b \in S_j$, where $i \neq j$. If $x \in S_j$, then $L \cup \{x\} \subseteq S_j \cup \{a\} \in \mathfrak{H}$, and a similar result holds if $x \in S_i$. Otherwise, $x \in S_k$ for some index $k$ distinct from $i$ and $j$. Then $\{a,b,x\}$ is a partial transversal of length 3, hence it is contained in a unique member of $\mathfrak{J} \subseteq \mathfrak{H}$. ∎

(341) For future reference, let us observe that if $M$ is an $EM(v,s)$, then $k(M) = s+1$ and $c^*(M) = vs-s-1$.

Now we are prepared to characterize $\mathfrak{M}_4(pq)$ in the final case as follows.

(342) Theorem. If $p$ and $q$ are distinct primes such that $p < \frac{2}{3}q+1$ and $(p+1) \mid (pq+1)$ but $(p,q) \neq (2,3)$, $(p,q) \neq (3,5)$, then every nontrivial member of $\mathfrak{M}_4(pq)$ is: (i) a $D_3(pq+2,p+2,1) \oplus P_{(p)}$, or (ii) an $EM(\frac{pq+1}{p+1} + 1, p+1)$.

Proof. Let $M = (E,\mathfrak{H}) \in \mathfrak{M}_4(pq)$, where $p$ and $q$ are as hypothesized and $M$ is nontrivial.

(343) Suppose first that $M$ is not simple, and let $a \in P(M)$, $|a| > 1$.

(344) By (234) and (308), there is a point $b \neq a$ such that $M_b$ is a $D_2(pq+1,p+1,1) \oplus P_{(p)}$, which we abbreviate for this discussion by $D_2(p)$. Evidently, $cl_M(aUb) - b$ is the unique nonsimple point of $M_b$, hence every point in $P(M) - P(cl_M(aUb))$ must be simple. There are at least two such points; hence there is a simple point $c \in P(M) - P(cl_M(aUb)$ such that $M_c$ is a $D_2(p)$. Then, as above, we conclude that every point in $P(M) - P(cl_M(aUc))$ is simple. Since $cl_M(aUc) \cap cl_M(aUb) = a$, it follows that $(P(M) - P(cl_M(aUc)) \cup (P(M) - P(cl_M(aUb)) = P(M) - \{a\}$, so $a$ is the unique nonsimple point of $M$. Moreover, since $|a| \neq |b|$, $M_a$ and $M_b$ are nonisomorphic matroids. Thus, $M_a$ is not a $D_2(p)$, so, by (308), $M_a$ is a trivioid.

(345) Let $\alpha$ be the common cardinality of the points of $M_a$. Then $\alpha | c^*(M_a) = pq$; hence $\alpha = 1$, $p$, $q$, or $pq$. Suppose that $\alpha \geq p$, and let $L$ be a line of $M$ containing $a$. Then $|L-a| = \alpha \geq p \geq 2$. Since the points of $M$ in $L-a$ are simple, $M_d$ is nontrivial, hence a $D_2(p)$, for some simple point $d$ in $L-a$. Therefore $L-d$ is a point of $M_d$, and $|L-d| > p$, since $|d| = 1 < \alpha$. But a $D_2(p)$ contains no $m$-point for $m > p$. Hence $\alpha = 1$, and since $r(M_a) = 3$ and $c^*(M_a) = pq$, $M_a$ is a $\sigma(1,2,pq+2)$.

Now $M_b$ is a $D_2(p)$, so

$$\left| \bigcup_{w \in P(M_b)} w \right| = pq + p+1$$

and

(346) $$|E| = pq + p+1 + |b| = pq + p+2.$$

On the other hand,

$$\left| \bigcup_{w \in P(M_a)} w \right| = pq + 2, \quad \text{by (345)},$$

so

(347) $$|a| = p.$$

Finally,

(348) $$k(M) = |E| - c^*(M) = pq + p+2 - pq = p+2.$$

(349) Let $\mathfrak{L}'$ be the family of lines of $M$ contained in $E-a$. For any distinct elements $x,y \in E-a$, $L = cl_M(\{x,y\}) \in \mathfrak{L}'$, for otherwise $a \subseteq L$, and hence $|L| \geq p+2 = k(M)$, which is absurd, because $L$ is properly contained in some hyperplane of $M$. For any $L \in \mathfrak{L}'$, $cl_M(L \cup a) \in \mathcal{H}$, and hence $|cl_M(L \cup a)| = p+2$. Since $|a| = p$, $|L| = 2$; hence every member of $\mathfrak{L}'$ is simple.

(350) Let $\mathcal{H}'$ be the family of hyperplanes of $M$ contained in $E-a$. For any $L \in \mathfrak{L}'$ and $x \in (E-a) - L$, $H = cl_M(L \cup \{x\}) \in \mathcal{H}'$, for otherwise $|H| \geq |L \cup \{x\}| + |a| = p+3 > k(M)$, which is absurd.

By (348) - (350), $M' = (E-a, \mathcal{H}')$ is a simple, rank 4

matroid design, and $d(M') = (pq,p,1,1)$. Therefore $M'$ is a $D_3(pq+2,p+2,1)$. Moreover, it is easy to see that $M = M' \oplus a$, so $M$ is a $D_3(pq+2,p+2,1) \oplus P(p)$.

(351) Suppose now that (343) does not hold; i.e., suppose that $M$ is simple. Then $M_a$ is a $D_2(p)$ for some $a \in P(M)$, and it follows by considering the sizes of the possible trivoids in $\mathfrak{M}_3(pq)$ that $M_a$ is a $D_2(p)$ for every $a \in P(M)$. We also note that $|E| = pq + p+2$ and $k(M) = p+2$.

(352) Since a $D_2(p)$ contains exactly one nonsimple point, which has cardinality $p$, it follows that every point of $M$ is incident with exactly one nonsimple line, which has cardinality $p+1$. Thus $E$ is partitioned by $v = \frac{pq + p+2}{p+1} = \frac{pq + 1}{p+1} + 1$ lines of cardinality $p+1$. Let the family of these lines be denoted by $\mathcal{S} = \{S_1,S_2,\ldots,S_v\}$. Since $k(M) = p+2$, $S_i \cup \{x\} \in \mathcal{H}$ for any $S_i \in \mathcal{S}$ and $x \in E-S_i$. Let $\mathcal{H}' = \{S_i \cup \{x\}: S_i \in \mathcal{S} \text{ and } x \in E-S_i\}$. For any $H \in \mathcal{H}-\mathcal{H}'$, $|H \cap S_i| \leq 1$ for every $S_i \in \mathcal{S}$ (since $H$ is closed); thus, $H$ is a partial transversal of $\mathcal{S}$ of length $p+2$.

For any partial transversal $\{x,y,z\}$ of $\mathcal{S}$ having length 3, $\{x,y,z\}$ is contained in no line of $M$, hence $H = cl(\{x,y,z\}) \in \mathcal{H}$, and, clearly, $H \in \mathcal{H}-\mathcal{H}'$. Thus, $(E,\mathcal{S},\mathcal{H}-\mathcal{H}')$

is a $TD_3(\frac{pq+1}{p+1} + 1,\ p+1,p+2,1)$, and, by (352), M is an $EM(\frac{pq+1}{p+1},\ p+1)$. ∎

(353) We point out that, for some values of p and q satisfying the conditions of (342), neither (i) nor (ii) is possible. For example, the pair $(p,q) = (3,17)$ satisfies the conditions of (342). However, a design $D_3(53,5,1)$ must contain

$$\lambda_0 = \frac{\binom{53}{3}}{\binom{5}{3}} = \frac{53\cdot 52\cdot 51}{5\cdot 4\cdot 3} \quad \text{blocks},$$

(by (335) with s=1), which is no integer, so there exists no $D_3(53,5,1)$. Likewise, an $EM(14,4)$ can exist only if a $TD_3(14,4,5,1)$ exists, which is impossible because

$$\lambda_0 = \frac{\binom{14}{3}}{\binom{5}{3}} 4^3 = \frac{14\cdot 13\cdot 12\cdot 4^3}{5\cdot 4\cdot 3}$$

is no integer. Therefore, by (239) and (342), there exists no nontrivial connected equicardinal matroid M such that $c^*(M) = 51$ and $r(M) \geq 4$. Further, by (263), every $M \in \mathfrak{M}_3(51)$ is a $D_2(52,4,1)$, which does exist [5 ]. Appendix II lists other co-circuit cardinalities for which only rank 3 nontrivial equicardinal matroids exist.

Determining the nontrivial members of $\mathfrak{M}_4(6)$ and $\mathfrak{M}_4(15)$ is a more difficult task than were the preceding cases, but the method of analysis is similar. We shall therefore simply present the end results.

(354) In (210) we showed that the equicardinal matroids $EG(3,2) \oplus P(2)$, $\mathcal{Y}$, and $IP(3)$ occur as rank 4 contractions of $W_{24}^*$; hence these matroids are nontrivial members of $\mathfrak{M}_4(6)$. The only other nontrivial member of $\mathfrak{M}_4(6)$ is a special matroid, $\Lambda$, which we shall now briefly describe.

Let $E'$ be a set of 9 elements, and let $\mathcal{L}_i = \{L_1^i, L_2^i, L_3^i\}$ for $i = 1,2,3,4$, be the parallel classes of an $EG(2,3)$ on the set $E'$. We choose two "distinguished" parallel classes, say $\mathcal{L}_1$ and $\mathcal{L}_2$, and let $\mathcal{H}_1 = \{L \cup L' : L \in \mathcal{L}_1 \text{ and } L' \in \mathcal{L}_2\}$. Now let $a$ be a 2-set disjoint from $E'$, and let $\mathcal{H}_2 = \{L \cup a : L \in \bigcup_{i=1}^{4} \mathcal{L}_i\}$. Then it is straightforward to check that $\Lambda = (E' \cup a, \mathcal{H}_1 \cup \mathcal{H}_2)$ is a rank 4, connected equicardinal matroid and that $k(\Lambda) = 5$, $c^*(\Lambda) = 6$. Thus, $\Lambda \in \mathfrak{M}_4(6)$. The points of $\Lambda$ are all simple except for $a$, and the lines of $\Lambda$ are all elementary except for the family of lines $\mathcal{L}_1 \cup \mathcal{L}_2$, each of which contains 3 simple points.

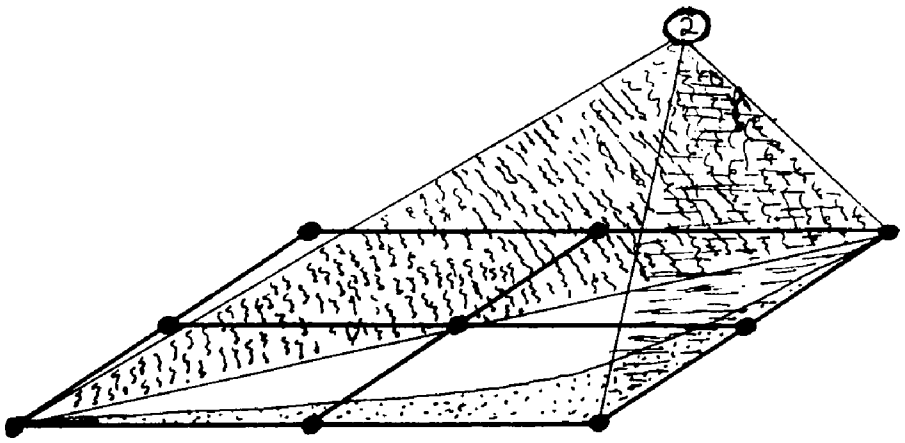


Fig. 7-- The equicardinal matroid $\Lambda$

(355) Now let us consider $\mathfrak{M}_4(15)$. Using constructions like these used in the proof of (342), it is easy to discover that $D_3(17,5,1) \oplus P(3)$ and $EM(5,4)$ are members of $\mathfrak{M}_4(15)$, and both are nontrivial. (There exists a $D_3(17,5,1)$, namely an $IP(4)$; in the next section, we shall prove that an $EM(5,4)$ exists.) The only other nontrivial member of $\mathfrak{M}_4(15)$ is a special matroid, $\Omega$, which we shall now describe.

Let $E'$ be a set of 16 elements, and let $\mathfrak{L}_i = \{L_1^i, L_2^i, L_3^i, L_4^i\}$, for $i = 1,2,3,4,5$, be the parallel classes of an $EG(2,4)$ on $E'$. We choose two distinguished parallel classes, say $\mathfrak{L}_1$ and $\mathfrak{L}_2$, and let $\mathfrak{H}_1 = \{L \cup L' : L \in \mathfrak{L}_1 \text{ and } L' \in \mathfrak{L}_2\}$.

Let $\mathcal{S}$ be the set of all 4-subsets of $E'$, no two members of which are contained together in a member of $\mathcal{L}_1 \cup \mathcal{L}_2$. It is easy to see that $|\mathcal{S}| = 4 \cdot 3 \cdot 2 \cdot 1 = 24$. Further, $\mathcal{L}_3 \cup \mathcal{L}_4 \cup \mathcal{L}_5 \subseteq \mathcal{S}$, and $|\mathcal{L}_3 \cup \mathcal{L}_4 \cup \mathcal{L}_5| = 12$. Letting $\mathcal{S}' = \mathcal{S} - (\mathcal{L}_3 \cup \mathcal{L}_4 \cup \mathcal{L}_5)$, it follows that $|\mathcal{S}'| = 12$, and it is not difficult to see that $\mathcal{S}'$ may also be partitioned into three parallel classes, say $\mathcal{L}_3'$, $\mathcal{L}_4'$, and $\mathcal{L}_5'$.

Now let $a$ and $b$ be two disjoint 3-sets that are disjoint from $E'$. Define

$$\mathcal{H}_2 = \{L \cup a : L \in \mathcal{L}_1 \cup \mathcal{L}_2\},$$

$$\mathcal{H}_3 = \{L \cup a : L \in \mathcal{S}\},$$

$$\mathcal{H}_4 = \{L \cup b : L \in \mathcal{S}'\},$$

and

$$\mathcal{H}_5 = \{\{x\} \cup a \cup b : x \in E'\}.$$

It is then a straightforward matter to verify that $\Omega = (E' \cup a \cup b, \bigcup_{i=1}^{5} \mathcal{H}_i)$ is a rank 4, connected, equicardinal matroid and $k(\Omega) = 7$, $c^*(\Omega) = 15$. Thus, $\Omega \in \mathfrak{M}_4(15)$. The points of $\Omega$ are all simple, except for $a$ and $b$, and the lines of $\Omega$ are all elementary, except for the family of lines $\mathcal{L}_1 \cup \mathcal{L}_2$, each of which contains 4 simple points.

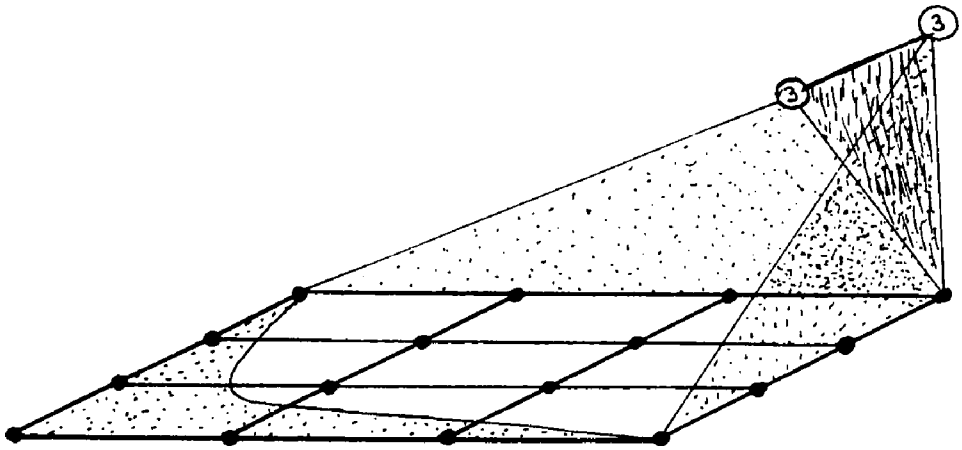



Fig. 8-- The equicardinal matroid $\Omega$

## 4.8. Transversal designs

Theorem (336) identifies a certain class of equicardinal matroids that arise from TD's and this class is used in theorem (342) to characterize $m_4(pq)$ for certain values of p and q. It would be useful, therefore, to have a theory concerning the existence of TD's, particularly those TD's of form $TD_3(v,s,s+1,1)$, which are used in the construction of equicardinal matroids. In this section we shall establish the elements of such a theory.

(356) Theorem. A $TD_t(k,s,k,1)$ such that $s > 1$ must satisfy $k \leq s+t-1$.

Proof. Let $\mathcal{D} = (E,\mathcal{S},\mathcal{J})$ be a $TD_t(k,s,k,1)$ such that $s > 1$, and let $\mathcal{S} = \{S_1, S_2,\ldots,S_k\}$. By definition of a TD, $t \geq 2$. Let $U = \{a_1, a_2,\ldots,a_{t-1}\}$ be a fixed PT of $\mathcal{S}$ such that $a_i \in S_i$ for $1 \leq i \leq t-1$. Since every PT of $\mathcal{S}$ having length $t$ is contained in a unique member of $\mathcal{J}$, the set $\mathcal{J}_0 = \{T-U: T\in\mathcal{J} \text{ and } U\subseteq T\}$ is a family of $s$ disjoint subsets of $E' = \bigcup_{i=t}^{k} S_i$, and $\bigcup_{T'\in\mathcal{J}_0} T' = E'$. Since $s > 1$, there is an element $b \in S_{t-1}-\{a_{t-1}\}$. Let $T_b$ be a member of $\mathcal{J}$ containing the PT $V = \{a_1, a_2,\ldots,a_{t-2},b\}$. Now $V \subseteq T_b \cap T$ for every $T \in \mathcal{J}$ such that $U \subseteq T$, so $|T_b-V) \cap T'| \leq 1$ for every $T' \in \mathcal{J}_0$. Since $|\mathcal{J}_0| = s$ and $\bigcup_{T'\in\mathcal{J}_0} T' = E'$, it follows that $|T_b-V| \leq s$; hence $k = |T_b| \leq s + |V| = s+t-1$. ∎

Our next theorem relates the existence of certain TD's to the existence of finite geometries.

(357) Theorem. If there exists a $TD_t(k,s,k,1)$ such that $s > 1$ and $k \geq s+t-2$, then there exists a $PG(2,s)$.

Proof. Let $(E,\mathcal{S},\mathcal{J})$ be a $TD_t(k,s,k,1)$ as above, and let $\mathcal{S} = \{S_1, S_2,\ldots,S_k\}$. By our hypotheses and (356), $s+t-2 \leq k \leq s+t-1$. Let $U = \{a_1, a_2,\ldots a_{b-2}\}$ be a fixed PT of $\mathcal{S}$ such that $a_i \in S_i$ for $1 \leq i \leq t-2$, where $U = \emptyset$

if $t = 2$. Let $E' = \bigcup_{i=k-s+1}^{k} S_i$, and let $\mathcal{T}' = \{T-u: T \in \mathcal{T}$ and $U \subseteq T\}$. Then every length - 2 PT of the set $\mathcal{S}' = \{S_{k-s+1},\ldots,S_k\}$ is contained in a unique member of $\mathcal{T}'$. Then every member of $\mathcal{B}' = \mathcal{S}' \cup \mathcal{T}'$ has cardinality $s$, and every two elements of $E'$ are contained in a unique member of $\mathcal{B}'$. Therefore $M' = (E',\mathcal{B}')$ is a matroid design, and, since $|E'| = s^2$, we have that $d(M') = (s(s-1),s-1,1)$. Therefore, by (125), $M'$ is an $EG(2,s)$. Hence there also exists a $PG(2,s)$, by (76). ∎

(358) It is clear from (335) that the parameters of a $TD_t(k,s,k,1)$ are always consistent. But, by the Bruck-Ryser Theorem (74) and (357), there are nevertheless many values of $s,k$, and $t$ for which a $TD_t(k,s,k,1)$ does not exist.

Next, we shall construct several series of TD's with $t = 3$, $k = s+1$ and $\lambda = 1$, to which the construction of (336) applies. First, we shall establish a theorem based on a result of Bose [ 3] in confounding theory.

For any prime power $q$ and positive integer $N$, let $m_N(N,q)$ be the maximum cardinality of a set $V$ of N-vectors over $GF(q)$ such that every N-subset of $V$ is independent.

(359) Theorem. For any prime power $q$,

(i) $$m_2(2,q) = q+1.$$

(ii) $$m_3(3,q) = \begin{cases} q+2, & \text{if } q \text{ is even.} \\ q+1, & \text{if } q \text{ is odd.} \end{cases}$$

(iii) $m_N(N,q) \geq N+3$, if $q$ is even and $N \leq q-1$, or if $q$ is odd and $N \leq q-2$.

Proof.

(360) (i) and (ii) are well-known, and proved in [ 3 ] by Bose.

(361) The following arrays $A_q$ and $B_q$ (due to Stanton [16 ]) exhibit $m_3(3,q)$ 3-vectors over $GF(q)$ no 3 of which are dependent, for the cases $q$ even and $q$ odd, respectively. In each case, $x$ is a primitive root of $GF(q)$.

$$A_q = \begin{pmatrix} 1 & 0 & 0 & x & x^2 & \cdots & x^{\frac{1}{2}(q-2)} & x^{\frac{1}{2}q} & x^{\frac{1}{2}(q+2)} & \cdots & x^{q-1} \\ 0 & 1 & 0 & x^2 & x^4 & \cdots & x^{q-2} & x & x^3 & \cdots & x^{q-1} \\ 0 & 0 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}.$$

$$B_q = \begin{pmatrix} 1 & 0 & 0 & x & x^2 & \cdots & x^{\frac{1}{2}(q-3)} & x^{\frac{1}{2}(q-1)} & x^{\frac{1}{2}(q+1)} & \cdots & x^{q-2} \\ 0 & 1 & 0 & x^2 & x^4 & \cdots & x^{q-3} & x & x & \cdots & x^{q-2} \\ 0 & 0 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}.$$

Let $$\begin{pmatrix} 1 & 0 & 0 & a_{11} & a_{12} & \cdots & a_{1r} \\ 0 & 1 & 0 & a_{21} & a_{22} & & a_{2r} \\ 0 & 0 & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$$

be a schematic representation of the arrays $A_q$ and $B_q$. We note the following properties of $A_q$ and $B_q$.

(362) $a_{1i} \neq 0$ and $a_{2i} \neq 0$, for every $i$.

(363) $a_{1i} \neq a_{1j}$ and $a_{2i} \neq a_{2j}$, for $i \neq j$,

(364) and $\dfrac{a_{1i}}{a_{2i}} \neq \dfrac{a_{1j}}{a_{2j}}$, for $i \neq j$.

These relations follow at once by inspection.

(365) Now let $I_N$ be the $N \times N$ unit matrix, and let

$$A'_q = \begin{pmatrix} x & x^2 & \dots & x^{\frac{1}{2}(q-2)} & x^{\frac{1}{2}q} & x^{\frac{1}{2}(q+1)} & \dots & x^{q-1} \\ x^2 & x^4 & \dots & x^{q-2} & x & x^3 & \dots & x^{q-1} \\ 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \\ I_N & & & & O & & & \end{pmatrix} \text{ for } q \text{ even,}$$

$$B'_q = \begin{pmatrix} x & x^2 & \dots & x^{\frac{1}{2}(q-3)} & x^{\frac{1}{2}(q-1)} & x^{\frac{1}{2}(q+1)} & \dots & x^{q-2} \\ x^2 & x^4 & \dots & x^{q-3} & x & x^3 & \dots & x^{q-2} \\ 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \\ I_N & & & & O & & & \end{pmatrix} \text{ for } q \text{ odd.}$$

Since, by hypothesis, $N \leq q-1$ if $q$ is even and $N \leq q-2$ if $q$ is odd, we may truncate $A'_q$ and $B'_q$ to the first $N$ columns. Call these truncations $A''_q$ and $B''_q$, respectively. We claim that every $N \times N$ submatrix $A$ of $A''_q$ (or $B''_q$) has column rank $N$. Indeed, suppose that $A(\alpha_1, \dots, \alpha_N)^T = 0$ for some $N$-vector $\alpha$. Let $A$ contain $r$ rows from $I_N$; clearly $r \geq N-3$. Then at most $N-r$ components of $\alpha$ are nonzero. But $N-r \leq 3$, so this implies a dependency relation among the columns of an

$(N-r) \times (N-r)$ submatrix of $A_q$, which is impossible, by (362)-(364). Hence $A_q''$, and likewise $B_q''$, have column rank $N$, so their row rank is $N$. Hence the rows of $A_q''$ ($B_q''$) are a family of $N+3$ $N$-vectors over $GF(q)$, every $N$ of which are independent. ∎

(366) Theorem. For every prime power $q$, there exists a $TD_3(q+1,q,q+1,1)$, and hence an $EM(q+1,q)$.

Proof.

(367) Let $q$ be given, let $x$ be a primitive root of $GF(q)$, and let $\mathcal{S}$ consist of the disjoint $q$-sets $S_i = \{(i,0), (i,x), \cdots (i,x^{q-1})\}$, $1 \leq i \leq q+1$. With $N = q-2$, we may apply (359) to obtain a $(q-2) \times (q+1)$ matrix $B$ over $GF(q)$, every $q-2$ columns of which are independent. Let $V$ denote the set of all $(q+1)$-tuples over $GF(q)$, let $y = (y_1, y_2, \cdots, y_{q+1})$ be a vector variable ranging over $V$, and let $\mathcal{T}$ be the set of all partial transversals $T_y = \{(i,y_i): 1 \leq i \leq q+1\}$ such that $B_y = 0$. Let $T = \{(j,a), (k,b), (\ell,c)\}$, $j \neq k \neq \ell \neq j$, be any length-3 PT of $\mathcal{S}$. By choice of $B$, there is one and only one solution $y^* \in V$ of $By = 0$ such that $y_j^* = a$, $y_k^* = b$, and $y_\ell^* = c$. Hence $T_{y^*}$ is the unique member of $\mathcal{T}$ containing $T$. Thus

$(\bigcup_{i=1}^{q+1} S_i, \mathcal{S}, \mathcal{J})$ is a $TD_3(q+1,q,q+1,1)$. The existence of an $EM(q+1,q)$ follows from (336). ∎

As in the case of t-designs, we may "compose" certain pairs of TD's, as shown in the following theorem.

(368) **Theorem.** If there exists a $TD_t(v,s,k,1)$ and a $TD_t(w,s',v,\lambda')$, then there exists a $TD_t(w,ss',k,\lambda')$.

*Proof.* Let $(E',\mathcal{S}',\mathcal{J}')$ be a $TD_t(w,s',v,\lambda')$, where $\mathcal{S}' = \{S_1',S_2',\ldots,S_w'\}$, and the members of $E'$ are chosen to be disjoint sets, each of cardinality $s$. Then each $T \in \mathcal{J}'$ is a collection of $v$ disjoint $s$-sets, so let $(\bigcup_{x\in T} x, T, \mathcal{J}_T)$ be a $TD_t(v,s,k,1)$. For each $i$, $1 \le i \le w$, let $S_i = \bigcup_{x\in S_i'} x$, and let $\mathcal{S} = \{S_1,\ldots,S_w\}$. Further, let $E = \bigcup_{x\in E'} x$ and $\mathcal{J} = \bigcup_{T\in\mathcal{J}'} \mathcal{J}_T$.

Let $A = \{a_1,\ldots,a_t\}$ be a PT of $\mathcal{S}$, where $a_i \in \sigma_i \in S_i'$ for each $i$, $1 \le i \le t$. Then $\{\sigma_1,\ldots,\sigma_t\}$ is a PT of $\mathcal{S}'$ of length $t$, and hence is contained in $\lambda'$ members of $\mathcal{J}'$. For each $T \in \mathcal{J}'$ containing $\{\sigma_1,\ldots,\sigma_t\}$, there is precisely 1 member of $\mathcal{J}_T$ containing $A$, and hence altogether there are precisely $\lambda'$ members of $\mathcal{J}$

containing A. Thus $(E,\mathcal{S},\mathcal{I})$ is a $TD_t(w,ss',k,\lambda')$. ∎

(369) From (59) we know that there exists a $D_3(v,4,1)$, i.e., a $TD_3(v,1,4,1)$, for every integer $v \equiv 2,4 \pmod 6$. Further, by (366), there exists a $TD_3(4,3,4,1)$. Hence (368) shows that there exists a $TD_3(v,3,4,1)$ for every $v \equiv 2,4 \pmod 6$.

(370) From (58) we know that there exists a $TD_3(q^2+1,1,q+1,1)$ for every prime power $q$, and, by (366), there exists a $TD_3(q+1,q,q+1,1)$. Hence (368) shows that there exists a $TD_3(q^2+1,q,q+1,1)$ for every prime power $q$.

The equicardinal matroids corresponding to the TD's of (369) and (370) are listed in Table 2.

TABLE 2

THREE INFINITE SERIES OF SIMPLE EQUICARDINAL MATROIDS THAT ARE NOT MATROID DESIGNS

| M | r(M) | \|P(M)\| | k(M) | $c^*(M)$ |
|---|---|---|---|---|
| EM(6n+2,3) | 4 | 18n+6 | 4 | 18n+2 |
| EM(6n+4,3) | 4 | 18n+12 | 4 | 18n+8 |
| EM(q+1,q) | 4 | $q^2+q$ | q+1 | $q^2-1$ |

Here $n$ is a nonnegative integer, and $q$ a prime power.

## 4.9. Conclusion

The results of sections 4.4 - 4.7 give a solution to

the characterization problem for equicardinal matroids in a large number of cases. Theorem (227) characterizes the trivioids in $\mathfrak{M}_n(\gamma)$ for any positive integers $n$ and $\gamma$. Theorems (249), (250), and (315) together characterize the nontrivial members of $\mathfrak{M}_n(\gamma)$, for all $n \geq 0$, whenever $\gamma$ is of the form $p$ or $p^2$ for some prime $p$. Theorems (263), (322), (333), and (342), together with paragraphs (354) and (355) identify the nontrivial members of $\mathfrak{M}_3(pq)$ and $\mathfrak{M}_4(pq)$ whenever $p$ and $q$ are distinct primes such that $p < \frac{2}{3}q+1$.

For certain values of $p$ and $q$, these theorems imply that $\mathfrak{M}_3(pq)$ or $\mathfrak{M}_4(pq)$ contains only trivioids, in which case $\mathfrak{M}_n(pq)$ is known for every $n$.

The characterization in the above cases is not complete only in the sense that the parameters for a t-design or a TD do not, in general, specify the structure of the t-design or TD uniquely. However, since the complete list of non-isomorphic t-designs with a given parameter set has been determined in only a very few cases, we are forced to leave this slight ambiguity in our solution of the characterization problem unresolved.

In Appendix II we have illustrated the scope of our results by listing all connected equicardinal matroids with

co-circuit cardinality $\gamma$, where $1 \leq \gamma \leq 100$ and $\gamma$ is a prime or the product of two primes.

When $\gamma$ has three or more distinct prime factors, say $\gamma = p_1 p_2 \cdots p_t$, $t \geq 3$, the existence of a nontrivial $M \in \mathbb{m}_n(p_i p_j)$ implies the existence of a nontrivial $M' \in \mathbb{m}_n(\gamma)$; namely, we take $M'$ to be a $\frac{\gamma}{p_i p_j}$ - inflation of $M$. However, it is certainly not in general true that every nontrivial member of $\mathbb{m}_n(\gamma)$ is an inflation of some nontrivial member of $\mathbb{m}_n(p_i p_j)$, where $p_i$ and $p_j$ are prime factors of $\gamma$. For example, EG(2,4) is contained in $\mathbb{m}_3(12)$, but it is both simple and nontrivial.

In closing, we point out a particularly interesting unsolved problem that parallels (141) for matroid designs. For a given $\gamma$, is the rank of every nontrivial, connected, equicardinal matroid with co-circuit cardinality $\gamma$ bounded? The results of Appendix II suggest that this is the case, although we have not even been able to establish it for $\gamma = 6$.

# APPENDIX I

## NONTRIVIAL D-CONSISTENT SEQUENCES WITH LEADING TERM N, $1 \leq N \leq 40$, AND ASSOCIATED MATROID DESIGNS

We list below all nontrivial D-consistent sequences of maximal length with leading term N, $1 \leq N \leq 40$. Those values of N, $1 \leq N \leq 40$, 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 matroid designs having d-sequence $D'$ are then listed after D and the symbol (m), where m is the length of $D'$. ($m \geq 3$ since $D'$ is nontrivial.)

A t-$(v,k,\lambda)$ design is denoted here by $D_t(v,k,\lambda)$. t-designs are discussed in sections 3.2 and 3.6. PG(n,s) and EG(n,s) denote, respectively, the finite projective and affine geometries of dimension n and order s. These are discussed in section 3.7. IP(s) denotes an inversive plane of order s. The inversive planes are treated in (58). Finally, $M^{(\ell)}$ denotes the truncation of the matroid M at level $\ell$ (see (43)).

Sources for the construction of all matroid designs 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 (106), 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 Matroid-Designs | References |
|---|---|---|---|---|
| 4 | 4, 2, 1, 1 | (3) | PG(2, 2) | [ 5 ] |
| | | (4) | EG(3, 2) | [ 5 ] |
| 6 | 6, 2, 1, 1, 1, 1 | (3) | EG(2, 3) | [ 5 ] |
| | | (4) | IP(3) | (58) |
| | | (5) | $D_4(11, 5, 1)$ | [19] |
| | | (6) | $D_5(12, 6, 1)$ | [19] |
| 8 | 8, 4, 2, 1, 1 | (4) | PG(3, 2) | [ 5 ] |
| | | (5) | EG(4, 2) | [ 5 ] |
| 9 | 9, 3, 1 | (3) | PG(2, 3) | [ 5 ] |
| 10 | 10, 2, 1,...,1 | (3) | $D_2(13, 3, 1)$ | [ 5 ] |
| | | (4) | $D_3(14, 4, 1)$ | [ 5 ] |
| | 8 terms | (5)-(10) | unknown | |
| 12 | 12, 2, 1,...,1 | (3) | $D_2(15, 3, 1)$ | [ 5 ] |
| | | (4) | $D_3(16, 4, 1)$ | [ 6 ] |
| | 10 terms | (5)-(12) | unknown | |

| N | Maximal D-Consistent Sequences | Initial Subsequence Lengths | Associated Matroid-Designs | References |
|---|---|---|---|---|
| | 12, 3, 1, 1, 1 | (3) | EG(2, 4) | [ 5] |
| | | (4) | IP(4) | (58) |
| | | (5) | unknown | |
| 16 | 16, 2, 1,...,1 | (3) | $D_2(19, 3, 1)$ | [ 5] |
| | | (4) | $D_3(20, 4, 1)$ | [ 6] |
| | 14 terms | (5)-(16) | unknown | |
| | 16, 4, 1, 1, 1, 1 | (3) | PG(2, 4) | [ 5] |
| | | (4) | $D_3(22, 6, 1)$ | [19] |
| | | (5) | $D_4(23, 7, 1)$ | [19] |
| | | (6) | $D_5(24, 8, 1)$ | [19] |
| | 16, 8, 4, 2, 1, 1 | (5) | PG(4, 2) | [ 5] |
| | | (6) | EG(5, 2) | [ 5] |
| 18 | 18, 2, 1,...,1 | (3) | $D_2(21, 3, 1)$ | [ 5] |
| | | (4) | $D_3(22, 4, 1)$ | [ 6] |
| | 16 terms | (5)-(18) | unknown | |
| | 18, 6, 2, 1 | (4) | EG(3, 3) | [ 5] |
| 20 | 20, 4, 1, 1 | (3) | EG(2, 5) | [ 5] |
| | | (4) | IP(5) | (58) |
| 21 | 21, 3, 1,...,1 | (3) | $D_2(25, 4, 1)$ | [ 7] |
| | 7 terms | (4)-(9) | unknown | |
| | 22, 2, 1,...,1 | (3) | $D_2(25, 3, 1)$ | [ 5] |
| | | (4) | $D_3(26, 4, 1)$ | [ 6] |
| | 20 terms | (5)-(22) | unknown | |
| 24 | 24, 2, 1, 1 | (3) | $D_2(27, 3, 1)$ | [ 5] |
| | | (4) | $D_3(28, 4, 1)$ | [ 6] |

| N | Maximal D-Consistent Sequences | Initial Subsequence Lengths | Associated Matroid-Designs | References |
|---|---|---|---|---|
| | 24, 3, 1 | (3) | $D_2(28, 4, 1)$ | [7] |
| | 24, 4, 2, 1, 1 | (4) | $PG(4, 2)^{(4)}$ | [5] |
| | | (5) | $EG(5, 2)^{(5)}$ | [5] |
| 25 | 25, 5, 1 | (3) | $PG(2, 5)$ | [5] |
| 27 | 27, 9, 3, 1 | (4) | $PG(3, 3)$ | [5] |
| 28 | 28, 2, 1,...,1 | (3) | $D_2(31, 3, 1)$ | [5] |
| | | (4) | $D_3(32, 4, 1)$ | [6] |
| | 26 terms | (5)-(28) | unknown | |
| 30 | 30, 2, 1,...,1 | (3) | $D_2(33, 3, 1)$ | [5] |
| | | (4) | $D_3(34, 4, 1)$ | [6] |
| | 28 terms | (5)-(30) | unknown | |
| | 30, 5, 1, 1 | (3) | $EG(2, 6)$ - does not exist | (74) |
| | | (4) | $D_3(37, 7, 1)$ - does not exist | |
| 32 | 32, 16, 8, 4, 2, 1, | (6) | $PG(5, 2)$ | [5] |
| | | (7) | $EG(6, 2)$ | [5] |
| 33 | 33, 3, 1 | (3) | $D_2(37, 4, 1)$ | [7] |
| 34 | 34, 2, 1, 1 | (3) | $D_2(37, 3, 1)$ | [5] |
| | | (4) | $D_3(38, 4, 1)$ | [6] |
| 36 | 36, 2, 1,...,1 | (3) | $D_2(39, 3, 1)$ | [5] |
| | | (4) | $D_3(40, 4, 1)$ | [6] |
| | 34 terms | (5)-(36) | unknown | |

| N | Maximal D-Consistent Sequences | Initial Subsequence Lengths | Associated Matroid-Designs | References |
|---|---|---|---|---|
| | 36, 3, 1,...,1 (15 terms) | (3) | $D_2(40, 4, 1)$ | [5] |
| | | (14)-(17) | unknown | |
| | 36, 4, 1,...,1 (8 terms) | (3) | $D_2(41, 5, 1)$ | [5] |
| | | (4)-(10) | unknown | |
| | 36, 6, 1 | (3) | PG(2, 6) - does not exist | (74) |
| | 36, 4, 2, 1,...,1 (6 terms) | (4)-(9) | does not exist | (119) |
| 40 | 40, 2, 1,...,1 (38 terms) | (3) | $D_2(43, 3, 1)$ | [5] |
| | | (4) | $D_3(44, 4, 1)$ | [6] |
| | | (5)-(40) | unknown | |
| | 40, 4, 1, 1 | (3) | $D_2(45, 5, 1)$ | [7] |
| | | (4) | unknown | |
| | 40, 5, 1 | (3) | unknown | |

## APPENDIX II

### NONTRIVIAL RANK 3 AND 4 EQUICARDINAL MATROIDS HAVING CO-CIRCUIT CARDINALITY $\gamma$ SUCH THAT $1 \leq \gamma \leq 100$ AND $\gamma$ IS NOT DIVISIBLE BY THREE DISTINCT PRIMES

For each integer $\gamma$, $1 \leq \gamma \leq 100$, such that $\gamma$ is not divisible by three distinct primes, we list below all nontrivial rank 3 and rank 4 equicardinal matroids having co-circuit cardinality $\gamma$. In each case, reference is made to the applicable existence theorems in the text. If, for some $\gamma$, the indicated theorem implies that there exist no nontrivial equicardinal matroids with co-circuit cardinality $\gamma$ and given rank, we show a dash (-). If, on the other hand, none of the possible equicardinal matroids with co-circuit cardinality $\gamma$ exist because their parameters are inconsistent, we show an asterisk (*). If the existence of a listed matroid is undetermined, we follow it by a question mark (?).

The following notation is used. PG(n,s) and EG(n,s) denote, respectively, the finite projective and affine

geometries of dimension n and order s, which are discussed in section 3.7. IP(s) denotes the inversive plane of order s. The inversive planes are treated in (58). $D_t(v,k,\lambda)$ denotes a t-$(v,k,\lambda)$ design. The t-designs are discussed in sections 3.2 and 3.6, and references for their construction are given there. EM(v,s) denotes a special type of rank 4 equicardinal matroid defined in (336). The operations of one-point extension and affine extension, denoted respectively by $\oplus$ and $\ominus$, are defined in (199) and section 4.5. Constructions for the special matroids $\Upsilon$, $\Lambda$, and $\Omega$ are given in (204), (354), and (355).

| γ | Rank 3 | Reference | Rank 4 | Reference |
|---|---|---|---|---|
| 1 | - | (249) | - | (249) |
| 2 | - | (249) | - | (249) |
| 3 | - | (249) | - | (249) |
| 4 | PG(2,2) | (250) | EG(3,2) | (315) |
| 5 | - | (249) | - | (249) |
| 6 | EG(2,3);PG(2,2)$\oplus$P(2); EG(2,2)$\ominus\sigma$(2,2,3) | (263) | EG(3,2)$\oplus$P(2);$\Upsilon$; IP(3); $\Lambda$ | (210),(354) |
| 7 | - | (249) | - | (249) |
| 9 | PG(2,3) | (250) | - | (315) |
| 10 | $D_2(13,3,1)$ | (308) | $D_3(14,4,1)$ | (333) |
| 11 | - | (249) | - | (249) |
| 13 | - | (249) | - | (249) |
| 14 | $D_2(15,3,1)\oplus$P(2) | (308) | $D_3(16,4,1)\oplus$P(2); EM(6,3) | (342) |
| 15 | EG(2,4)$\oplus$P(3); EG(2,3)$\ominus\sigma$(3,2,4) | (263) | $D_3(17,5,1)\oplus$P(3); EM(5,4);$\Omega$. | (355) |

| Y | Rank 3 | Reference | Rank 4 | Reference |
|---|---|---|---|---|
| 17 | - | (249) | - | (249) |
| 19 | - | (249) | - | (249) |
| 21 | $D_2(25,4,1)$ | (308) | $D_3(26,5,1)$? | (333) |
| 22 | $D_2(25,3,1)$ | (308) | $D_3(26,4,1)$ | (333) |
| 23 | - | (249) | - | (249) |
| 25 | PG(2,5) | (250) | - | (315) |
| 26 | $D_2(27,3,1)\oplus P(2)$ | (308) | $D_3(28,4,1)\oplus P(2)$; EM(10,3) | (342) |
| 29 | - | (249) | - | (249) |
| 31 | - | (249) | - | (249) |
| 33 | $D_2(37,4,1)$ | (308) | * | (333) |
| 34 | $D_2(37,3,1)$ | (308) | $D_3(38,4,1)$ | (333) |
| 35 | * | (313) | - | (239) |
| 37 | - | (249) | - | (249) |
| 38 | $D_2(39,3,1)\oplus P(2)$ | (308) | $D_3(40,4,1)\oplus P(2)$; EM(14,3) | (342) |
| 39 | $D_2(40,4,1)\oplus P(3)$ | (308) | $D_3(41,5,1)\oplus P(3)$?; EM(11,4)? | (342) |
| 41 | - | (249) | - | (249) |
| 43 | - | (249) | - | (249) |
| 46 | $D_2(49,3,1)$ | (308) | $D_3(50,4,1)$ | (333) |
| 47 | - | (249) | - | (249) |
| 49 | PG(2,7) | (250) | - | (315) |
| 51 | $D_2(52,4,1)\oplus P(3)$ | (308) | * | (342) |
| 53 | - | (249) | - | (249) |
| 55 | $D_2(61,6,1)$ | (308) | * | (333) |
| 57 | $D_2(61,4,1)$ | (308) | $D_3(62,5,1)$? | (333) |
| 58 | $D_2(61,3,1)$ | (308) | $D_3(62,4,1)$ | (333) |
| 59 | - | (249) | - | (249) |
| 61 | - | (249) | - | (249) |
| 62 | $D_2(63,3,1)\oplus P(2)$ | (308) | $D_3(64,4,1)\oplus P(2)$; EM(22,3) | (342) |
| 65 | $D_2(66,6,1)\oplus P(5)$? | (308) | * | (342) |

| Y | Rank 3 | Reference | Rank 4 | Reference |
|---|---|---|---|---|
| 67 | - | (249) | - | (249) |
| 69 | $D_2(73,4,1)$ | (308) | * | (333) |
| 71 | - | (249) | - | (249) |
| 73 | - | (249) | - | (249) |
| 74 | $D_2(75,3,1)\oplus P(2)$ | (308) | $D_3(76,4,1)\oplus P(2)$; | (342) |
| 77 | - | (308) | - | (239) |
| 79 | - | (249) | - | (249) |
| 82 | $D_2(85,3,1)$ | (308) | $D_3(86,4,1)$ | (337) |
| 85 | $D_2(91,6,1)$? | (308) | $D_3(92,7,1)$? | (333) |
| 86 | $D_2(87,3,1)\oplus P(2)$ | (308) | $D_3(88,4,1)\oplus P(2)$; EM(30,3)? | (342) |
| 87 | $D_2(88,4,1)\oplus P(3)$ | (308) | * | (342) |
| 89 | - | (249) | - | (249) |
| 91 | $EG(2,7)\ominus\sigma(7,2,8)$ | (308) | - | (322) |
| 93 | $D_2(97,4,1)$ | (308) | * | (333) |
| 94 | $D_2(97,3,1)$ | (308) | $D_3(98,4,1)$ | (333) |
| 95 | $D_2(96,6,1)\oplus P(5)$? | (308) | * | (342) |
| 97 | - | (249) | - | (249) |

## LIST OF REFERENCES


[1] E. F. Assmus and H. F. Mattson, New 5-designs, J. Combinatorial Theory 6 (1969), 122-151

[2] G. Birkhoff, Lattice Theory, Amer. Math. Soc., Coll. Pubns. 25 (1967).

[3] R. C. Bose, Mathematical theory of the symmetrical factorial designs, Sankhya 8 (1947), 107-166.

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

[5] M. Hall, Jr., Combinatorial Theory, Blaisdell, Waltham, Mass., 1967.

[6] H. Hanani, On quadruple systems, Can. J. Math. 12 (1960), 145-157.

[7] H. Hanani, The existence and construction of balanced incomplete block designs, Ann. Math. Stat. 32 (1961), 361-386.

[8] H. Hanani, On some tactical configurations, Can. J. Math. 15 (1963), 702-722.

[9] F. Harary, Graph Theory, Addison-Wesley, Reading, Mass., 1969.

[10] D. R. Hughes, On t-designs and groups, Amer. J. Math. 87 (1965), 761-778.

[11] W. M. Kantor, Characterization of finite projective and affine spaces, Can. J. Math. 21 (1969).

[12] N. Mendelsohn, unpublished manuscript from the Second Annual Chapel Hill Conference on Combinatorial Mathematics and Its Applications, University of North Carolina, Chapel Hill, N. C., 1970.

[13] U. S. R. Murty, Equicardinal matroids and finite geometries, in Combinatorial Structures and their Applications, Gordon and Breach, New York, 1969.

[14] J. Riordan, Combinatorial Identities, Wiley, New York, 1968.

[15] A. Seidenberg, Lectures in Projective Geometry, Van Nostrand, Princeton, N. J., 1962.

[16] R. Stanton, Types of Statistical Designs, Canadian Mathematical Congress, Saskatoon, Sas., 1963, Ch. V.

[17] W. T. Tutte, Lectures on Matroids, J. Res. Nat. Bur. Standards Sect. B 69 (1965), 1-47.

[18] H. Whitney, On the abstract properties of linear dependence, Amer. J. Math. 57 (1935), 509-533.

[19] E. Witt, Uber Steinersche Systeme, Abh. Hamburg 12 (1938) 265-275.