SOME PROBLEMS IN
COMBINATORIAL THEORY

With Particular Reference to Induced Matroids

by

M. J. PIFF

Thesis submitted for the degree of Doctor of Philosophy at the University of Oxford.

CONTENTS

ABSTRACT

In Chapter 1 it is shown that transversal matroids and strict gammoids are dual matroids, and hence that Hall's and Menger's Theorems are dual theorems. Corollaries are the results on minimal and maximal presentations of transversal matroids. It is suggested by the proofs that the correct context in which to study transversal matroids is by considering the dual pair of matroids. The maximal presentation of an infinite independence structure is shown to be unique. Finally, Dilworth's Theorem is derived from Hall's Theorem by a similar method to the derivation of Menger's Theorem.

Chapter 2 demonstrates that the properties of being binary or regular are of finite character. Various operations on matroids are also shown to preserve representability, the principal one being induction through a directed graph. In Chapter 3 the same result is proved for algebraic representability.

Chapter 4 is concerned with the automorphisms of independence structures. It is shown that all groups are possible, up to isomorphism, for the automorphism groups of a) graphic geometries, b) transversal geometries, c) partition geometries. The proof of b) relies heavily on the results of Chapter 1. The existence of cyclic matroids, and of certain cyclic transversal matroids and hence of certain cyclic strict gammoids, is demonstrated.

Finally, Chapter 5 is concerned with enumerating the equivalence classes of matroids under isomorphism. Bounds are obtained for general

matroids, representable matroids and transversal matroids.

Unless specifically stated otherwise, all theorems may be assumed to be original. It is also specifically stated when a theorem is not original but the proof or derivation is.

ACKNOWLEDGEMENTS

I should like to thank Dr D. J. A. Welsh very much for his help and encouragement over the period in which this research was done. Most of the problems tackled here were suggested by him.

My thanks also go to Dr A. W. Ingleton for supervising me for one term when Dr Welsh was absent.

Finally, I am indebted to the Oxford University Department of Mathematics for providing me with an S.R.C. Studentship, without which this research would not have been possible.

Dept. of Pure Maths. M. J. P.
University of Sheffield.

Formerly
Keble College, Oxford

0. INTRODUCTION

This work is concerned with the theory of abstract independence. The theory of finite independence structures, or matroids, was developed in 1935 by Whitney [42] and further developed by Minty [24] Tutte [36] and others. For the standard terminology, the reader is referred to these papers, or to Harary and Welsh [14] or Crapo and Rota [8].

The cardinality of a set S is denoted by $|S|$. If $J \subseteq I$ and $|J| < \infty$ then we write $J \subset\subset I$. We denote an indexed set by $\{x_i : i \in I\}$, and a family by $(x_i : i \in I)$, where in this case x_i and x_j may be equal when $i \neq j$.

An independence structure on the set S is a collection of independent subsets of S with the following properties:

(M 0) $\emptyset \in \underline{M}$.

(M 1) $A \in \underline{M}$ if and only if $B \in \underline{M}$ for every $B \subset\subset A$.

(M 2) If $A, B \in \underline{M}$, $A, B \subset\subset S$, and $|B| = |A| + 1$ then there exists some $b \in B - A$ such that $A \cup \{b\} \in \underline{M}$.

Property (M 1) states that independence is a property of finite character, and, when S is finite, simply says that if $A \in \underline{M}$ and $B \subseteq A$ then $B \in \underline{M}$.

A subset of S which is not independent is called dependent. Clearly every dependent subset contains a finite minimal dependent subset or circuit of $\underline{M}$. By an easy application of Zorn's Lemma, every independent subset is contained in a maximal independent subset, or base of $\underline{M}$. In the finite case, Whitney [42], and in the infinite case, Rado [32], showed that bases of an independence structure have the same cardinality. In proving this result, Rado used the following strengthening of the axiom of choice for a family of finite sets, henceforth referred to as Rado's Selection Principle.

Lemma 1 Let $\underline{A} = (A_i : i \in I)$ be a family of finite subsets of a set S. For each $J \subset\subset I$, let α_J be a choice function for $\underline{A}_J = (A_i : i \in J)$. Then there exists a choice function α for $\underline{A}$ such that for any $K \subset\subset I$ there exists a J with $K \subseteq J \subset\subset I$ with $\alpha|_K = \alpha_J|_K$, where $|_K$ denotes the restriction of the function to K.

We call an independence structure on a finite set a matroid. Whitney showed that we can define a dual matroid for any matroid on a finite set. We denote the dual of $\underline{M}$ by $\underline{M}^*$. The bases of $\underline{M}^*$ are the complements of the bases of $\underline{M}$. The circuits of $\underline{M}^*$ are called cocircuits of $\underline{M}$, and its bases are called cobases.

A loop of an independence structure $\underline{M}$ on S is an element $s \in S$ such that $\{s\}$ is dependent. A coloop is an $s \in S$ such that s is in every base of $\underline{M}$. If S is finite then s is a coloop of $\underline{M}$ if and only if s is a loop of $\underline{M}^*$. Elements $s_1, s_2 \in S$ are said to be parallel if s_1 and s_2 are not loops, but $\{s_1, s_2\}$ is dependent. An independence structure without loops or parallel elements is called a geometry.

If $\underline{M}$ is an independence structure on S, and $X \subseteq S$, the *rank* $r(X)$ is the cardinal of any maximal $Y \in M$ such that $Y \subseteq X$. The *rank* of $\underline{M}$, $r(\underline{M})$ is just $r(S)$. The *closure* $\bar{X}$ of $X \subseteq S$ is the set

$$\bar{X} = \{y \in S : y \in X \text{ or } y \in C \subseteq X \cup \{y\} \text{ for some circuit } C \text{ of } \underline{M}\}.$$

If $X = \bar{X}$ then we say that X is *closed*, or that X is a *flat* of $\underline{M}$.

Let $\underline{M}$ be an independence structure on S and let $C(\underline{M})$ denote the set of circuits of $\underline{M}$. Let $A, B \subseteq S$ be disjoint, and define

$$C' = \{X \subseteq S : X = C - A \text{ for some } C \in C(\underline{M}),\ C \subseteq S - B,\ S \neq \emptyset\}$$

and let C'' be the set of minimal members of C'. Then C'' is the set of circuits of an independence structure $\underline{M}.(S - A)|(S - A - B)$ which is the *minor* of $\underline{M}$ obtained by *contracting* A and *deleting* B.

Lemma 2 $\underline{M}.(S - A)|(S - A - B) = \underline{M}.(S - U)|(S - A - B)$ for any maximal $U \in \underline{M}$ with $U \subseteq A$.

Proof The finite case is well known, and the infinite case presents no additional problems.

A minor of form $\underline{M}.S|(S - B)$ is called a *restriction* of $\underline{M}$, and is a *finite restriction* if $S - B$ is finite. We denote it by $\underline{M}|(S - B)$.

Lemma 3 If $\underline{M}$ contains some matroid $\underline{M}'$ as a minor, then some finite restriction of $\underline{M}$ also contains $\underline{M}'$ as a (contraction) minor.

Proof Let $\underline{M}' = \underline{M}.(S - A)|(S - A - B)$, with $A \in \underline{M}$, and let $C_1', \ldots, C_q'$

be the circuits of $\underline{M}'$. Then there exist $C_1, \ldots, C_q \in C(\underline{M})$ such that $C_i = C'_i \cup A_i$ $(i = 1, \ldots, q)$, and $A_i \subset\subset A$. Put $A' = \bigcup_{i=1}^{q} A_i$, and $\underline{M}|(S - A - B) \cup A'$ contains $\underline{M}'$ as a contraction minor.

A set $X \subseteq S$ is called *co-dependent* if it has non-empty intersection with every base of $\underline{M}$. A minimal co-dependent set is called a *cocircuit*. A *hyperplane* of $\underline{M}$ is a maximal subset of S which does not contain any base of $\underline{M}$. Clearly a hyperplane is a flat of $\underline{M}$, and for any base B of $\underline{M}$ and $b \in B$, $\overline{B - \{b\}}$ is a hyperplane, and every hyperplane is of this form.

Lemma 4 Every do-dependent set of $\underline{M}$ contains a cocircuit of $\underline{M}$.

The cocircuits of $\underline{M}$ are the complements of hyperplanes of $\underline{M}$.

Proof Suppose X is co-dependent. Let U be a maximal independent subset of $S - X$, and B a base of $\underline{M}$ with $U \subset B$ (U cannot be a base of $\underline{M}$). For any $b \in B \cap X$, the complement of $\overline{B - \{b\}}$ is a cocircuit of $\underline{M}$ contained in X.

If every two elements of S are contained in a circuit of $\underline{M}$, we say that $\underline{M}$ is *non-separable*, otherwise $\underline{M}$ is *separable*.

If for any two bases B_1 and B_2 of $\underline{M}$ there exists a bijection $\alpha : B_1 \to B_2$ such that, for any $x \in B_1$, $(B_1 - \{x\}) \cup \{\alpha(x)\}$ and $(B_2 - \{\alpha(x)\}) \cup \{x\}$ are bases of $\underline{M}$, then we say that $\underline{M}$ is *base-orderable*.

Special structures.

We list here, for reference, a few special structures which will be met later.

A collection S of vectors over a division ring forms an independence structure, with independence defined as linear independence.

The set of partial transversals $\underline{M} = \underline{M}(\underline{A})$ of a family $\underline{A} = (A_i : i \in I)$ of subsets of a set S forms an independence structure on S if the family $\underline{A}$ is *restricted*, that is, no element of S is in infinitely many sets of $\underline{A}$. $\underline{M}$ is called a transversal structure, and any family $\underline{B}$ such that $\underline{M} = \underline{M}(\underline{B})$ is called a *presentation* of $\underline{M}$. If $\underline{M}$ is *coloop-free* then $\underline{M}$ has only restricted presentations.

If k is a non-negative integer, the set of all subsets of S of cardinal at most k forms an independence structure on S called the k-*uniform* structure on S.

Let S be a set, k a positive integer, and $\underline{H}$ a set of subsets of S such that each subset in $\underline{H}$ has cardinal at least k and every k-subset of S is a subset of just one set of $\underline{H}$, whilst some $(k + 1)$-subset of S is a subset of none of the sets of $\underline{H}$. Then the collection M of $(k + 1)$-subsets of S which are subsets of no set of $\underline{H}$ forms an independence structure on S called a k-*partition* structure. If $k > 1$ the structure is a geometry. $\underline{H}$ is its set of hyperplanes.

Let G be an undirected graph with edge set E. The collection $\underline{M}(G)$ of subsets of E which contain no finite cycle of G forms an independence structure on E. We call $\underline{M}(G)$ the *cycle independence structure* of G, and say that $\mathbf{M}(G)$ is *graphic*.

It is shown in [28] that the properties of being transversal or of being graphic are of finite character, that is, they hold for $\mathbf{M}$ if and only if they hold for every finite restriction of $\mathbf{M}$. A proof of the former result is incorporated in Theorem 1.23 below.

1. TRANSVERSAL MATROIDS AND GAMMOIDS.

It is well known [25] that we may take the partial transversals of a restricted family $A = (A_i : i \in I)$ of subsets of a set S as the independent sets of an independence structure on S. Also, given any finite directed graph G with vertex set V and edge set E, and a distinguished set $B \subseteq V$, we may take the subsets of V which may be linked into B as the independent sets of a matroid on V [26, 31]. The former structure we call a transversal structure, the latter a strict gammoid.

The main result of this chapter is that the dual of a transversal matroid is a strict gammoid and vice versa. As applications of this result, we redevelop work done by Mason [23] and Bondy and Welsh [4] in this new light, and demonstrate the duality between Hall's Theorem on transversals and Menger's Linkage Theorem.

Unless stated to the contrary, all sets in this chapter are finite.

Preliminaries

Let G be a directed graph with vertex set V and edge set E. A path in G is a sequence $P = (v_0, v_1, \ldots, v_k)$ of distinct vertices of G such that $k \geqslant 0$ and $(v_{i-1}, v_i) \in E$ $(i = 1, \ldots, k)$. P has initial vertex v_0 and terminal vertex v_k. Two paths are said to be disjoint if their vertex sets are disjoint. We say that there exists a linking of $A \subseteq V$ onto $B \subseteq V$ if, for some bijection $\alpha : A \to B$ we can find disjoint paths $(P_a : a \in A)$ in G such that P_a has initial vertex a and terminal vertex $\alpha(a)$.

Given a graph G and a subset $B \subseteq V$, we put $\underline{M}\,(G, B)$ equal to the collection of subsets of V which may be linked onto a subset of B, and call this collection a <u>strict gammoid</u> on V. For any $X \subseteq V$, $\underline{M}\,(G, B)|X$ is called a <u>gammoid</u>.

Suppose that G is bipartite, with $E \subseteq V' \times V''$. We see that if we put

$$A_v = \{v\} \cup \{w : (w, v) \in E\} \qquad\qquad (v \in V'')$$

then $\underline{M}\,(G, V'')$ is the collection of partial transversals of $\underline{A} = (A_v : v \in V'')$. This special type of transversal matroid is called <u>fundamental</u> by Bondy and Welsh [4] because each A_v is the fundamental cocircuit of v with respect to the cobase V'. A general transversal matroid may be obtained as $\underline{M}\,(G, V'')|V'$.

We require a few lemmas about transversal matroids. Let G^* be the graph obtained from G by reversing the orientation of its edges.

<u>Lemma 1</u> Let G be a bipartite graph with $E \subseteq V' \times V''$. Then $\underline{M}\,(G^*, V')$ is the dual matroid of $\underline{M}\,(G, V'')$.

<u>Proof</u> Obvious from the definitions.

<u>Lemma 2</u> A cotransversal matroid (that is, such that its dual is transversal) is a contraction of a fundamental transversal matroid.

<u>Proof</u> From the definition and Lemma 1.

Lemma 3 Let $\underline{M}$ be the collection of partial transversals of the family $\underline{A} = (A_1, \dots, A_n)$, written $\underline{M} = \underline{M}(\underline{A})$. Suppose that $A_i \neq \emptyset$ $(i = 1, \dots, n)$. Then if $\underline{M}$ has no coloops, $n = r(\underline{M})$.

Proof Brualdi [6].

Corollary 4 If $\underline{M} = \underline{M}(A_1, \dots, A_n)$ and $r(\underline{M}) < n$ then $\underline{M} = \underline{M}(A_{i_1}, \dots, A_{i_r})$ for some $\{i_r, \dots, i_r\} \subseteq \{1, \dots, n\}$.

Proof Application of Lemma 3 to $\underline{M}|T$, where T is the coloop-free part of S, gives the result.

The fundamental duality theorem.

Let G be a directed graph, with vertex set V and edge set E. For each $v \in V$ define

$$A_v = \{v\} \cup \{w \in V : (v, w) \in E\}.$$

Put $\underline{A} = (A_v : A_v : v \in V)$, and for any $X \subseteq V$ put $\underline{A}_X = (A_v : v \in X)$.

Lemma 5 Let A, B be subsets of V. Then A can be linked onto B in G if and only if $V - A$ is a transversal of $\underline{A}_{V-B}$.

Proof First suppose that A is linked onto B in G by disjoint paths $(P_v : v \in A)$. We define a function $\alpha : (V - A) \to (V - B)$ by

$$\alpha(u) = \begin{cases} v & \text{if } (v, u) \in P_x \text{ for some } x \in A. \\ u & \text{otherwise.} \end{cases}$$

α is well-defined, since the paths are disjoint, and is an injection. $\alpha(u) \notin B$ because this would imply either that some path had at least two vertices in B, or that some vertex of B was on no path. Finally,

α is onto $V - B$ since if $v \in V - B$ then either v is on some path, and then cannot be the terminal vertex of this path, or v is on no path and $\alpha(v) = v$. Clearly $u \in A_{\alpha(u)}$ $(u \in V - A)$, and $V - A$ is a transversal of $\underline{A}_{V-B}$.

Conversely, suppose we have a bijection $\alpha:(V - A) \to V - B$ such that $u \in A_{\alpha(u)}$ for all $u \in V - A$. Take $v \in B - A$. Then $(\alpha(v), v) \in E$. Either $\alpha(v) \in A$ or $(\alpha^2(v), \alpha(v)) \in E$. Either $\alpha^k(v) \in A$ for some A or we obtain an infinite sequence $(\alpha^r(v))$. But since G is finite we must then have $\alpha^r(v) = \alpha^s(v)$ for some $r < s$. Choosing r minimal, we then have $\alpha(\alpha^{r-1}(v)) = \alpha(\alpha^{s-1}(v))$. But then, since α is bijective, we have $\alpha^{r-1}(v) = \alpha^{s-1}(v)$, a contradiction of the minimality of r. Thus we obtain a path $\{\alpha^k(v), \ldots, \alpha(v), v\}$ from A to B. Similarly we obtain paths for every $v \in B - A$. These paths are disjoint since α is bijective. Adjoining the trivial paths (v) for $v \in A \cap B$, we obtain a linking of A onto B.

<u>Theorem 6</u> $\underline{M}(G, B) = \underline{M}^*(\underline{A}_{V-B})$. Thus $\underline{M}(G, B)$ is a matroid on V.

The dual of any transversal matroid is a strict gammoid and vice versa.

<u>Proof</u> The first part of our statement is just Lemma 5. We only need to show that the dual of a transversal matroid is a strict gammoid. We can assume we are given $\underline{M}(A_1, \ldots, A_r)$ where $(A_1, \ldots, A_r)$ possesses a transversal, by Corollary 4. Let B be the complement

of such a transversal, and reindex $(A_1, \ldots, A_r)$ as $\underline{A} = (A_v : v \in V-B)$ is such a way that $v \in A_v$ for all $v \in V - B$. Form a directed graph G on V with edge set

$$E = \{(v, w) : w \in A_v\}.$$

Then clearly $\underline{M}^*(\underline{A}) = M(G, B)$.

Theorem 6 is our fundamental duality theorem.

In the proof of Theorem 6 we are allowed to take any transversal of $\underline{A}$ in constructing the directed graph. Thus

Corollary 7 Let B' be a base of $\underline{M}(G, B)$. Then $\underline{M}(G, B) = \underline{M}(G', B')$ for some directed graph G' on V. The associated families $\underline{A}_{V-B}$ and $\underline{A}'_{V-B'}$ can be chosen to be identical apart from re-indexing.

The first half of Corollary 7 is Mason's principal result ([23], Theorem 4.1.1.). We shall use the second half later, when we look at minimal and maximal presentations.

Corollary 8 A strict gammoid is the contraction of a fundamental transversal matroid.

Proof By Lemma 2 and Theorem 6.

Corollary 9 The class of gammoids is closed under the operations of restriction and contraction, and consists of the class of minors (in fact, contractions) of transversal matroids.

Proof By Corollary 8, any minor $\underline{M}$ of a strict gammoid is a contraction of a transversal matroid, or a minor of a fundamental transversal matroid, which is itself a strict gammoid. But then by Theorem 6 $\underline{M}^*$ is a minor of a transversal matroid, or a contraction of a transversal matroid. Again by Theorem 6, $\underline{M}$ is a deletion of a strict gammoid, that is, $\underline{M}$ is a gammoid.

Corollary 10 The dual of a gammoid is a gammoid.

Proof For the dual of a gammoid is the contraction of a transversal matroid by Theorem 6, and by Corollary 9 this is a gammoid, since a transversal matroid is a gammoid.

Corollary 10 was originally proved by Mason ([23] Th. 4. 2. 1.).

We say that an independence structure $\underline{M}$ has the full exchange property [6] if, given any two bases B_1 and B_2 of $\underline{M}$ there exists a bijection $\alpha : B_1 \to B_2$ such that for any $X \subseteq B_1$ both $(B_1 - X) \cup \alpha(X)$ and $(B_2 - \alpha(X)) \cup X$ are bases of $\underline{M}$. It is well known that transversal matroids have the full exchange property, and that the property is inherited under the operations of deletion, contraction and taking duals. Thus

Corollary 11 Gammoids have the full exchange property.

Proof By Theorem 6.

This result was originally proved by Brualdi, and was proved independently by Mason [21].

Corollary 12 A gammoid is representable over every sufficiently large field.

Proof By Theorem 6 and the result of Chapter 2 on transversal matroids.

Corollary 12 was originally proved by Mason [23].

Extensions and Corollaries.

We now turn our attention to the relationship between Menger's and Hall's Theorems, and look at some more general linkage theorems.

Let G be a directed graph, and suppose that A, B and C are subsets of V. C is said to block A from B if every path from A to B in G intersects C.

Theorem 12 (Menger) Given subsets $A, B \subseteq V$, A can be linked into B in G if and only if there is no set $C \subset V$ blocking A from B with $|C| < |A|$.

Proof By Hall's Theorem, A can be linked into B if and only if $V - A$ contains a transversal of $\underline{A}_{V-B}$, that is, for all $X \subseteq V - B$,

$$\left| \bigcup_{v \in X} A_v - A \right| \geq |X|.$$

We show the equivalence of these conditions to Menger's conditions.

First, suppose that for some $C \subset V$ with $|C| < |A|$, C blocks A from B. Put

$$Y = \{v \in V: C \text{ blocks } v \text{ from } B\}$$

Then $A \cup C \subseteq Y$. Put $X = Y - C \subseteq V - B$. Then $\bigcup_{v \in X} A_v \subseteq Y$ so

$$\left| \bigcup_{v \in X} A_v - A \right| \leq |Y - A|$$

$$= |C| + |X| - |A| < |X| .$$

Conversely, suppose that for some $X \subseteq V - B$

$$\left| \bigcup_{v \in X} A_v - A \right| < |X| .$$

Since $\underline{A}_{V-B}$ possesses a transversal, we must have, putting $Y = \bigcup_{v \in X} A_v$, that $Z = Y \cap A \neq \emptyset$, and our condition is that

$$|Y| - |Z| < |X|$$

Put $D = Y - X$, so that $|D| < |Z|$. Then D blocks Y from B, hence blocks Z from B. $C = D \cup (A - Z)$ clearly blocks A from B and $|C| < |A|$, which completes the proof.

Suppose now that we have a matroid $\underline{M}$ on V. Put $\underline{M}(G, \underline{M})$ equal to the collection of subsets of V which can be linked in G onto an independent subset of V in $\underline{M}$. If $\underline{A} = (A_i : i \in I)$ is a family of subsets of V and $\underline{M}$ is a matroid on I then we denote by $\underline{M}(\underline{A}, \underline{M})$ the collection of partial transversals of subfamilies $\underline{A}_X$ such that $X \in \underline{M}$.

<u>Theorem 13</u> $\underline{M}(G, \underline{M}) = \underline{M}^*(\underline{A}, \underline{M}^*)$ where $\underline{A}$ is the family associated with G. Thus $\underline{M}(G, \underline{M})$ is a matroid on V.

<u>Proof</u> By Lemma 5 and the result on induced matroids through a bipartite graph .

Corollary 14. The matroid $\underline{M}(G, \underline{M})$ may be obtained by the following sequence of operations on $\underline{M}$ (Cf. Corollary 8):

a) Addition of a disjoint set of coloops to $\underline{M}$;

b) Induction through a bipartite graph;

c) A sequence of contractions.

Proof Put $\underline{N} = M(G, \underline{M})$. Then $\underline{N}^* = \underline{M}(\underline{\Delta}, \underline{M}^*)$. Let V' be a disjoint copy of V, with $V' = \{v' : v \in V\}$, and define a matroid $\underline{L}$ on $V \cup V'$ by

$$\underline{L} = \{X' \subseteq V' : X \in \underline{M}^*\} .$$

Thus $\underline{L}^*$ is a coloop extension of $\underline{M}$ up to isomorphism. Let G_1 be the bipartite graph on $V \cup V'$ with edges (v', w) where $v' \in V'$, $w \in V$ and $w \in \Delta_v$. Then clearly $\underline{N}^* = \underline{M}(G_1, \underline{L})|V$. But then $\underline{N} = \underline{M}^*(G_1, \underline{L}) \cdot V$, and by Theorem 13 $\underline{M}^*(G_1, \underline{L})$ is obtained from $\underline{L}^*$ by induction through a bipartite graph.

Corollary 15 If $\underline{M}$ has the full exchange property, then so does $\underline{M}(G, \underline{M})$.

Proof For the property is inherited under coloop extension, induction through a bipartite graph and contraction [6] .

Corollary 14 will be used in Chapter 3.

Finally, we suppose we are given two matroids $\underline{M}_1$ and $\underline{M}_2$ on V with $r(\underline{M}_1) = r(\underline{M}_2) = r$. A linking of $\underline{M}_1$ onto $\underline{M}_2$ in G is said to exist if we can link some base of $\underline{M}_1$ onto some base of $\underline{M}_2$ in G.

Let $\underline{A} = (A_i : i \in I)$ be a family of subsets of V, and let $\underline{M}_1$, $\underline{M}_2$ be matroids on I, V respectively. For $X \subseteq V$ define

$$I(X) = \{i \in I : v \in A_i \text{ for some } v \in X\}$$

Then if $r(\underline{M}_1) = r(\underline{M}_2) = r$ we know that the condition that there exist bases B_1 and B_2 of $\underline{M}_1$ and $\underline{M}_2$ such that B_2 is a transversal of $\underline{A}_{B_1}$ is [5, 39] that for every $X \subseteq V$ we should have

$$r_1(I(X)) + r_2(V - X) \geqslant r$$

For a general graph G with $X \subseteq V$ we define

$$\tilde{X} = \bigcup_{v \in X} A_x = X \cup \{v \in V : (x, v) \in E, \text{ some } x \in X\}.$$

<u>Theorem 13</u> The matroids $\underline{M}_1$ and $\underline{M}_2$ on V with $r(\underline{M}_1) = r(\underline{M}_2) = r$ possess a linking in G if and only if, for all $X \subseteq V$ we have

$$r_1^*(\tilde{X}) + r_2(X) \geqslant |X|.$$

<u>Proof</u> $\underline{M}_1$ and $\underline{M}_2$ possess a linking in G if and only if there exist bases B_1^* and $\underline{B}_2^*$ of $\underline{M}_1^*$ and $\underline{M}_2^*$ such that B_2^* is a transversal of $\underline{A}_{B_1^*}$, i.e. if and only if, for all $X \subseteq V$

$$r_1^*(\bigcup_{x \in X} A_x) + r_2^*(V - X) \geqslant |V| - r$$

$$\text{or} \qquad r_1^*(\tilde{X}) + r_2(X) \geqslant |X|$$

since $r_2^*(V - X) - |V - X| + r = r_2(X)$.

Note We give a direct proof of the necessity of this condition. Suppose that for some $X \subseteq V$ we have

$$r_1^*(\tilde{X}) + r_2(X) < |X|.$$

Then

$$r_1(V - \tilde{X}) + |\tilde{X}| - r + r_2(X) < |X|$$

and for any base B_1 of $\underline{M}_1$ we have

$$|B_1 \cap (V - \tilde{X})| + |\tilde{X}| - r + r_2(X) < |X|$$

$$\text{or} \quad |B_1 \cap \tilde{X}| > r_2(X) + |\tilde{X} - X|.$$

For any base B_2 of $\underline{M}_2$ we take the set

$$D = (B_2 \cap X) \cup (\tilde{X} - X)$$

which separates $B_1 \cap \tilde{X}$ from B_2, whilst $|D| < |B_1 \cap \tilde{X}|$. Putting $C = D \cup (B_1 - \tilde{X})$ we see that C separates B_1 from B_2, and $|C| < r$.

Minimal and maximal presentations.

Let $\underline{M}(G, B)$ be a strict gammoid, and suppose $v \in V - B$. Then A_v contains a circuit of $\underline{M}(G, B)$. For if X is a base of $A_v - \{v\}$ in $\underline{M}(G, B)$, then $\{v\} \cup X$ is a circuit of $\underline{M}(G, B)$, since clearly v is dependent upon $A_v - \{v\}$, whilst any proper subset of $\{v\} \cup X$ is independent. The following theorem tells us that we can find a 'minimal' graph inducing the same independence structure.

Theorem 14 Let $\underline{M}$ be a strict gammoid on V. Then we can write $\underline{M} = \underline{M}(G_c, B)$ for some directed graph G_c on V and base B of $\underline{M}$, where the associated family $\underline{A}_c = (A_{c,v} : v \in V)$ is such that $A_{c,v}$ is a circuit whenever $v \in V - B$, and $A_{c,v} = \{v\}$ for $v \in B$.

Proof Suppose $\underline{M} = \underline{M}(G, B)$ for some graph G and base B of $\underline{M}$, and suppose G is not of the desired form. We can certainly assume that $A_v = \{v\}$ for $v \in B$. Suppose A_u is not a circuit of $\underline{M}$ for some $u \in V - B$. Let B' be a base of $\underline{M}$ having maximal intersection with A_u. Then $\underline{M} = \underline{M}(G', B')$ for some directed graph G' on V, such that the families $\underline{A}_{V-B}$ and $\underline{A}'_{V-B'}$ are identical apart from indexing (Corollary 7). Suppose $A_u = A'_w$ for some $w \in V - B'$. Then clearly any path from w to B' passes through $(A'_w - \{w\}) \cap B'$, and consequently all edges leaving w other than those to B' can be dropped. We thus produce a new graph with one more associated set which is a circuit. The process is repeated for all other sets in the associated family which are not already singletons or circuits.

Corollary 15 Every transversal matroid $\underline{M}$ has a presentation $\underline{M} = \underline{M}(\underline{A})$ such that every set of $\underline{A}$ is a cocircuit of $\underline{M}$.

Proof The dual of Theorem 14.

Corollary 15 was originally proved by Bondy and Welsh [4], and states that the minimal presentations of a transversal matroid are cocircuit presentations.

We now look at the maximal presentations of a strict gammoid.

Theorem 16 Let $\underline{M} = \underline{M}(G, B)$. Then $\underline{M} = \underline{M}(\bar{G}. B)$, where $\bar{G}$ is obtained from G be adding all edges (u, v) such that v is in the closure of A_u in $\underline{M}$ when $u \in V - B$, and all edges (u, v) when $u \in B$.

Proof As in Theorem 14, we transform to a base B' with $|B' \cap A_u|$ maximal, so $\underline{M} = M(G', B')$, and $A_u = A'_w$, say. It is trivial that we may add all edges (w, x) such that x is in the closure of A'_w. But we can then return to our original base B, and A_u has become closed.

It is clear that we can add no more edges to $\bar{G}$ without altering the induced matroid, and such a graph we refer to as maximal. For any maximal graph G, A_u is closed for all $u \in V$.

Theorem 17 Let $\underline{M} = \underline{M}(G, B) = \underline{M}(G', B')$, where G, G' are maximal. Then the associated families $\underline{A}$ and $\underline{A}'$ are identical up to re-indexing.

Proof Clearly we only need to show that $\underline{A}_{V-B}$ and $\underline{A}'_{V-B'}$ are identical up to re-indexing, since, for $v \in B$ or $v \in B'$ we have $A_v = V$ or $A_v{}' = V$. We shall construct the family $\underline{A}_{V-B}$ intrinsically, and this will prove its uniqueness.

We know that if G is maximal then the sets $A_v (v \in V - B)$ are closed. Thus we search amongst the closed sets, or flats, of $\underline{M}$. For

$X \subseteq V$ we write $F(X)$ for the collection of flats of $\underline{M}$ properly contained in X. We define the function $\beta(X)$ on the collection of flats of $\underline{M}$ inductively by

$$\beta(X) = |X| - r(X) - \sum_{Z \in F(X)} \beta(Z).$$

We show by induction on $r(X)$ that $\beta(X)$ is zero unless X is the closure of a circuit of $\underline{M}$, when $\beta(X)$ counts the number of times X appears in the family $\underline{A}_{V-B}$. For let X be a flat and suppose that the result is true for flats of rank less than $r(X)$. We may assume that $|X \cap B| = r(X)$ by Corollary 7. Then for $v \in V - B$ we have $A_v \subseteq X$ if and only if $v \in X$, and so, by induction,

$$\begin{aligned} \beta(X) &= |X| - r(X) - \sum_{Z \in F(X)} \beta(Z) \\ &= |X| - r(X) - |\{A_v \in F(X) : v \in X - B\}| \\ &= |\{v \in X - B : A_v = X\}|, \end{aligned}$$

since

$$\begin{aligned} |X| - r(X) &= |X - B| \\ &= |\{v \in X - B : A_v \subseteq X\}|. \end{aligned}$$

For $r(X) = 0$ we have $\beta(X) = |X|$, and clearly X is the collection of loops of $\underline{M}$, which appears exactly $|X|$ times in $\underline{A}_{V-B}$.

Finally, if $\beta(X) \neq 0$ then there exists some $v \in X - B$ such that $A_v = X$. But then $\{v\} \cup (X \cap B)$ is a circuit of $\underline{M}$ whose closure is X. Thus $\beta(X) = 0$ unless X is a circuit closure.

Corollary 18 Let $\underline{M}$ be a coloop-free transversal matroid. Then $\underline{M}$ has a unique maximal presentation up to re-indexing.

Proof For if $\underline{M}$ is coloop-free then every presentation of $\underline{M}$ corresponds to at least one graph inducing $\underline{M}^*$, and the result follows from Theorem 17.

Corollary 18 was originally proved by Mason [21, 22].

The β-function above is simply Mason's α-function restricted to the flats of the strict gammoid. An alternative development of the α-function criterion may be found in [17]. We note here that if $\underline{M}$ happens to be a strict gammoid, then the calculation of β gives a method of constructing an inducing graph for $\underline{M}$. We in fact only need consider circuit closures in calculating β.

Finally, a fairly easy corollary of the theory is a result of Bondy [3].

Theorem 19 Let $\underline{M}$ be a transversal matroid on V, and suppose that $x, y \in V$ are in series in $\underline{M}$, that is, that x and y are parallel in $\underline{M}^*$. Then $\underline{M}:(V - \{y\})$ is transversal.

Proof Write $\underline{M}^* = \underline{M}(G, B)$ where $x \in B$ and G is maximal. Then $\underline{M}^*|(V - y) = \underline{M}(G - y, B)$, since $(v, x) \in E$ whenever $(v, y) \in E$, and all paths from y to B in G necessarily terminate in x. Thus $\underline{M}^* | (V - y)$ is a strict gammoid, and the result follows from Theorem 6.

Gammoids and strict gammoids.

A gammoid $\underline{M}$ on a set S is the restriction of some strict gammoid to S. It is a valid question to ask, how many elements must we add to S before we can find a strict gammoid on the extended set which restricts to $\underline{M}$?

Theorem 20 Let $\underline{M}$ be a gammoid on a set S with $|S| = m$. Then there exists a set T with $|T| \leqslant m + 2^m$ and $S \subseteq T$, and a directed graph G on T and subset B of S such that $\underline{M} = \underline{M}(G, B) | S$.

Proof Let $\underline{M}(G', B)$ be a strict gammoid on a set V with $S \subseteq V$ such that $\underline{M} = \underline{M}(G', B) | S$. We may assume that B is a base of $\underline{M}$, that is, that $B \subseteq S$.

For each circuit C of $\underline{M}$ choose a blocking set $X_C \subset V$ for C with $|X_C| = |C| - 1$. Put

$$T = S \cup \left(\bigcup_C X_C \right)$$

For each base B' of $\underline{M}$ there exists a linking in G' of B' onto B, say $(P_b : b \in B')$. For each path $P_b = \{b, \ldots, x_1, \ldots, x_2, \ldots, x_t, \ldots, b'\}$ where $b, x_1, \ldots, x_t, b'$ are the only elements of P_b in T we put the edges $(b, x_1), \ldots, (x_t, b')$ in G. Thus B' is a base of $\underline{M}(G, B)$.

If C is a circuit of $\underline{M}$ then X_C is a blocking set for C in G. Thus G is the required graph, since $|T| \leqslant n + 2^m$.

Infinite generalizations.

If we take a graph G on an infinite set V and form $\underline{M}(G, B)$ as before, it would appear difficult to find necessary and sufficient conditions on G for $\underline{M}(G, B)$ to be an independence structure. Perfect [26] gives only sufficient conditions. However, we can use the gammoid methods as a tool to prove the results on presentations of transversal structures. Let $\underline{M} = \underline{M}(\underline{A})$ be a coloop-free transversal structure on a set V. Then, by the infinite generalization of Lemma 3, $\underline{A}$ is restricted, that is, every element of V is in only finitely many sets of $\underline{A}$. Let $V - B$ be a base of $\underline{M}$, so that $V - B$ is a transversal of $\underline{A}$. Then we may reindex $\underline{A}$ so that $\underline{A} = (A_v\colon v \in V - B)$ where $v \in A_v$ for all $v \in V - B$. We construct a directed graph G on V as in the finite case. G has the property that it possesses no infinite path terminating in B, for if $P = \{\ldots, v_n, \ldots, v_1, v_0\}$ were such a path with $v_0 \in B$ we could define the bijection

$$f\colon \{v_0\} \cup (V - B) \to V - B \text{ by}$$

$$f(v) = \begin{cases} v_{n+1} & \text{if } v = v_n \in P \\ v & \text{if } v \notin P \end{cases}$$

and $v \in A_{f(v)}$ for all $v \in \{v_0\} \cup (V - B)$, a contradiction, since

$(V - B)$ is a base of $\underline{M}$.

Lemma 21 With $\underline{M} = M(\underline{A})$, G and B as above, $V - B_1$ is a maximal transversal of $\underline{A}$ if and only if B_1 is a minimal set with the property that it can be linked onto B in G.

Proof If B_1 can be linked onto B then, as in Lemma 5, $V - B_1$ is a transversal of $\underline{A}$. Conversely, if $V - B_1$ is a maximal transversal of $\underline{A}$, then this defines a linking of some subset X of B_1 onto B, the proof of Lemma 5 working because there are no infinite paths terminating in B. But then by the first part $V - X$ is a transversal of $\underline{A}$, which forces $X = B_1$ because $V - B_1$ was assumed to be a maximal transversal and $V - B_1 \subseteq V - X$.

Lemma 21 gives us an analogue of Corollary 7 on switching from one base to another. This allows us to prove

Theorem 22 If $\underline{M} = \underline{M}(\underline{A})$ is a coloop-free transversal structure, then $\underline{A}$ may be reduced to a cocircuit presentation.

Proof Similar to Corollary 15. Suppose $\underline{A} = (A_i : i \in I)$ and we choose a fixed set A_u, $u \in I$. We choose a transversal $V - B'$ of $\underline{A}$ such that $(V - B') \cap (V - A_u)$ is maximal, that is, so that $B' \cap A_u$ is maximal, and form a graph G' from $\underline{A}$. Deleting edges as in Corollary 15, we reduce $A_u = A_w'$ to a cocircuit. We form a collection

H consisting of all presentations of $\underline{M}$ which are obtained from $\underline{A}$ by replacing some or all of its sets A_v by cocircuits contained in A_v, and order H by putting $\underline{A}' \leqslant \underline{A}''$ if $A'_v \subseteq A''_v$ for all $i \in I$. By a trivial application of Zorn's Lemma, H possesses a minimal member, and by the first part, this has to be a cocircuit presentation.

Theorem 23 A coloop-free transversal independence structure $\underline{M}$ on V possesses a unique maximal presentation up to re-indexing.

Proof Let B be a base of $\underline{M}$. For each $v \in V$ put

$$B_v = \begin{cases} \{v\} & v \in B \\ C_v - \{v\} & v \notin B \end{cases}$$

where C_v is the fundamental circuit of v with respect to B. Let I be the collection of all subsets $U \subset\subset V$ which are of the form

$$X \cup \left(\bigcup_{v \in X} B_v \right)$$

for some $X \subset\subset V$, and such that $\underline{M}|U$ is coloop-free. For each $U \in I$, let P_U be the collection of presentations of $\underline{M}|U$ which are of the form

$$\underline{A} = (A_v : v \in U \cap B,\ v \in A_v)$$

P_U is finite, since $\underline{M}|U$ is coloop free, and the indexing in terms of $U \cap B$ allows only a finite number of presentations.

For $U_1, \ldots, U_m \in I$ choose a maximal presentation

$\underline{A}_{U_1 \cup \dots \cup U_m} \in P_{U_1 \cup \dots \cup U_m}$. Clearly $\underline{A}_{U_1 \cup \dots \cup U_m}$ can be restricted in a natural way to give presentations $\underline{A}_{U_i} \in P_{U_i}$. Thus for $U_1, \dots, U_m \in I$ we define a choice function $\alpha_{U_1, \dots, U_m}$ on $P_{U_1}, \dots, P_{U_m}$.

By Rado's Selection Principle there exists a choice function α on $(P_i : i \in I)$ such that for any $i_1, \dots, i_n \in I$ there exist $i_1, \dots, i_n, \dots, i_m \in I$ such that

$$\alpha(P_{i_r}) = \alpha_{i_1, \dots, i_m}(P_{i_r}) \quad (1 \leqslant r \leqslant n).$$

For each $v \in B$ we form the union over all $U \in I$ with $v \in U$ of the sets of $\alpha(P_U)$ indexed by v, and call the resulting set A_v. Then $\underline{A} = (A_v : v \in B)$ will be shown to be a maximal presentation of $\underline{M}$.

We first show that $\underline{A}$ is a presentation of $\underline{M}$. Suppose $X \subset\subset V$ and $X \in \underline{M}$. Then we can certainly find $U \in I$ with $X \subset U$ by taking a suitable union Y of circuits of $\underline{M}$ which covers X, then forming $U = Y \cup \bigcup_{v \in Y} B_v$. But

$$\alpha(P_U) = \alpha_{U, U_2, \dots, U_m}(P_U)$$

for some $U_2, \dots, U_m \in I$, and so X is a partial transversal of $\alpha(P_U)$, hence of $\underline{A}$. Suppose on the other hand that $X \subset\subset V$ and X is a partial transversal of $\underline{A}$. Choose $U_1, \dots, U_n \in I$ such that $\alpha(U_1), \dots, \alpha(U_n)$ cover all appearances of X in $\underline{A}$. Then putting $U = U_1 \cup \dots \cup U_n$, we know that

$$\alpha(P_U) = \alpha_{U, U_1, \ldots, U_n, \ldots, U_m} (P_U)$$

for some $U_{n+1}, \ldots, U_m$, and consequently, since $\alpha_{U, U_1, \ldots, U_m}(P_U)$ is obtained by restricting a presentation of $\underline{M}|(U \cup \ldots \cup U_m)$ to U, it follows that X must be independent in $\underline{M}$. Thus the finite independent sets of $\underline{M}$ are the finite partial transversals of $\underline{A}$. However, $\underline{A}$ is restricted, since every $v \in V$ is in a circuit of $\underline{M}$ and consequently is limited to a finite number of sets of $\underline{A}$. Thus $\underline{M} = \underline{M}(\underline{A})$.

We have shown, incidentally, that the property of an independence structure of being transversal is of finite character (see [28]).

Now let $\underline{E} = (E_i : i \in I)$ be any other presentation of $\underline{M}$. For each $X \subset\subset V$ put

$$I_X = \{i \in I : E_i \cap X \neq \emptyset\}.$$

$$B_X = \{v \in B : A_v \cap X \neq \emptyset\}.$$

Put $J = \{X \subset\subset V\}$. Then for each $X \in J$ we know that $(A_v \cap X : v \in B_X)$ is obtained by restricting a maximal presentation of, say, $\underline{M}|Y$ to X, where $X \subseteq Y \subset\subset V$. But then $(E_i \cap Y : i \in I_Y)$ is another presentation of $\underline{M}|Y$, and we know that the latter presentation can be embedded in the former, that is, there exists an injection $\beta' : I_Y \to B_Y$ such that $E_i \subseteq A_{\beta(i)}$ $(i \in I_Y)$. Put $\beta = \beta'|_X$. For each $X \in J$ let K_X be the set of injections $\beta : I_X \to B_X$ such that $E_i \subseteq A_{\beta(i)}$ $(i \in I_X)$. For $X_1, \ldots, X_m \in J$ let the choice function $\alpha_{X_1, \ldots, X_m}$ on $K_{X_1}, \ldots, K_{X_m}$ be chosen as the restrictions of an injection of

$I_{X_1 \cup \ldots \cup X_m}$ into $B_{X_1 \cup \ldots \cup X_m}$ to $X_1, \ldots, X_m$ respectively.

By Rado's Selection Principle we form a choice function on $\underline{K} = (K_X : X \in J)$. Now if $i \in I_{X_1}$ and $i \in I_{X_2}$ then $\alpha(K_{X_1})(i) = \alpha(K_{X_2})(i)$, since the two injections are both restrictions of some injection of $I_{X_1 \cup \ldots \cup X_m}$ for some $X_3, \ldots, X_m$. Thus we may define an injection $\beta : I \to B$ by taking $\beta(i) = \alpha(K_X)(i)$ for any X with $i \in I_X$. It is trivial to verify that β is such that $E_i \subseteq A_{\beta(i)}$ for all $i \in I$.

Suppose now that $\underline{E} = (E_i : i \in I)$ and $\underline{F} = (F_j : j \in J)$ are two presentations of $\underline{M}$ such that there exist injections $\alpha : I \to J$ and $\beta : J \to I$ such that $E_i \subseteq F_{\alpha(i)}$ for all $i \in I$ and $F_j \subseteq E_{\beta(j)}$ for all $j \in J$. We shall show that both α and β must be bijections, and that $E_i = F_{\alpha(i)}$ for all $i \in I$, and $F_j = E_{\beta(j)}$ for all $j \in J$. This will prove the uniqueness of the maximal presentation.

Suppose $k \in I$ and consider $k_m = (\beta\alpha)^m(k)$ for $m = 0, 1, 2, \ldots$ Then $E_k \subseteq E_{k_m}$ for all m, and so, since $\underline{E}$ and $\underline{F}$ are restricted, therefore $k_m = k_n$ for some $m \geqslant n$. But then

$$\beta . \alpha(\beta\alpha)^{m-1}(k) = \beta . \alpha(\beta\alpha)^{n-1}(k)$$

and since β is injective, we have

$$\alpha(\beta\alpha)^{m-1}(k) = \alpha(\beta\alpha)^{n-1}(k)$$

Continuing, we have $(\beta\alpha)^p(k) = (\beta\alpha)^{m-n}(k) = k_p = k$. But then $\beta . \alpha(k_p) = k$, and so β is a surjection. Moreover, if we had $E_k \subset F_{\alpha(k)}$ we should have $E_k \subset E_{k_1} \subseteq \ldots \subseteq E_{k_p} = E_k$, a contradiction.

Thus $E_k = F_{\alpha(k)}$ as required. By symmetry α is surjective and $F_j = E_{\beta(j)}$ for any $j \in J$.

A note on Dilworth's Theorem.

We use a similar method to that used in Lemma 5 and Theorem 12 to deduce Dilworth's Theorem from Hall's Theorem.

Let V be a poset under $\leqslant$. For each $v \in V$ put

$$B_v = \{u \in V : v > u\}$$

We can consider there to be a graph G on V with $(v, u) \in E$ if and only if $v > u$. Then $B_v = A_v - \{v\}$. A chain in V is a set $C = \{v_1, \ldots, v_n\} \subseteq V$ such that $v_1 > v_2 > \ldots > v_n$. Thus C is a path in G.

Lemma 24 V is the union of p disjoint chains if and only if $\underline{B}$ has a partial transversal of defect p.

Proof Suppose $V = C_1 \cup \ldots \cup C_p$ where $C_1, \ldots, C_p$ are disjoint chains of V, and let X be the p-set consisting of the maximal elements of each chain. We define $\alpha: (V - X) \to V$ by putting $\alpha(v)$ equal to the unique predecessor of v in whichever chain v happens to be. Clearly $v \in B_{\alpha(v)}$ for all $v \in V - X$, and $V - X$ is a partial transversal of $\underline{B}$ of defect p.

Conversely, suppose that $V - X$ is a partial transversal of $\underline{B}$ of defect p, so that $|X| = p$, and let the injection $\alpha:(V - X) \to V$

be such that $v \in B_{\alpha(v)}$ for all $v \in V - X$. For any $u \in V - X$ we can construct a chain consisting of $u, \alpha(u), \ldots, \alpha^p(u)$, where p is the first positive integer such that $\alpha^p(u) \in X$. Clearly $\alpha^p(u) > \ldots > \alpha(u) > u$. Let $C_1, \ldots, C_t$ be the collection of maximal chains which can be constructed in this way. Then these chains are disjoint since α is injective, and together cover $V - X$. We cover the remainder of X with $p - t$ single element chains.

An <u>antichain</u> in V is a subset $X \subseteq V$ no two elements of which are comparable.

<u>Theorem 25</u> (<u>Dilworth</u>) V may be covered with p disjoint chains if and only if V contains no antichain of cardinal greater than p.

<u>Proof</u> Suppose V can not be covered with p disjoint chains. Then by Lemma 24 and the defect version of Hall's Theorem, we have, for some $Z \subseteq V$,

$$\left| \bigcup_{v \in Z} B_v \right| < |Z| - p \, .$$

Let X be the collection of maximal elements of Z, so that X is an antichain. Then

$$\bigcup_{v \in Z} B_v = \{u \in V;\ u < x \text{ for some } x \in X\} = Z - X$$

and so

$$|Z| - p > \left| \bigcup_{v \in Z} B_v \right| = |Z - X| = |Z| - |X|$$

that is, $|X| > p$ as required.

Conversely, suppose that X is an antichain with $|X| = q$. Then put $Z = \{v \in V: v \leqslant x$ for some $x \in X\}$. We see that

$$\bigcup_{v \in Z} B_v = Z - X,$$

$$\left| \bigcup_{v \in Z} B_v \right| = |Z| - q$$

and so V is not the union of p disjoint chains if $p < q$.

We again obtain Hall-type conditions, and an alternative formulation of a well-known theorem.

The author has since discovered that Fulkerson has derived Dilworth's Theorem from Menger's Theorem by a similar method to the above (see: D. R. Fulkerson, "Note on Dilworth's Decomposition Theorem for Partially Ordered sets", Proc. Amer. Math. Soc. Vol. 7 (1956), 701 - 2).

2. LINEAR REPRESENTABILITY

An independence structure M on a set S is said to be linear, representable, or linearly representable over a field F if there exists some mapping f of S into some vector space V over F such that $U \subseteq S$ is independent in M if and only if $f|_U$ is a bijection of U onto an independent set f(U) of vectors of V. If M is representable over GF(2), we say that M is binary (see [24]). A structure which is representable over every field is called regular. If there exists some field over which M is representable, then we simply say that M is representable.

Rado [33] showed that a matroid is representable over a field of characteristic p if and only if it is representable over some $GF(p^r)$, and that it is representable over a field of characteristic zero if and only if it is representable over some algebraic extension of the rationals. Tutte [36] characterised binary matroids as those which do not contain the 2-uniform matroid on four elements as a minor, and regular matroids as those which are binary and do not contain the Fano matroid or its dual as a minor.

Edmonds [9] showed that any transversal matroid is representable over a transcendental extension of the rationals. Independently Mirsky and Perfect [25] showed that this result held true for general transversal structures. Piff and Welsh [29] showed that a representation of a transversal matroid could be obtained over any sufficiently large field.

Ingleton [16] recently obtained necessary conditions for a matroid to be representable. Vamos [37] obtained necessary and sufficient conditions involving a certain polynomial ideal, and showed that the property of being representable is of finite character. He also showed that a matroid is representable over a field of characteristic zero if and only if it is representable over an infinite number of fields of different characteristics.

The characteristic set

The characteristic set $C(\underline{M})$ of a matroid $\underline{M}$ is the set of characteristics of fields over which $\underline{M}$ is representable. A point arising from work of Ingleton [16] and Vamos [37] is the question of what sets of numbers are the characteristic sets of some matroid. Vamos showed that $0 \in C(\underline{M})$ if and only if $C(\underline{M})$ is infinite. The Fano matroid with one line missing has characteristic set $P - \{2\}$ where $P = \{0, 2, 3, 5, 7, 11, \ldots\}$. Ingleton also gives a matroid with characteristic set $P - \{3\}$. Lazarson [20] produced, for any prime p, a matroid with characteristic set not containing p (and not containing certain other primes as well).

We discuss Lazarson's matroids in the context of fields, but the argument remains the same for division rings. Let F be a field of characteristic p, and let $\{\underline{e}_1, \ldots, \underline{e}_n\}$ be independent vectors over F. Put $\underline{e} = \underline{e}_1 + \ldots + \underline{e}_n$ and consider the linear matroid $\underline{M}(n, p)$ on

$$S = \{\underline{e}_1, \ldots, \underline{e}_n, \underline{e}, \underline{e} - \underline{e}_1, \ldots, \underline{e} - \underline{e}_n\}.$$

Lazarson restricted his attention to the case where $p \neq 0$ was such that $p \mid (n - 1)$, and showed that if $q \nmid (n - 1)$, then $q \notin C(\underline{M}(n, p))$. We prove a more general result, which shows the existence of certain characteristic sets.

<u>Theorem 1</u> We have

$$C(\underline{M}(n, p)) = \begin{cases} \{p\} , & 0 < p < n \\ \{0\} \cup \{q\colon q \geqslant n,\ q \text{ prime}\}, & p \geqslant n \text{ or } p = 0. \end{cases}$$

<u>Proof</u> Suppose $\underline{M}(n, p)$ is representable over a field H, with a representation $g : S \to V(H)$. Put $g(\underline{e}_i) = \underline{f}_i$ $(i = 1, \ldots, n)$. Suppose $g(\underline{e}) = \underline{f}$, where

$$\underline{f} = a_1\underline{f}_1 + \ldots + a_n\underline{f}_n \qquad (a_1, \ldots, a_n \in H).$$

Then without loss of generality we can assume $a_1 = \ldots = a_n = 1$, since we can always alter g so that $g(\underline{e}_i) = a_i\underline{f}_i$ $(i = 1, \ldots, n)$ if necessary. Thus assume $\underline{f} = f_1 + \ldots + \underline{f}_n$. Now $\{\underline{e}_1, \underline{e}, \underline{e} - e_1\}$ is a circuit, and also $\{\underline{e} - \underline{e}_1, \underline{e}_2, \ldots, e_n\}$ is a circuit. These two facts imply that

$$\begin{aligned} g(e - e_1) &= (b_1 + b_2)\underline{f}_1 + b_2\underline{f}_2 + \ldots + b_2\underline{f}_n \\ &= c_2\underline{f}_2 + \ldots + c_n\underline{f}_n \end{aligned}$$

for some $b_1, b_2, c_2, \ldots, c_n \in H$, and so $b_1 + b_2 = 0$ and $g(e - e_1) = b_2(\underline{f} - \underline{f}_1)$. Again we can assume that $b_2 = 1$ since we can always alter g if necessary. Thus we can assume that

$$g(\underline{e} - \underline{e}_i) = \underline{f} - \underline{f}_i \qquad (i = 1, \ldots, n).$$

Let I_n be the $n \times n$ identity matrix, J_n the $n \times n$ matrix of 1's, and K_n the $n \times 1$ matrix of 1's. Then $\underline{M}(n, p)$ may be considered as the set of columns of the matrix

$$[I_n \,\vdots\, J_n - I_n \,\vdots\, K_n]$$

over any field H over which $\underline{M}(n, p)$ is representable. We work out all sub-determinants of this matrix which are of size $n \times n$. Then the corresponding set of n columns is dependent if and only if the determinant is zero modulo q, where q is the characteristic of H.

First, $|I_n| = 1$. If we take the first $(n - s)$ columns of I_n and some s columns of $J_n - I_n$, $0 < s \leq n$, then we need only work out the lower right $s \times s$ determinant:

$$|R_s| = \left|\begin{array}{c:c} I_{n-s} & 0 \\ \hdashline 0 & R_s \end{array}\right|$$

If two rows of R_s consist entirely of 1's, then $|R_s| = 0$. Otherwise we have, to within a factor of -1, one of two other cases to consider:

a) $R_s = J_s - I_s$

$$|R_s| = \begin{vmatrix} 0 & 1 & & & 1 \\ 1 & 0 & 1 & & \\ 1 & \ddots & 0 & \ddots & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 1 & & & & 0 \end{vmatrix}$$

Adding every other row to the first, we reduce it to a row of terms $(s - 1)$. Taking out the factor $(s - 1)$, we are reduced to case b):

b)

$$|R_s| = \left|\begin{array}{c|c} 1 & \\ 1 & \\ \vdots & J_{s-1} - I_{s-1} \\ \vdots & \\ \hline 1 & 1 \; - \; - \; - \; 1 \end{array}\right| = \left|\begin{array}{c|c} K_{s-1} & J_{s-1} - I_{s-1} \\ \hline I_1 & K^{T}_{s-1} \end{array}\right|$$

Subtracting the second column from the first and expanding by the first column, we see that

$$|R_s| = \left|\begin{array}{c|c} 1 & 0 \; 1 \; 1 \; - \; - \; - \; 1 \\ \hline 0 & \\ 0 & \\ \vdots & R_{s-1} \\ \vdots & \\ 0 & \end{array}\right| = |R_{s-1}|$$

$$= \ldots\ldots = |R_2| = 1$$

Thus $|J_s - I_s| = \pm (s - 1)$

Finally, if the column K_n is included together with any column of I_n or $J_n - I_n$, then subtraction of the latter from the former reduces us to a case already considered.

Thus the only values taken by determinants are

$$0, \pm 1, \ldots, \pm (n - 1).$$

Thus if $p < n$ and $p \neq q$ then some determinant has value $p \neq 0$ mod q and 0 mod p, so $q \notin C(\underline{M}(n, p))$. If $p, q \geqslant n$, or $p = 0$ and $q \geqslant n$, or $q = 0$ and $p \geqslant n$, then $\underline{M}(n, p) = \underline{M}(n, q)$. The conclusion of the theorem now follows.

The problem of determining possible characteristic sets is closely connected with the problem of characterizing matroids which are representable over a given field.

Binary and regular matroids.

The only conditions existing at present for a matroid to be representable over a given field are those of Tutte. We give here a new, fairly short ad-hoc proof of his theorem on binary matroids.

Theorem 2 The matroid $\underline{M}$ is binary if and only if it does not contain as a minor the 2-uniform matroid on four elements.

Proof We first make a few trivial observations on the effect of contracting an element of a binary matroid. We know that if $z \in S$ and C_1 is a circuit of $\underline{M}.(S - \{z\})$, then either C_1 or $C_1 \cup \{z\}$ is a circuit of $\underline{M}$. Moreover, if C is a circuit of $\underline{M}$ and $z \in C$, then $C - \{z\}$ is a circuit of $\underline{M}.(S - \{z\})$. If $z \notin C$ then either C is a circuit of $\underline{M}.(S - \{z\})$ or some $U \subset C$ is a circuit of $\underline{M}.(S - \{z\})$. But this implies that $U \cup \{z\}$ is a circuit of $\underline{M}$, hence that $(C - U) \cup \{z\}$ is a circuit of $\underline{M}$, since $\underline{M}$ is binary and C is a circuit. Therefore C is the disjoint union of two circuits of $\underline{M}.(S - \{z\})$.

We know that $\underline{M}$ is binary if and only if the symmetric difference of any two circuits of $\underline{M}$ is a disjoint union of circuits of $\underline{M}$ [24]. We also know that the conditions of the theorem are necessary, since any minor of a binary matroid is binary, whilst the 2-uniform matroid on four elements is not binary. We prove sufficiency by induction on $|S|$. The result is trivial for $|S| < 4$.

Suppose $\underline{M}$ is a matroid on S satisfying the excluded minor condition, and suppose the theorem is true on all smaller sets. We shall show that the symmetric difference of any two circuits of $\underline{M}$ is a disjoint union of circuits of $\underline{M}$. Thus we may assume that $S = C_1 \cup C_2$ where C_1 and C_2 are circuits of $\underline{M}$, and $C_1 \cap C_2 \neq \emptyset$. Put $X = C_1 \cap C_2$, $Y_1 = C_1 - C_2$, $Y_2 = C_2 - C_1$. We have to show that $Y = Y_1 \cup Y_2$ is a disjoint union of circuits.

a) If $|Y_1| = |Y_2| = 1$ and either $|X| = 1$ or $Y_1 \cup Y_2$ is a circuit, the result is trivial.

b) $Y_1 = \{y_1\}$, $Y_2 = \{y_2\}$ and Y is independent. For some $x_1, x_2 \in X$, $Y \cup X - \{x_1, x_2\}$ is a base of $\underline{M}$. But then $\underline{M}.\{x_1, x_2, y_1, y_2\}$ is 2-uniform, a contradiction.

c) $Y_1 = \{y, z, \dots\}$. $C_1 - \{y\}$ is a circuit of $\underline{M}.(S - \{y\})$ and, by induction, C_2 is a disjoint union of at most two circuits of $\underline{M}.(S - \{y\})$. Thus the symmetric difference of $C_1 - \{y\}$ and C_2 is a disjoint union of circuits of $\underline{M}.(S - \{y\})$. We may thus write

$$Y = S_1 \cup \dots \cup S_r \cup \dots \cup S_t$$

where S_i $(i = 1, \dots, t)$ is a circuit of $\underline{M}$ and

$$S_i \cap S_j = \begin{cases} \{y\} & i, j \leq r \\ \emptyset & \text{otherwise} . \end{cases}$$

Suppose r were even. Then by the induction hypothesis

$$Y = T_1 \cup \dots \cup T_h \cup \{y\},$$

where $T_1, \dots, T_h$ are disjoint circuits of $\underline{M}$, since symmetric differences of $S_1, \dots, S_r$ may be taken in pairs. But by the induction hypothesis, $\underline{M}|(S - \{y\})$ is binary and so for each $i = 1, \dots, h$ $T_i - \{y\}$ is a disjoint union of at most two circuits of

$$\underline{M}|(S - \{y\}).(S - (\{y\} \cup \{z\})),$$

hence of $\underline{M}.(S - \{z\})$. Thus

$$Y - \{z\} = R_1 \cup \dots \cup R_k \cup \{y\}$$

where $R_1, \ldots, R_k$ are circuits of $\underline{M}.(S - \{z\})$. But $Y - \{z\}$ is the symmetric difference of $C_1 - \{z\}$ and C_2, and C_2 is the disjoint union of at most two circuits of $\underline{M}.(S - \{z\})$, which is binary by the induction hypothesis. Thus $C_1 - \{z\}$ is the symmetric difference of at most three circuits of $\underline{M}.(S - \{z\})$, and finally $\{y\}$ is a symmetric difference of circuits of $\underline{M}.(S - \{z\})$, a contradiction.

Thus r is odd, and we may pair $S_1, \ldots, S_{r-1}$, take symmetric differences in pairs, and use the induction hypothesis.

An easy generalization of this result to other prime fields does not seem possible.

We now show that the properties of being representable over a given finite field or of being regular are of finite character, thus strengthening Vamos' result, which says that if every finite restriction of $\underline{M}$ is representable over some field, then $\underline{M}$ is representable over some (possibly other) field.

Theorem 3 Let $\underline{M}$ be an independence structure on S, and F a finite field. Then $\underline{M}$ is representable over F if and only if every finite restriction of $\underline{M}$ is representable over F.

Proof Suppose that every finite restriction of $\underline{M}$ is representable over F. Let B be a base of $\underline{M}$. For each $s \in S - B$, let C_s be the fundamental circuit of s with respect to B. Put

$$B_s = \begin{cases} C_s - \{s\}, & s \in S - B \\ \{s\} & , s \in B . \end{cases}$$

Let V be a vector space over F generated by independent vectors $(\underline{v}_b : b \in B)$. For each $s \in S$ put

$$V_s = \{\underline{v} \in V\colon \underline{v} \text{ is in the span of } \{\underline{v}_b\colon b \in B_s\}\}.$$

Clearly, for any $T \subset\subset S$ we may put

$$T' = T \cup \left(\bigcup_{s \in T} B_s \right)$$

and choose a representation $f_T\colon T' \to V$ for $\underline{M}|T'$ such that $f_T(b) = \underline{v}_b$ for all $b \in T' \cap B$. Since $f_T(s) \in V_s$ for all $s \in T$, f_T induces a choice function h_T on the family $(V_s : s \in T)$ by

$$h_T(V_s) = f_T(s).$$

By Rado's Selection Principle, there exists a choice function h for $(V_s\colon s \in S)$ such that for any $T \subset\subset S$ we have $h|_T = h_U|_T$ for some U with $T \subseteq U \subset\subset S$. Define $f\colon S \to V$ by $f(s) = h(V_s)$ for all $s \in S$. From the property of h above, we may take T to be either a circuit or a finite independent set, and clearly f must be a representation for $\underline{M}$.

<u>Corollary 4</u> The following conditions on an independence structure $\underline{M}$ are equivalent:

1) $\underline{M}$ is binary;

2) The symmetric difference of any finite collection of circuits of $\underline{M}$ is a disjoint union of circuits of $\underline{M}$;

3) $\underline{M}$ does not contain the 2-uniform matroid on four elements as a minor;

4) For any circuit C and cocircuit D, $|C \cap D|$ is even.

Proof The equivalence of 1), 2) and 3) and 1) $\Rightarrow$ 4) follow from [24, 36] and Theorem 3. It only remains to show that if $|C \cap D|$ is always even then $\underline{M}$ is binary. However, we write out the incidence matrix A of the fundamental cocircuits of some base B, the cocircuits indexing the rows and S indexing the columns. For any $s \notin B$, s is in only a finite number of fundamental cocircuits, namely, those associated with elements of its fundamental circuit with respect to B. It is easily verified as in the finite case that the columns of A give a representation of $\underline{M}$ over $GF(2)$.

Tutte [36] showed that a finite matroid $\underline{M}$ on S is regular if and only if it has a unimodular representation over the rationals, that is, a representation $f: S \to V$ over the rationals such that if $\{s_1, \ldots, s_m\}$ is a circuit of $\underline{M}$ then for some permutation $\{i_1, \ldots, i_m\}$ of $\{1, \ldots, m\}$ we have

$$f(s_{i_1}) + \ldots + f(s_{i_r}) - f(s_{i_{r+1}}) - \ldots - f(s_{i_m}) = 0 \qquad (^*).$$

Theorem 5 An independence structure $\underline{M}$ is regular if and only if every finite restriction of $\underline{M}$ is regular.

Proof Similar to the proof of Theorem 3, but taking F as the rationals and

$V_s = \{\underline{v} \in V : v = v_{b_1} + \dots + v_{b_r} - v_{b_{r+1}} - \dots - v_{b_n},\ \text{some } b_1, \dots, b_n \in B_s\}$.

We also choose f_T to be a unimodular representation.

We obtain a unimodular representation $f:S \to V$ over the rationals, which is also a representation over every prime field, hence over every field. f satisfies condition (*).

Corollary 6 The following conditions on an independence structure $\underline{M}$ are equivalent:

1) $\underline{M}$ is regular;

2) $\underline{M}$ is binary and does not contain the Fano matroid or its dual as a minor;

3) The circuit and cocircuit incidence matrices $\underline{C}$ and $\underline{D}$ may be oriented, that is, their non-zero entries may be replaced by $+1$ or -1, in such a way that the dot product of any row of $\underline{C}$ with any row of $\underline{D}$ is zero. ($\underline{C}$ and $\underline{D}^T$ are orthogonal).

Proof The equivalence of 1) and 2) follows from [36] and Theorem 5. Suppose $\underline{C}'$ and $\underline{D}'$ may be obtained by orienting $\underline{C}$ and $\underline{D}$, and $\underline{C}'$ and $\underline{D}'^T$ are orthogonal. Then taking a base of $\underline{M}$ and just taking the rows of $\underline{D}'$ which correspond to the fundamental cocircuits with respect to B, the columns then give a representation of $\underline{M}$ (as in Corollary 4.) over any field. Hence 3) => 1).

Finally, suppose $\underline{M}$ is regular, and thus has a representation f, by Theorem 5, which satisfies (*). Let $C = \{s_1, \ldots, s_n\}$ be a circuit of $\underline{M}$, and suppose

$$f(s_1) + \ldots + f(s_r) - f(s_{r+1}) - \ldots - f(s_n) = 0.$$

In $\underline{C}$, we change the + 1's in positions $(C, s_{r+1}), \ldots, (C, s_n)$ to - 1's. We do the same for all circuits and thus obtain an orientation $\underline{C}'$ of $\underline{C}$. Let D be a cocircuit of $\underline{M}$ and B any base of $\underline{M}$ such that $|B \cap D| = 1$. Consider the representation f expressed in terms of the vectors $(f(b) : b \in B)$, that is, such that, for each $s \in S$, $f(s)$ is expressed as a linear combination of these vectors. Suppose $B \cap D = \{b_1\}$, and consider the set

$\{s \in S : b_1$ is in the fundamental circuit of s with respect to $B\}$.

This set is precisely D, since it is certainly contained in D and necessarily meets every base of $\underline{M}$. Now for each $d \in D$ we take the coefficient of $f(b_1)$ in the expression of d in terms of $(f(b) : b \in B)$ and put it in position (D, d) of $\underline{D}$. Repeating for each cocircuit, we obtain an orientation $\underline{D}'$ of $\underline{D}$. It is now readily verified that the rows of $\underline{C}'$ and $\underline{D}'$ are orthogonal, since the oriented row corresponding to D is orthogonal to the oriented fundamental circuits of its corresponding base B, and so is orthogonal to all of the oriented circuits, as in the finite case, since any circuit can be obtained by combining fundamental circuits.

Operations on matroids

In this section, various matroid operations will be shown to preserve representability. Whitney showed in his original paper that if a matroid $\underline{M}$ is representable over a field F then $\underline{M}^*$ is representable over F, a corollary of which is the fact that any minor of $\underline{M}$ is representable over F.

If $|S| = n$ and $\underline{M}$ is a matroid on S and $k \leqslant n$, we call the matroid with independent sets

$$\{U \subseteq S : U \in \underline{M}, |U| \leqslant k\}$$

the k-truncation of $\underline{M}$.

Theorem 7 Let $\underline{M}$ be a matroid on the finite set S which is representable over the finite field F. Then there exists an integer N such that the k-truncation of $\underline{M}$ is representable over any extension G of F with $|G| > N$. (or over any sufficiently large extension of F).

Proof If $r = r(\underline{M})$, it is sufficient to prove the result for the $(r - 1)$ - truncation $\underline{M}'$ of $\underline{M}$. Let $f : S \to V$ be a representation of $\underline{M}$ over some finite extension G of F in a vector space V of rank r. Let $X_1, \ldots, X_q$ be the independent $(r - 1)$-sets of $\underline{M}$. Consider the planes of V spanned by $f(X_1), \ldots, f(X_q)$. Putting $|G| = t$, each plane contains t^{r-1} elements of V, thus together they contain at most $q.t^{r-1}$ elements. Thus provided $t > q$, they do not cover V. Choose $\underline{v} \in V$ which does not lie in the union of the planes.

Put $T = \{s\} \cup S$, where $s \notin S$, and let $\underline{M}''$ be the matroid on T

induced by the representation $f:T \to V$ given by putting $f(s) = \underline{v}$. We see that $\underline{M}' = \underline{M}^{\pi}.S$, since any independent $(r - 1)$-set of $\underline{M}$ is independent in $\underline{M}^{\pi}.S$, but the rank is reduced to $(r - 1)$ on contraction. Thus $\underline{M}'$ is representable.

Theorem 8 Let $\underline{M}$ be a matroid on S which is representable over the finite field F, and let G be a bipartite graph with vertices $S \cup T$ and edges $E \subseteq T \times S$. Then $\underline{M}' = \underline{M}(G, S)$ is representable over any sufficeintly large extension of F.

Proof Let $r(\underline{M}) = r$. We prove the result by induction on $|T|$. Take $t \in T$ and suppose we have a representation $f:(S \cup T - \{t\}) \to V$ in a vector space over an extension G of F, where V has dimension r. Suppose that t is linked only to $\{s_1, \ldots, s_n\} \subseteq S$ in G. We shall show that we can put

$$f(t) = a_1 f(s_1) + \ldots + a_n f(s_n)$$

for some $a_1, \ldots, a_n \in G$, provided G is large enough, to obtain a representation of $\underline{M}'$. If $s_1, \ldots, s_n$ are all loops the conclusion is trivial. Suppose $\{t\} \cup U$ is a finite dependent set of $\underline{M}'$. Then $s_1, \ldots, s_n$ are all in the span of U, so $a_1 f(s_1) + \ldots + a_n f(s_n)$ is in the span of $f(U)$ for any $a_1, \ldots, a_n \in G$. Suppose on the other hand that $\{t\} \cup U$ is an independent set of $\underline{M}'$. Then at least one of $f(s_1), \ldots, f(s_n)$ is independent of $f(U)$. Let V' be the subspace of V spanned by $f(s_1), \ldots, f(s_n)$. Then for each independent set $\{t\} \cup U$ of $\underline{M}'$ the set $f(U) \cap V'$ will be contained within some hyperplane H_U of V', otherwise V' would be in the span of $f(U)$. If G is sufficiently large, reasoning similar to that in the proof of Theorem 7 will show us that these hyperplanes do not together cover V'. We can find $\underline{v} \in V'$ not in any of the hyperplanes, and put $f(t) = \underline{v}$ to obtain a representation of $\underline{M}'$.

<u>Corollary 9</u> Let $\underline{M}$ be a trnsversal matroid on a set T. Then $\underline{M}$ is representable over any large enough field.

<u>Proof</u> For $\underline{M}$ is induced through a bipartite graph from a matroid in which every subset is independent, and such a matroid is representable over every field.

The <u>union</u> $\underline{M}_1 \vee \ldots \vee \underline{M}_n$ of matroids $\underline{M}_1$ on $S_1, \ldots, \underline{M}_n$ on S_n is the matroid on $S = S_1 \cup \ldots \cup S_n$ with independent sets $X_1 \cup \ldots \cup X_n$ where $X_1 \in \underline{M}_1, \ldots, X_n \in \underline{M}_n$.

<u>Corollary 10</u> Let $\underline{M}_1, \ldots, \underline{M}_n$ be representable over a field F. Then $\underline{M}_1 \vee \ldots \vee \underline{M}_n$ is representable over any sufficiently large extension of F.

<u>Proof</u> For $\underline{M}_1 \vee \ldots \vee \underline{M}_n$ may be induced from matroids $\underline{M}'_1, \ldots, \underline{M}'_n$ isomorphic to $\underline{M}_1, \ldots, \underline{M}_n$, which are on disjoint sets, and $\underline{M}'_1 \vee \ldots \vee \underline{M}'_n$ is clearly representable over F.

Corollary 11 For any matroids $\underline{M}_1, \ldots, \underline{M}_n$,

$$C(\underline{M}_1) \cap \ldots \cap C(\underline{M}_n) \subseteq C(\underline{M}_1 \vee \ldots \vee \underline{M}_n).$$

Proof For if $\underline{M}_1, \ldots, \underline{M}_n$ are representable over fields of characteristic p, then there is some Galois field over which all are representable.

Corollary 12 Let G be a directed graph with vertex set V, and $\underline{M}$ a matroid on V which is representable over a field F. Then $\underline{M}(G, \underline{M})$ is representable over any sufficiently large extension of F.

Proof The dual of Theorem 8 with $\underline{M}'$ restricted to T.

Corollary 13 A gammoid $\underline{M}$ is representable over any sufficiently large field.

Proof The dual of Corollary 9.

It is known that no vector space over an infinite field is the union of a finite number of hyperplanes. Thus Theorem 7 - Corollary 13 remain valid when F is infinite and the phrase 'any sufficiently large extension of' is omitted in the statement of these theorems for infinite F.

3. ALGEBRAIC REPRESENTABILITY

An independence structure $\underline{M}$ on a set S is said to be algebraically representable (or algebraic) over a field F if there exists a mapping f of S into some extension field G of F such that $U \subseteq S$ is independent in $\underline{M}$ if and only if f maps U bijectively onto a set $f(U)$ of independent transcendentals over F.

Ingleton [16] showed the existence of algebraic matroids which were not linear. Thus, the natural algebraic matroid on the set $S = \{r, s, t, rst, rs, st, tr, r+s+t, r+s, s+t, t+r\}$, where r, s and t are independent transcendentals over $GF(2)$, is readily shown not to be linear over any field. A natural generalization based on Theorem 2.1 leads to matroids which are algebraic over $GF(p)$, but not linear over any field.

In the case of fields of characteristic zero, we have

Theorem 1 If $\underline{M}$ is algebraic over a field F of characteristic zero, then $\underline{M}$ is linear over some transcendental extension of F.

Proof This is essentially [19], Ch. 10, Prop. 10.

No one has yet produced a non-algebraic matroid. Defining the algebraic characteristic set in the obvious way, no one has yet determined the characteristic set of any matroid, other than when the matroid is linear over fields of all characteristics. No necessary and sufficient conditions are known for a matroid to be algebraic.

However, there are certain results which can be proved.

Lemma 2 If $\underline{M}$ is algebraic over $F(\alpha)$ and α is algebraic over F, then $\underline{M}$ is algebraic over F.

Proof Suppose $f:S \to G$ is an algebraic representation of $\underline{M}$ over $F(\alpha)$. Suppose $\{s_1, \ldots, s_r\} \in \underline{M}$. Then $\{f(s_1), \ldots, f(s_r)\}$ are independent transcendentals over $F(\alpha)$, hence over F. Conversely, suppose that $\{s_1, \ldots, s_r\} \notin \underline{M}$, so that $\{f(s_1), \ldots, f(s_r)\}$ are algebraically dependent over $F(\alpha)$, and thus, say, $f(s_1)$ is algebraic over $F(\alpha, f(s_2), \ldots, f(s_r))$. Then by an elementary result on algebraic dependence, it follows that $f(s_1)$ is algebraic over $F(f(s_2), \ldots, f(s_r))$. Thus f is an algebraic representation over F.

Repeated application of this Lemma gives

Theorem 3 If $\underline{M}$ is algebraic over the field F, where F is of characteristic p, then $\underline{M}$ is algebraic over $GF(p)(t_1, \ldots, t_m)$ for some independent transcendentals $t_1, \ldots, t_m$ over $GF(p)$.

Proof Let $f:S \to G$ be an algebraic representation of $\underline{M}$ over F. Let X be the set of coefficients in the set of polynomials expressing the dependence of circuits of $\underline{M}$ over F. Then $f:S \to H = GF(p)(X \cup f(S))$ is an algebraic representation of $\underline{M}$, and H has finite transcendence degree m over $GF(p)$. Let $\{t_1, \ldots, t_m\}$ be a transcendence base of H over $GF(p)$, and apply Lemma 2.

I conjecture, but can not prove, that the reduction initiated in Theorem 3 can be continued down to the prime field GF(p).

We turn now to the effect of matroid operations on algebraic matroids. Clearly any restriction of an algebraic matroid is algebraic over the same field. It is not known whether the dual of an algebraic matroid is algebraic.

Theorem 4 Let $\underline{M}$ be a matroid on S which is algebriac over F. Then for $T \subseteq S$, $\underline{M}.T$ is algebraic over some transcendental extension of F.

Proof Let $\underline{f}: S \to G$ be an algebraic representation of $\underline{M}$ over F. Then G is an extension field of $F(f(S - T)) = H$. We shall show that if $f' = f|_T$, then $f': T \to G$ is an algebriac representation of $\underline{M}.T$ over H. For $U \in M.T$ if and only if, for some base B of $(S - T)$ in $\underline{M}$, $B \cup U \in \underline{M}$, which is the case if and only if $f(B \cup U)$ is a set of independent transcendentals over F. But this is true if and only if $f(U)$ is a set of independent transcendentals over F(B), hence over $F(f(S - T)) = H$.

Corollary 5 Every minor of an algebraic matroid is algebraic.

Theorem 6 Let $\underline{M}$ be a matroid on S which is algebriac over F. Then any truncation of $\underline{M}$ is algebraic over some transcendental extension of F.

Proof We only need to prove the result for an $(r - 1)$-truncation $\underline{M}'$ of $\underline{M}$, where $r = r(\underline{M})$. Let $f: S \to G$ be an algebraic representation of $\underline{M}$ over F. Let $\{t_1, \dots, t_r\}$ be the image in G of some base of $\underline{M}$ under f. We look for an element of the form $t = t_1^{a_1} \times \dots \times t_r^{a_r}$ where $a_1, \dots, a_r$ are integers and t is independent of $f(U)$ for any $(r - 1)$-set $U \in \underline{M}$. Such an element t may be found as in the linear case (Theorem 2.7). For the set

$$V = \{s \in G: s = t_1^{a_1} \times \dots \times t_r^{a_r};\ a_1, \dots, a_r \ \text{integers}\}$$

is a module over the integers, the sum in the module being taken as the product in G. Also, for any independent $(r - 1)$-set $U \in \underline{M}$, $\overline{f(U)} \cap V$ has dimension at most $(r - 1)$, where the bar denotes algebraic closure, otherwise $\{t_1, \dots, t_r\}$ would be in the span of $f(U)$. The forbidden elements of V thus lie in the union of a finite collection of hyperplanes of V, and this union can not equal all of V.

Thus we can find the required element t, and as in Theorem 2.7 we extend $\underline{M}$ by one element and then contract this element, to obtain $\underline{M}'$.

Theorem 7 Let $\underline{M}$ be a matroid on S which is algebraic over F, and let G be a bipartite graph with vertex set $S \cup T$ and edge set $E \subseteq T \times S$. Then $\underline{M}(G, \underline{M})$ is algebraic over F.

Proof The proof is similar to the proof of Theorem 2.8, but we make use of multiplication as in the proof of Theorem 6 instead of addition.

Corollary 8 A transversal matroid is algebraic over any field.

Theorem 9 Let G be a finite directed graph on V and M a matroid on V which is algebraic over F. Then M(G, M) is algebraic over some transcendental extension of F.

Proof We use Corollary 1.14, Theorem 7 and Theorem 4. The new transcendentals are introduced to represent the coloops added in Corollary 1.14 a).

4. AUTOMORPHISMS

Let $\underline{M}$ be an independence structure on the set S. The automorphism group $A(\underline{M})$ of $\underline{M}$ is the set of permutations α of S such that $U \in \underline{M}$ if and only if $\alpha(U) \in \underline{M}$.

It is well known that for any group H there exists a graph G with point automorphism group isomorphic to H. In this chapter we show that for any group H there exists an independence structure $\underline{M}$ with automorphism group isomorphic to H. We show that $\underline{M}$ may be chosen to be a graphic, transversal or partition geometry. In addition, we show that there exist matroids $\underline{M}$ such that $A(\underline{M})$ is a group of cyclic permutations of S, contrary to a conjecture of Ingleton.

Automorphism groups of graphs.

Most of the material of this section may be found in Harary [11]. Let G be a graph with vertex set V and edge set E. The point-automorphism group $A_p(G)$ of G is the group of permutations α of V which are such that $(u, v) \in E$ if and only if $(\alpha(u), \alpha(v)) \in E$. The cycle automorphism group $A_c(G)$ is the group of permutations α of E which are such that C is a cycle of G if and only if $\alpha(C)$ is a cycle of G.

Frucht [10] proved that

Theorem 1 For any finite group H there exists a graph G with $A_p(G)$ isomorphic to H.

Sabidussi [35] extended Theorem 1 to infinite groups. He also proved

/

the following theorem [34].

<u>Theorem 2</u> For any group H and positive integer p there exists a p-connected graph G with $A_p(G)$ isomorphic to H.

An extension of Theorem 2 to the case where p is any infinite cardinal is given in [13], but the above result is sufficient for our purposes.

<u>Graphic geometries</u>.

Let $\underline{M}(G)$ be the cycle independence structure of G. Then clearly

$$A(M(G)) = A_c(G).$$

<u>Lemma 3</u> Let G be a 3-connected graph on V, with $|V| \geqslant 3$. Then

$$A_c(G) \cong A_p(G).$$

<u>Proof</u> The finite case was proved by Whitney [41].

Suppose $\alpha \in A_c(G)$ and $v \in V$. Put

$$st(v) = \{e \in E : e = (v, w),\ w \in V\}.$$

$st(v)$ is a cocircuit of $M(G)$, since $\underline{M}(G)$ is non-separable. Since α maps bases to bases, it necessarily maps hyperplanes to hyperplanes, and consequently cocircuits to cocircuits.

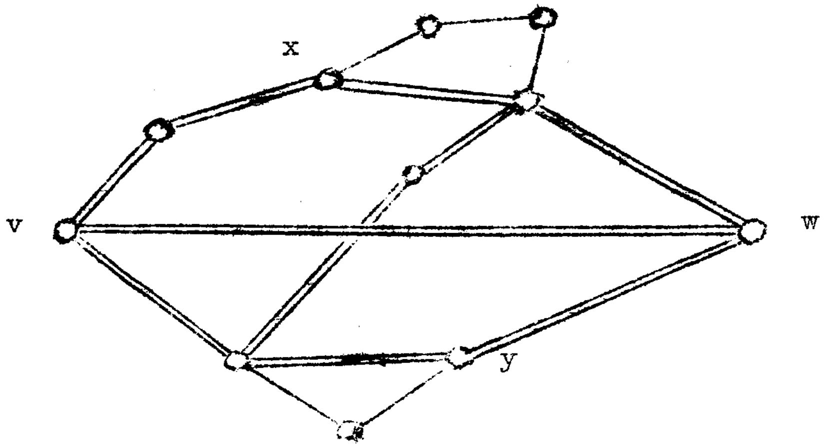
We wish to show that for some $v' \in V$ we have $\alpha(st(v)) = st(v')$. Now if $e, f \in E - st(v)$ then, since G is 3-connected, $G - v$ is at least 2-connected and hence there exists a circuit $C \subseteq E - st(v)$ such that $e, f \in C$. But then $\alpha(e), \alpha(f) \in \alpha(C)$, and so the removal of $\alpha(st(v))$ from G results in a graph G' in which any pair of edges is contained in a circuit. But this is only possible if $G - \alpha(st(v))$ has one connected component consisting only of a single vertex v' say, and we must have $\alpha(st(v)) = st(v')$.

Thus α induces a map $\alpha' : V \to V$ by putting $\alpha'(v) = v'$ if $\alpha(st(v)) = st(v')$. α' must be a bijection, by symmetry, and the correspondence $\alpha <-> \alpha'$ is a bijection of $A_c(G)$ onto $A_p(G)$ which preserves the group structure of $A_c(G)$, that is, $(\alpha\beta)' = \alpha'\beta'$ for all $\alpha, \beta \in A_c(G)$. Thus the correspondence is a group isomorphism .

Combining Lemma 3 with Theorem 2 with $p \geq 3$ we have

Theorem 4 For any group H there exists a graphic, non-transversal, non-separable geometry $\underline{M}$ with $A(\underline{M}) \cong H$.

Proof $\underline{M} = \underline{M}(G)$ as constructed in Theorem 2 with $p \geq 3$ is non-separable and is also a geometry. We show that $\underline{M}$ is not base-orderable by showing that $\underline{M}$ contains the matroid $\underline{M}(K_4)$ of the complete graph K_4 as a minor. However, every 3-connected graph contains a homeomorph of K_4 if it has no parallel edges. For suppose $v, w \in V$ and $(v, w) \in E$. Then there exist at least two other paths from v to w in G .



We take vertices x and y on these two paths. Then $G - v - w$ must contain a path from x to y, and part of this path, plus the three paths from v to w give a homeomorph of K_4.

Corollary 5 For any group H, there exists a geometric lattice with automorphism group isomorphic to H.

Proof Take the geometric lattice of flats of the geometry of Theorem 4 (see, e.g., [8]).

Transversal geometries

Lemma 6 Let $\underline{M}(A)$ be a coloop-free transversal structure on S, and suppose $\underline{A} = (A_i : i \in I)$ is maximal. Then $A(\underline{M}(\underline{A}))$ is equal to the set of permutations α of S which permute $\underline{A}$, that is, are such that there exists some permutation α' of I such that

$$\alpha(A_i) = A_{\alpha'(i)} \text{ for all } i \in I \qquad (^*)$$

Proof Suppose α permutes $\underline{A}$. Then there exists α' satisfying $(^*)$. Suppose $X = \{x_{i_1}, \ldots, x_{i_n}\} \in \underline{M}(\underline{A})$, and $x_{i_r} \in A_{i_r}$ $(r = 1, \ldots, n)$. Then clearly $\alpha(x_{i_r}) \in A_{\alpha'(i_r)}$ $(r = 1, \ldots, n)$, so $\alpha(X) \in \underline{M}(\underline{A})$. But then, by symmetry, $\alpha^{-1}(X) \in \underline{M}(\underline{A})$, and so $\alpha \in A(\underline{M}(\underline{A}))$.

Conversely, suppose $\alpha \in A(\underline{M}(\underline{A}))$, and consider the family $\underline{A}' = (\alpha(A_i) : i \in I)$. If $X \in \underline{M}(\underline{A})$ then $X \in \underline{M}(\underline{A}')$, and conversely if $X \in \underline{M}(\underline{A}')$ then $X \in \underline{M}(\underline{A})$, so $\underline{A}'$ is a presentation for $\underline{M}(\underline{A})$. Suppose $\underline{A}'$ were not maximal, so that, say, $\underline{M}(\underline{A}'') = \underline{M}(\underline{A}')$ where, for some $j \in I$,

$$A_j'' = A_j \cup \{s\} \qquad s \notin A_j'$$

$$A_i'' = A_i' \qquad i \neq j$$

Then $\underline{B} = (B_i : i \in I)$ is a presentation of $\underline{M}(\underline{A})$, where

$$B_j = A_j \cup \{\alpha^{-1}(s)\}$$

$$B_i = A_i \qquad i \neq j.$$

However, $\underline{A}$ is maximal, so it must be possible to embed $\underline{B}$ in $\underline{A}$. But then by Theorem 1.23 $\underline{B}$ is maximal and for some $\beta : I \to I$ we have $B_i = A_{\beta(i)}$. However, clearly the set B_j occurs a different number of times in $\underline{B}$ and $\underline{A}$. (each number of repetitions being finite because $\underline{B}$ and $\underline{A}$ are restricted) giving a contradiction. Thus $\underline{A}'$ is maximal and for some $\alpha' : I \to I$ we have $(^*)$.

<u>Theorem 7</u> For any group H there exists a non-binary transversal geometry $\underline{M}(\underline{A})$ with automorphism group isomorphic to H.

<u>Proof</u> Let G be a graph without endpoints, that is, such that every vertex has degree at least two, and such that $A_p(G) \cong H$. We define a fundamental transversal structure $\underline{M}(\underline{A})$ on $E \cup V$, where $\underline{A} = (A_v : v \in V)$, and

$$A_v = \{v\} \cup \{(v, w) \in E\}.$$

We first observe that $\underline{A}$ is a maximal presentation. For if $(v, w) \in E$ then (v, w) can not be added to A_x for $x \neq v, w$, since $\{v, w, (v,w)\}$ is a circuit. Similarly if $v \in V$ then there exist $w, x \in V$ such that $w \neq x$ and $(v, w), (v, x) \in E$. But then it follows that v is restricted to Λ_v. Thus $\underline{\Lambda}$ is maximal.

Consequently, by Lemma 6, if $\alpha \in \Lambda(\underline{M}(\underline{\Lambda}))$ then there exists a permutation $\alpha' : V \to V$ such that

$$\alpha(\Lambda_v) = \Lambda_{\alpha'(v)} \quad \text{for all} \quad v \in V. \qquad (^*)$$

Now for each $v \in V$, v is an element of only one of the sets of $\underline{\Lambda}$, namely Λ_v, whilst for each $e = (v, w) \in E$, $e \in \Lambda_v$ and $e \in \Lambda_w$. Thus $\alpha(v)$ must be a vertex of G by $(^*)$, and we must have $\alpha' = \alpha|_V$. Also $e \in (v, w) \in E$ is such that $e \in \Lambda_v \cap \Lambda_w$. But

$$\{\alpha(e)\} = \alpha(\Lambda_v) \cap \alpha(\Lambda_w) = \Lambda_{\alpha(v)} \cap \Lambda_{\alpha(w)} = \{(\alpha(v), \alpha(w))\}$$

and so $\alpha(e) = (\alpha(v), \alpha(w))$. Thus α' is an incidence-preserving permutation of V, that is, a point-automorphism of G.

Thus the mapping $\Lambda(\underline{M}(\underline{\Lambda})) \to \Lambda_p(G)$ given by $\alpha \to \alpha'$ is readily seen to be a homomorphism, and to be onto $\Lambda_c(G)$. Its kernel is trivially the identity, and so $\Lambda(\underline{M}(\underline{\Lambda})) \cong \Lambda_p(G)$.

If we choose G to contain a circuit, say $\{(v_0, v_1), (v_1, v_2), \ldots, (v_n, v_0)\}$ then the set $C = \{v_0, (v_0, v_1), (v_1, v_2), \ldots, (v_n, v_0)\}$ is a circuit of $\underline{M}(\underline{\Lambda})$. Also Λ_{v_0} is a cocircuit of $\underline{M}(\underline{\Lambda})$, and $|\Lambda_{v_0} \cap C| = 3$, showing that $\underline{M}(\underline{\Lambda})$ is non-binary by Corollary 2.4.

The geometry constructed in Theorem 7 is non-graphic, since it is non-binary.

Corollary 8 For any group H there exists a geometric strict gammoid $\underline{M}$ with $\Lambda(\underline{M}) \cong H$.

Proof The fundamental transversal structure in Theorem 7 is a strict gammoid which, in the infinite case, is clearly of finite character.

An alternative construction is given in -

Theorem 9 For any group H there exists a non-fundamental transversal geometry $\underline{M}(\underline{A})$ with $A(\underline{M}(\underline{A})) \cong H$.

Proof Let G be a 4-connected graph with $A_p(G) \cong H$. Define $\underline{A} = (A_v : v \in V)$ on E by putting $A_v = \{(v,w) \in E\}$. We show that $\underline{A}$ is a maximal presentation of $\underline{M}(\underline{A})$. Suppose $e = (u, w) \in G$, and u, w, v are distinct vertices of G, so that $(u, w) \notin A_v$. Since G is 4-connected, there exist two vertex-disjoint paths from u to w in $G - v - e$. Let X be the union of the edge sets of these paths. Then $X \cup \{e\}$ is a circuit of $\underline{M}(\underline{A})$. However, if we add e to A_v, $X \cup \{e\}$ becomes independent. Thus $\underline{A}$ is a maximal presentation. Hence, by Lemma 6, for any $\alpha \in A(\underline{M}(\underline{A}))$ there exists a map $\alpha' : V \rightarrow V$ such that $\alpha(A_v) = A_{\alpha'(v)}$ for all $v \in V$. Also, if $e = (v, w) \in E$ then $\{e\} = A_v \cap A_w$ so $\alpha(A_v) \cap \alpha(A_w) = \{\alpha(e)\}$. But then $A_{\alpha'(v)} \cap A_{\alpha'(w)} = \{\alpha(e)\}$, showing that $\alpha(e) = (\alpha'(v), \alpha'(w))$, and thus that α' is a point-automorphism of G. It is readily verified that the correspondence $\alpha \text{ <-> } \alpha'$ is a bijection of $A(\underline{M}(\underline{A}))$ onto $A_p(G)$ and is a group isomorphism.

This matroid is again non-binary. $\underline{A}$ is minimal, for suppose $e = (v, w) \in E$ and let Y be the edge set of any circuit of $G - v$

through w. Then e can not be removed from A_v, otherwise $Y \cup \{e\}$ becomes dependent. Consequently, by Theorem 1.22, each set A_v is a cocircuit and by taking a circuit $C = X \cup \{e\}$ as in the first part of the proof we have $|C \cap A_v| = 3$.

Corollary 10 For any group H, there exists a 2-partition geometry $\underline{M}$ with $A(\underline{M}) \cong H$.

Proof The 3-truncation $\underline{M}$ of the geometry constructed in Theorem 7 is a 2-partition geometry. It has non-trivial hyperplanes $\{u, (u, v), v\}$ where $(u, v) \in E$, and is readily verified to have automorphism group isomorphic to H.

Since a binary geometry of rank 3 can have at most seven elements, if we choose $|V \cup E| > 7$ then $\underline{M}$ will be non-binary and hence non-graphic. Also, since by a result of Mason [21, 22] a rank 3 transversal geometry can have at most three 3-element circuits, $\underline{M}$ will also be non-transversal if $|E| > 3$.

Transitive automorphism groups.

We now examine some specific finite groups, and consider whether or not they are the automorphism group of any matroid. We first prove the trivial

Lemma 11 For any matroid $\underline{M}$, $A(\underline{M}) = A(\underline{M}^*)$

Proof For $\alpha \in A(\underline{M})$ if and only if α maps bases onto bases. But if B is a base of $\underline{M}$ and $\alpha(B)$ is a base of $\underline{M}$, then $\alpha(S - B) = S - \alpha(B)$ is a cobase of $\underline{M}$. Thus α maps cobases onto cobases, and $\alpha \in A(\underline{M}^*)$.

Let T be an n-element set. The group of all permutations of T is called the symmetric group, and we denote it by S_n. The group of even permutations of T is called the alternating group, and is denoted by A_n.

Theorem 12 Let $\underline{M}$ be a matroid on the n-element set T. Then $A(\underline{M}) = S_n$ if and only if $\underline{M}$ is r-uniform for some r.

Proof Suppose $A(\underline{M}) = S_n$ and let B be a base of $\underline{M}$ with $|B| = r$. Let A be any other subset of T with $|A| = r$. Then we can find a permutation of T mapping B onto A. Thus A is a base of $\underline{M}$ and $\underline{M}$ is r-uniform. The converse is equally trivial.

Theorem 13 An independence structure $\underline{M}$ on an infinite set T has the full permutation group of T as its automorphism group if and only if (a) $\underline{M}$ is r-uniform for some finite $r = r(\underline{M})$, or (b) $\underline{M}$ consists of all subsets of T.

Proof For either $r(\underline{M})$ is finite or every finite subset of T is independent.

Theorem 14 Let T be an n-element set with $n > 2$. Then for no matroid $\underline{M}$ on T do we have $A(\underline{M}) = A_n$.

Proof Since $n > 2$ and $A(\underline{M}) = A(\underline{M}^*)$, either $r(\underline{M}) < n - 1$ or $r(\underline{M}^*) < n - 1$ for any matroid $\underline{M}$ on T. We assume that $r = r(\underline{M}) < n - 1$. But A_n is $(n - 2)$-transitive and, as in Theorem 12, if $A_n \subseteq A(\underline{M})$ then $A(\underline{M}) = S_n$.

For a further discussion of transitive groups and matroids, see Welsh [40].

Cyclic matroids

Let $\underline{M}$ be a matroid on the n-element set $T = \{1, 2, \ldots, n\}$. We call $\underline{M}$ cyclic if $A(\underline{M})$ is generated by the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix}.$$

Kagno [18] and Harary and Palmer [12] showed that there exists no graph G on an n-element set V with $A_p(G)$ generated by a cyclic permutation of V. For $n \geq 3$. This does not obviously imply that other than in the trivial cases it is impossible to find a graph G with $\underline{M}(G)$ cyclic, though this result must surely be true. However, it lead Ingleton to conjecture that cyclic matroids other than the trivial ones on one or two-element sets did not exist. In the remainder of this chapter we shall demonstrate the existence of cyclic matroids for almost all values of n, and the existence of cyclic transversal matroids for an infinite number of values of n.

Lemma 15 There is no cyclic matroid on a set T for $2 < |T| < 8$.

There is no cyclic matroid of rank 3 on a set T with $|T| = 8$.

Proof Since $A(\underline{M}) = A(\underline{M}^*)$ and no matroid of rank less than three on T when $|T| > 2$ can be cyclic, we know that if $2 < |T| < 6$ the result must be true. Also if $\underline{M}$ is of rank three on T and $|T| = 6$, it is easily seen that $\underline{M}$ does not admit a cyclic permutation of T unless $\underline{M}$ is 3-uniform, when $A(\underline{M}) = S_6$. This fact is seen by considering the effect of a cyclic permutation on a non-trivial hyperplane of $\underline{M}$ if such is assumed to exist.

Suppose $T = \{1, 2, \ldots, 7\}$, $\underline{M}$ is of rank 3 on T and $A(\underline{M})$ includes

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}.$$

No two non-trivial lines of $\underline{M}$ can intersect in more than a single element. However, if $L = \{k_1, \ldots, k_s\}$ is a non-trivial line of $\underline{M}$ then we must have the numbers $k_i - k_j$ $(i, j = 1, \ldots, s, i \neq j)$ distinct mod 7. The only possibility up to isomorphism is that $\underline{M}$ includes only the lines $L = \{1, 2, 4\}$, $\alpha L, \ldots, \alpha^6 L$. But then $\beta \in A(\underline{M})$, where

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 7 & 5 & 6 & 4 \end{pmatrix}$$

and $\underline{M}$ is not cyclic.

Similarly if $T = \{1, 2, \ldots, 8\}$ and $\underline{M}$ is cyclic and of rank 3 on T then either $\underline{M}$ has non-trivial lines $L = \{1, 2, 4\}, \alpha L, \ldots, \alpha^7 L$ up to isomorphism, and $\beta \in A(\underline{M})$, where

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 2 & 8 & 5 & 7 & 6 & 4 \end{pmatrix}$$

or $\underline{M}$ contains only lines L such that $L, \alpha L, \ldots, \alpha^7 L$ are not all distinct. But then $\beta' \in A(\underline{M})$ where

$$\beta' = \begin{pmatrix} 1 & 5 \\ 5 & 1 \end{pmatrix}.$$

Theorem 16 Let T be a set with $|T| \geqslant 8$. There exists a cyclic matroid on T.

Proof a) $T = \{1, \ldots, 8\}$. Put

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix}$$

and let $\underline{M}$ be the rank 4 partition geometry with non-trivial hyperplanes $H = \{1, 2, 3, 5\}, \alpha H, \ldots, \alpha^7 H$. We show that if $\beta \in A(\underline{M})$ and $\beta(1) = 1$ then β is the identity permutation. Call $H, \alpha H, \ldots \alpha^7 H$ $a, \ldots, h$ respectively. The only hyperplanes containing 1 are a, e, g and h, so β must permute these. Since 4 and 6 are in only one of these hyperplanes, whilst the other elements except 1 are in two of them, β must permute 4 and 6.

Case (i) $\beta(4) = 4$, $\beta(6) = 6$. Since $\beta(e) = e$, either $\beta(5) = 5$ or $\beta(5) = 7$.

In the first case it is readily verified that β is the identity permutation. If $\beta(5) = 7$ and $\beta(7) = 5$ then $\beta(3) = 3$ (c), $\beta(2) = 8$ (a,g), $\beta(8) = 2$. But then $\beta(b) = \{8, 3, 4, 6\}$, a contradiction.

Case (ii) $\beta(6) = 4$, $\beta(4) = 6$. Then $\beta\{5, 7\} = \{2, 8\}$ and $\beta\{2, 8\} = \{5, 7\}$ since $\beta(e) = h$. But then β must permute a and g and thus $\beta(3) = 3$. Hence $\beta(2) = 2$ (b) a contradiction.

b) $T = \{1, \ldots, n\}$, $n > 8$. Let $\underline{M}$ be the 2-partition geometry on $\underline{T}$ with lines $L = \{1, 2, 4\}$ αL, ... $\alpha^{n-1}(L)$, where

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix}.$$

Suppose $\beta \in A(\underline{M})$ and $\beta(1) = 1$. We shall show that β is the identity permutation. Since

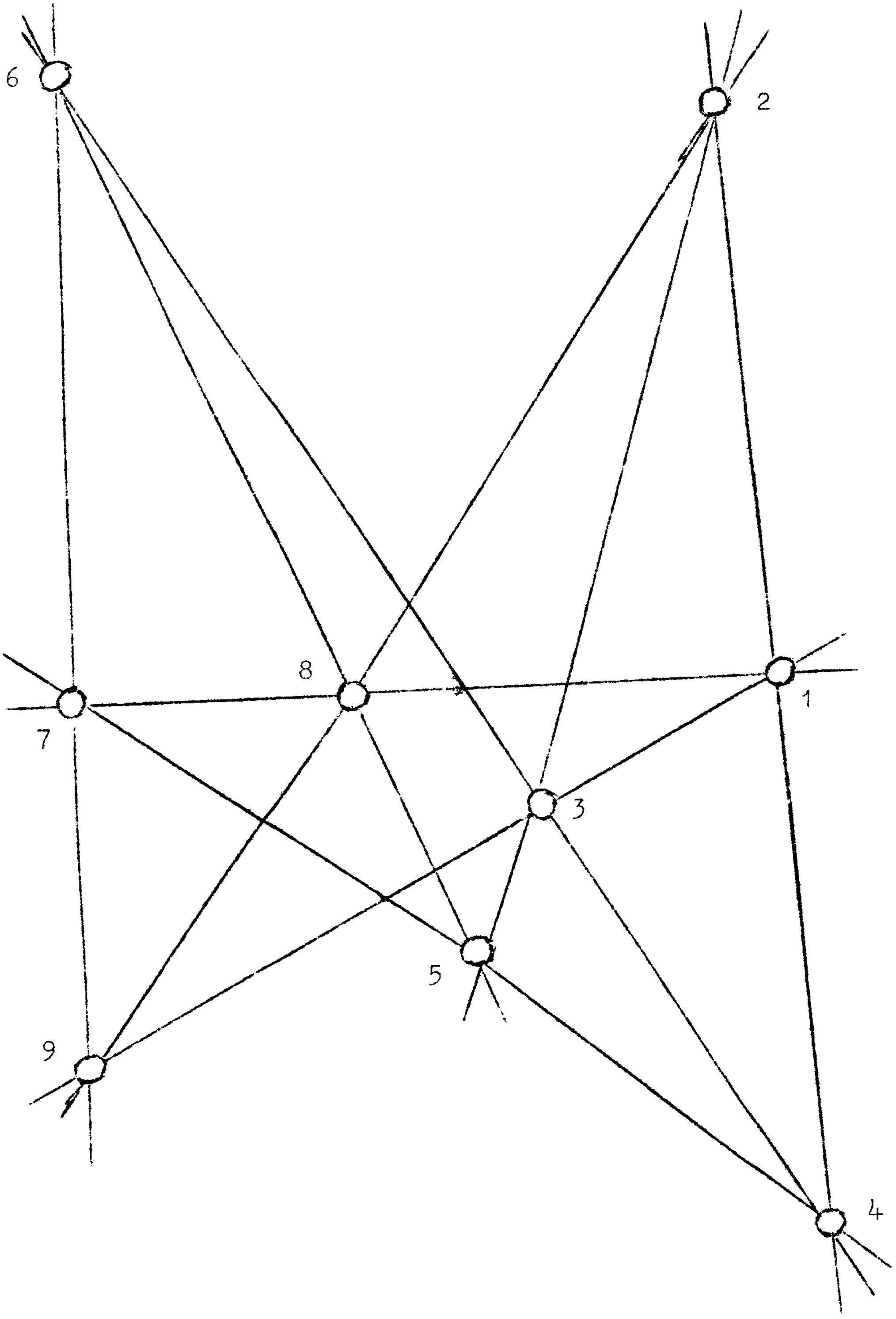
$$\{n - 2, n - 1, 1\}, \{n, 1, 3\}, \{1, 2, 4\}$$

are the only lines of $\underline{M}$ containing 1, β must permute them. Putting $S = \{n - 2, n - 1, n, 1, 2, 3, 4\}$, it follows that $\beta(S) = S$.

In the case $n = 9$ we have $\beta(\{5, 6\}) = \{5, 6\}$ and hence $\beta(8) = 8$. However, for the same reason, $\beta(6) = 6$, $\beta(4) = 4$, etc, and it follows that β is the identity.

If $n > 9$ then for any $s \in S$ put $g(s)$ equal to the number of lines of $\underline{M}$ which contain s and exactly one other element of S. Since S is invariant under β, therefore g must be invariant under β. However g only equals 2 for 3, so $\beta(3) = 3$. But then $\beta(1) = 1$ implies $\beta(n) = n$. The same argument gives $\beta(n - 1) = n - 1, \ldots, \beta(2) = 2$.

The cyclic matroid on nine elements is shown in the diagram.



All of the matroids constructed in Theorem 16 have too many hyperplanes to be transversal. We show that

Theorem 17 There exists no cyclic transversal matroid on a set T with $|T|$ a prime power greater than 2.

Proof For suppose $\underline{M} = \underline{M}(\underline{A})$ is a cyclic transversal matroid on the set $T = \{1, \ldots, n\}$ where $n = p^m$. Clearly $\underline{M}$ has no coloops, since $A(\underline{M})$ is transitive, and so we may take $\underline{A}$ to be the unique maximal presentation of $\underline{M}$. Suppose $\underline{A} = (A_1, \ldots, A_r)$ and suppose α is the generating permutation of $A(\underline{M})$, where

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots\ldots & n \\ 2 & 3 & \ldots\ldots & 1 \end{pmatrix}$$

Consider the sets A_1, $\alpha(A_1)$, $\alpha^2(A_1)$, $\ldots$. Let s be the smallest integer greater than zero such that $\alpha^s(A_1) = A_1$. Since $\alpha^n(A_1) = A_1$ we must have $s|n$, so $s = p^t$ for some $t \leqslant m$. If $t = m$ then $A_1, \alpha A_1, \ldots, \alpha^{n-1}A_1$ are distinct sets of $\underline{A}$, $r(\underline{M}) = n$ and we have a contradiction. Thus $t < m$ and $\alpha^{n/p}(A_1) = A_1$. Similarly $\alpha^{n/p}(A_i) = A_i$ for all $i = 1, \ldots, r$. But then $1 \in A_i$ if and only if $p^{m-1} + 1 \in A_i$ and $A(\underline{M})$ admits a transposition of 1 and $p^{m-1} + 1$, a contradiction.

We now show the existence of cyclic transversal matroids.

Theorem 18 There exist cyclic transversal matroids on a set T for infinitely many values of $|T|$.

Proof We show that there exists a cyclic transversal matroid on T whenever $|T| = m(m+1)$, where m is an integer and $m \geqslant 9$. Let $T = \{1, \ldots, m(m+1)\}$ and define the families $\underline{A} = (A_1, \ldots, A_m)$ and $\underline{B} = (B_1, \ldots, B_{m+1})$ by

$$A_i = \{a_{i,p,s} : 0 \leqslant p \leqslant m;\ s = 0, 1, 3; a_{i,p,s} \equiv i + pm + s \pmod{m(m+1)}\} \qquad (i = 1, \ldots, m)$$

$$B_j = \{b_{j,q,s} : 0 \leqslant q \leqslant m-1;\ s = 0,1,3; b_{j.q,s} \equiv j + q(m+1) + s \pmod{m(m+1)}\} \qquad (j = 1, \ldots, m+1).$$

Put $\underline{C} = \underline{A} \cup \underline{B}$. Clearly $\alpha \in A(\underline{M})$ where

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots\ldots & m(m+1) \\ 2 & 3 & \ldots\ldots & 1 \end{pmatrix}$$

since $\alpha(A_i) = A_{i+1}$ $(1 = 1, \ldots, m-1)$, $\alpha(A_m) = A_1$, $\alpha(B_j) = B_{j+1}$ $(j = 1, \ldots, m)$, $\alpha(B_{m+1}) = B_1$.

We no show that $\underline{C}$ is a maximal presentation of $\underline{M} = \underline{M}(\underline{C})$. (It is trivial that $\underline{M}$ has no coloops, so this statement makes sense.). Suppose $t \notin A_1$ for some $t \in T$. We shall show that there exists a transversal X of $(A_2, \ldots, A_m, B_1, \ldots, B_{m+1})$ disjoint from $A_1 \cup \{t\}$. But then t can not be added to A_1, since $X \cup \{t\}$ is not a transversal of $\underline{C}$. There exist at most two values of p such that $a_{i,p,s} = t$ for any i, s. Without loss of generality, we take these to be $p = 0, 1$, because of the symmetry implied by $\alpha \in A(\underline{M})$. Thus $a_{i,p,s} \neq t$ for $2 \leqslant p \leqslant m+1$. But we see that

$$X_1 = \{a_{2,2,3}, a_{3,2,3}, \ldots, a_{m-3,2,3}, a_{m-2,3,0}, a_{m-1,3,0}, a_{m,2,3}\}$$

$$= \{2m+5, 2m+6, \ldots, 3m, 4m-2, 4m-1, 3m+3\}$$

is a transversal of $(A_2, \ldots, A_m)$ disjoint from $A_1 \cup \{t\}$. We then observe that $X_1 \cup \{t\}$ is disjoint from the set $\{b_{j,q,s} : q = 4, 5\}$. For t can not have a value higher than $2m + 3$, and the largest value of elements of X_1 is $4m - 1$, whilst this set ranges from $4m + 5$ to $6m + 9$. Thus put

$$X_2 = \{b_{j,q,s} : j = 1, \ldots, m + 1; q = 4, s = 0 \text{ if } b_{i,4,0} \notin A_1, \text{ otherwise } q = 5, s = 3\}.$$

The elements above with $q = 4$ range from $4m + 5$ to $5m + 5$, whilst those with $q = 5$ range from $5m + 9$ to $6m + 9$. Thus all the elements are distinct and are disjoint from $X_1 \cup \{t\}$. Also if $b_{i,4,0} \in A_1$ then $b_{i,5,3} = b_{i,4,0} + m + 4 \notin A_1$, because $b_{i,4,0} + m \in A_1$ and no two elements of A_1 differ by 4. $X = X_1 \cup X_2$ is the desired transversal, and A_1 is maximal. By symmetry $A_2, \ldots, A_m$ are maximal.

A similar argument shows the maximality of B_1. Suppose $t \notin B_1$ and, with analogous reasoning, put

$$Y_1 = \{b_{2,2,3}, b_{3,2,3}, \ldots, b_{m-2,2,3}, b_{m-1,3,0}, b_{m,3,0}, b_{m+1,2,3}\}$$
$$= \{2m + 7, 2m + 8, \ldots, 3m + 3, 4m + 2, 4m + 3, 3m + 6\}$$

$Y_1 \cup \{t\}$ is disjoint from the set $\{a_{i,p,s} : p = 4, s = 3 \text{ or } p = 6, s = 1\}$ and is disjoint from B_1. Put

$$Y_2 = \{a_{i,p,s} : i = 1, \ldots, m; p = 4, s = 3 \text{ if } a_{i,4,3} \notin B_1, \text{ otherwise } p = 6, s = 1\}.$$

The elements of Y_2 are within the ranges $4m + 4$ to $5m + 3$ and $6m + 2$ to $7m + 1$, so the elements are all distinct. Also, if $a_{i,4,3} \in B_1$

then

$$\begin{aligned} a_{i,6,1} &= i + 6m + 1 \\ &= i + 4m + 3 + 2(m + 1) - 4 \\ &= a_{i,4,3} + 2(m + 1) - 4 \qquad (\mathrm{mod}\ m(m + 1)) \end{aligned}$$

which is not in B_1. Thus as before $B_1, \ldots, B_{m+1}$ are maximal.

Thus $A(\underline{M})$ is the set of permutations of T which permute $\underline{C}$, hence permute $\underline{A}$ and $\underline{B}$, since the sets of $\underline{A}$ and $\underline{B}$ have different cardinalities. Suppose $\beta \in A(\underline{M})$ and $\beta(1) = 1$. A pair $\{v,w\} \subset T$ is a subset of at least three subsets of $\underline{A}$ if and only if v and w are congruent modulo m. Since the property of pairs of being in a certain number of sets of $\underline{A}$ is preserved under β, it follows that β permutes the congruence classes modulo m of T. The action on these congruence classes is exactly the same as in the proof of Theorem 16 part b), and the congruence classes are consequently left invariant by β, hence

$$\beta(\{m, 2m, \ldots, (m+1)m\}) = \{m, 2m, \ldots, (m+1)m\}$$

Similarly

$$\beta(\{(m+1), 2(m+1), \ldots, m(m+1)\}) = \{(m+1), 2(m+1), \ldots, m(m+1)\}$$

implying that $\beta(m(m+1)) = m(m+1)$. Repetition of the argument gives $\beta(m(m+1) - 1) = m(m+1) - 1, \ldots, \beta(2) = 2$, and so β is the identity permutation.

The essential requirement of this proof is that $|T|$ should have two large enough coprime factors.

By taking the duals of Theorems 17 and 18, we get parallel results for strict gammoids.

5. ENUMERATION

The principal results of this chapter are a new lower bound for the number of non-isomorphic geometries on an n-element set, and a comparable upper bound. The lower bound improves upon previous bounds of Crapo [7], Welsh [38], and a conjecture of Crapo and Rota [8] that the number of non-isomorphic geometries was of the order of

$$k^{(3/2)^n} .$$

The upper bound is the first non-trivial upper bound, so far as the author knows.

Various other bounds for different classes of matroids are obtained, some of which improve upon existing bounds and are obtained less laboriously.

The number of matroids.

Theorem 1 below is essentially the result proved in [30].

Theorem 1 The number $f(n)$ of non-isomorphic geometries on an n-set satisfies

$$f(n) \geqslant (n^2/4)^{2^n n^{-5/2}} /n! \qquad (1 \leqslant n < \infty).$$

Theorem 1 is a corollary of

Theorem 2 The number $p(n)$ of non-isomorphic partition geometries on an n-element set satisfies

$$n^{h.2^n n^{-3/2}} \geqslant p(n) \geqslant (n^2/4)^{2^n n^{-5/2}} /n! \qquad (1 \leqslant n < \infty)$$

for some $h > 0$. Thus for n sufficiently large

$$n^{h.2^n n^{-3/2}} \geq p(n) \geq n^{2^n n^{-5/2}} .$$

Finally, our upper bound is given in

<u>Theorem 3</u>. The number $g(n)$ of non-isomorphic matroids on an n-set satisfies

$$g(n) \leq n^{k2^n n^{-1}} \qquad (2 \leq n < \infty)$$

for some $k > 0$.

Before proving Theorem 2 we need a Lemma on partition geometries, and also a Lemma of a technical nature.

<u>Lemma 4</u> Let $\underline{H} = \{H_i : i \in I\}$ be a clutter of subsets of a set S such that for some $k > 1$

$$\min_{i \in I} |H_i| > k > \max_{i,j \in I} |H_i \cap H_j|$$

Then we may take $\underline{H}$ to be the set of non-trivial hyperplanes of a k-partition geometry.

<u>Proof</u> Under the given assumptions, any k-subset of S is a subset of at most one member of $\underline{H}$. We augment $\underline{H}$ by adding to it all k-subsets of S which are subsets of no member of $\underline{H}$, and then clearly the augmented collection forms the collection of hyperplanes of a k-partition geometry.

<u>Lemma 5</u> If N and N/p are integers and $N > p > 1$ then

$$ {}_N C_{N/p} < (4p)^{N/p}. $$

<u>Proof</u> We have

$$ {}_N C_{N/p} = \frac{N!}{(N - N/p)!\,(N/p)!} . $$

By Stirling's Theorem, for all $m > 0$,

$$ \sqrt{2\Pi}\ m^{m+\frac{1}{2}}\, e^{-m} < m! < \sqrt{2\Pi}\ m^{m+\frac{1}{2}}\, e^{1/12\ -m}, $$

thus

$$ {}_N C_{N/p} < \frac{\sqrt{2\Pi}.\ N^{N+\frac{1}{2}}.\ e^{1/12\ -N}}{2\Pi\ (N/p)^{N/p+\frac{1}{2}}\, e^{-N/p} (N - N/p)^{N-N/p+\frac{1}{2}} e^{-N+N/p}} $$

$$ = \frac{e^{1/12}}{\sqrt{2\Pi}} \cdot \left(\frac{p}{N}\right)^{\frac{1}{2}} \cdot \frac{p^{N/p}}{(1 - 1/p)^{N-N/p+\frac{1}{2}}} . $$

But we know that

$$ \lim_{p \to \infty} (1 - 1/p)^{-p} = e, $$

the sequence being monotonic. Thus

$$ (1 - 1/p)^{-p} < 4 \qquad (p > 1) $$

and

$$ {}_N C_{N/p} < p^{N/p} \{(1 - 1/p)^{-p}\}^{N/p - N/p^2 + 1/2p} $$
$$ < (4p)^{N/p}.\ 4^{-N/p^2 + 1/2p} . $$

However,

$$ 4^{-N/p^2 + 1/2p} = 4^{-(2N - p)/2p^2} < 1 $$

and the result follows.

Proof of Theorem 2. We choose families of sets $\underline{H} = (H_1, H_2, \ldots, H_p)$, where $p > 1$ is an as yet unspecified integer, and, for some $t > 1$, and for all i, j with $1 \leqslant i, j \leqslant p$,

$$|H_i| = t, \quad |H_i \cap H_j| < t - 1.$$

The number of ways of choosing H_1 is clearly ${}_nC_t$. Given H_1, the number of t-subsets of S intersecting H_1 in more than $t - 2$ elements is seen to be

$$a = t(n - t) + 1.$$

Thus, if ${}_nC_t > a$ we may choose H_2 in $({}_nC_t - a)$ ways. H_1 and H_2 together exclude at most $2a$ choices for H_3, so if ${}_nC_t > 2a$ we may choose H_3 in at least $({}_nC_t - 2a)$ ways. Continuing, provided ${}_nC_t > (p - 1)a$ we may choose H_p in at least $({}_nC_t - (p - 1)a)$ ways.

We now impose the condition that

$$p \leqslant {}_nC_t / a$$

and then the number of permissible families is at least

$${}_nC_t \cdot ({}_nC_t - a) \ldots ({}_nC_t - (p - 1)a).$$

Now the ranges of two such distinct familes $\underline{H}$ and $\underline{H}'$ will be identical if and only if, for some permutation α of $\{1, 2, \ldots, n\}$, $H_i = H'_{\alpha(i)}$ $(i = 1, \ldots, n)$. Thus the number of differnet ranges is at least

$$\begin{aligned} &{}_nC_t \cdot ({}_nC_t - a) \ldots ({}_nC_t - (p - 1)a)/p! \\ \geqslant\ & pa \cdot (p - 1)a \ \ldots \ a / p\,! \\ =\ & a^p. \end{aligned}$$

But unequal ranges give rise to different geometries, which may possibly be isomorphic. However, the equivalence classes of geometries under isomorphism have size at most $n!$, consequently $p(n) \geqslant a^p/n!$ We choose t and p so as to maximize this expression. Put

$$t = [n/2] \quad , \quad p = [{}_nC_{[n/2]}/a]$$

so that

$$a = [n^2/4] + 1.$$

From Stirling's Theorem, we know that, if n is even,

$$ {}_nC_{n/2} = \frac{n!}{(n/2)!(n/2)!}$$

$$> \frac{\sqrt{2\Pi}}{2\Pi} \cdot \frac{n^{n+\frac{1}{2}}\, e^{-n}}{\{(n/2)^{n/2+1/2}\}^2\{e^{-n/2}\}^2\{e^{1/6n}\}^2}$$

$$= \frac{1}{\sqrt{2\Pi}} \qquad \frac{n^{n+1/2}e^{-1/3n}}{(r/2)^{n+1}} = \frac{1}{\sqrt{2\Pi}} \cdot 2^{n+1}.n^{-1/2}. e^{-1/3n}$$

and if n is odd,

$${}_nC_{[n/2]} = \frac{n}{(n-1)/2} \cdot {}_{n-1}C_{(n-1)/2}$$

$$> \frac{2n}{n-1} \cdot \frac{1}{\sqrt{2\Pi}} \cdot 2^n(n-1)^{-1/2}. e^{-1/3(n-1)}$$

$$> \frac{1}{\sqrt{2\Pi}} \cdot 2^{n+1}. n^{-1/2}. e^{-1/3(n-1)}.$$

In either case

$${}_nC_{[n/2]} > \frac{1}{\sqrt{2\,\Pi}} \; 2^{n+1}. n^{-1/2}. e^{-1/3(n-1)}$$

and consequently

$$p > \frac{1}{\sqrt{2\Pi}} \frac{2^{n+1} n^{-1/2} e^{-1/3(n - 1)}}{n^2/4 + 1} - 1$$

$$= \frac{8e^{-1/3(n - 1)}}{\sqrt{2\Pi}(1 + 4/n^2)} \cdot 2^n n^{-5/2} - 1$$

$$> 2^n n^{-5/2}$$

if $n > 2$, say. But

$$p(n) \geqslant a^p/n\,! > (n^2/4)^p / n\,!$$

and the lower bound follows by the above after checking the cases $n = 1$ and $n = 2$.

The weaker lower bound is obtained readily from this bound, its only advantage being its neater form.

To obtain the given upper bound, we observe that if $\underline{M}$ is a k-partition matroid on S, then each non-trivial hyperplane of $\underline{M}$ has at least $(k + 1)$ k-subsets. Since each k-subset of $\underline{M}$ occurs in at most one of the non-trivial hyperplanes, it follows that the number of the latter can be at most ${}_nC_k/(k + 1)$. Putting $N = {}_nC_k$, $p = k + 1$, we see that the number of ways of choosing the non-trivial hyperplanes is at most

$$\sum_{r=0}^{N/p} {}_N C_r < (N/p + 1)\,{}_NC_{N/p}$$

$$< (N/p + 1)(4p)^{N/p} \quad \text{(by Lemma 5)}$$

$$< n^{d \cdot {}_{n+1}C_{k+1} \cdot n^{-1}} / n$$

for some $d > 0$, since $N/p = {}_{n+1}C_{k+1} / n$. The maximum of the last expression occurs when $k + 1 = [(n + 1)/2]$ and, summing over k and using Stirling's Theorem we obtain an overall bound of

$$n^{d \cdot {}_{n+1}C_{[(n+1)/2]} \cdot n^{-1}} < n^{h \cdot 2^n n^{-3/2}}$$

for some $h > 0$.

Before proving Theorem 3 we need a further Lemma.

Lemma 6 Let $\underline{M}$ be a matroid of rank r on an n-set S, Put

$$K_i = \{\bar{C} : C \text{ is a circuit of } \underline{M}, |C| = i + 1\}$$

$$(i = 0, 1, \ldots, r).$$

Then $\underline{M}$ is determined uniquely by the family $\underline{K} = (K_i)$.

Proof Suppose we are given $\underline{K}$. If $\bar{C} \in K_i$ and $X \subseteq \bar{C}$ with $|X| = i + 1$, then X is dependent. It follows that we may recover the circuits of $\underline{M}$ from $\underline{K}$ by taking the minimal sets X such that $|X| = i + 1$ and $X \subseteq \bar{C} \in K_i$ for some i.

Proof of Theorem 3. Let $\underline{M}$ be a matroid on the n-set S, and let $\bar{C}_{i,1}, \ldots, \bar{C}_{i,r_i}$ be the distinct members of K_i. We note that $|C_{i,j} \cap C_{i,k}| < i$ if $j \neq k$. Since each $C_{i,j}$ has $(i + 1)$ i-subsets for each j, we must have

$$(i + 1)r_i \leq {}_nC_i$$

$$r_i \leq {}_{n+1}C_{i+1} /(n + 1).$$

Thus our problem is first to find an upper bound for the number of different families $\underline{T} = (T_i : i = 0, 1, \ldots, [n/2])$, where each T_i is a set of subsets of S, with

$$|T_i| \leqslant {}_{n+1}C_{i+1}/(n + 1) = q_i .$$

Putting $N = 2^n$, the number of ways of choosing T_i is

$$\sum_{j=0}^{q_i} {}_NC_j < (q_i + 1)\, {}_NC_{q_i} .$$

$$< N.\, {}_NC_{q_i} .$$

Putting $p_i = N/q_i$ and using Lemma 5 we have

$${}_NC_{q_i} < (4p_i)^{q_i}$$

so the number of different families $\underline{T}$ is at most

$$\prod_{i=0}^{[n/2]} N.\, {}_NC_{q_i} < 2^{n^2} . \prod_{i=0}^{[n/2]} {}_NC_{q_i} .$$

We split this product into two parts according as $p_i \gtrless n^4$.

$$\prod_{p_i \geqslant n^4} {}_NC_{q_i} \leqslant \prod_{p_i \geqslant n^4} (2^n)^{2^n/n^4} < 2^{2^n/n^2}$$

$$\prod_{p_i < n^4} {}_NC_{q_i} < \prod_{p_i < n^4} (4n^4)^{\,q_i}$$

$$< (4n^4)^{\sum_{p_i < n^4} q_i}$$

$$< (4n^4)^{2^n/(n+1)} .$$

Thus the whole product is less than

$$2^{n^2} . \; 2^{2^n/n^2} . \; (4n^4)^{2^{m+1}/(n+1)}$$

$$< \frac{1}{2} . \; n^{k.2^n/n}$$

for large enough n and for $k > 4$. The result then follows by considering $\underline{M}$ or $\underline{M}^*$ according as $r(\underline{M}) \lessgtr [n/2]$.

Theorem 3 gives a better bound than may be obtained by simply using the fact that a matroid is determined by its bases. The latter gives an easy bound of

$$(n + 1). \; 2^{{}^nC_{[n/2]}} < 2^{2^n n^{-1/2}}$$

The number of representable matroids

Theorem 7 The number $R_d(n)$ of non-isomorphic matroids on an n-set S which are representable over a finite field F with $|F| = d$ satisfies

$$k_1 . \; 2^{n^2/4} / n! < R_d(n) < k_2 . \; d^{n^2/4}$$

for some $k_1, k_2 > 0$.

We note that the lower bound is independent of d. The proof uses the following

Lemma 8 If $d > 1$, and n is a positive integer, then

$$d^{(n^2-1)/4} < \sum_{r=0}^{n} d^{\,r(n-r)} < (\sqrt{(\Pi/\log_e d)} + 1)d^{n^2/4}.$$

Proof The left hand inequality follows from putting $r = (n-1)/2$ or $r = n/2$ according as n is odd or even.

For the other inequality, we have

$$\sum_{r=0}^{n} d^{r(n-r)} = d^{n^2/4}. \sum_{r=0}^{n} d^{-(r-n/2)^2}$$
$$= d^{n^2/4}. B,$$

and we compare B with the area $A = \sqrt{(\Pi/\log_e d)}$ under the curve $y = d^{-x^2}$.

If n is even then

$$B = \sum_{r=-n/2}^{n/2} d^{-r^2}$$

$$= \sum_{r=-n/2}^{-1} d^{-r^2} + \sum_{r=0}^{n/2-1} d^{-(r+1)^2} + 1$$

$$< A + 1$$

and if n is odd we have, taking the sums over integer steps,

$$B = \sum_{r=-n/2}^{n/2} d^{-r^2} = \sum_{r=-n/2}^{-1/2} d^{-r^2} + \sum_{r=-1/2}^{n/2-1} d^{-(r+1)^2} + d^{-1/4}$$

$$< A + 1.$$

Proof of Theorem 7 We first obtain the upper bound. We restrict our attention first of all to matroids of a fixed rank r, and it is sufficient only to consider matroids which have a fixed common base $\{s_1, \ldots, s_r\} \subseteq S$

and representations $f: S \to V_r(F)$ in a fixed vector space $V_r(F)$ such that $f(s_i) = \underline{e}_i$ $(i = 1, \ldots, r)$, $\{\underline{e}_1, \ldots, \underline{e}_r\}$ being a fixed basis of $V_r(F)$. Suppose $\underline{M}_1$ and $\underline{M}_2$ are different matroids with representations f_1 and f_2. Clearly $f_1 \neq f_2$. However any representation is determined by a choice of $r(n - r)$ elements of F, namely the coordinates of $f(s_i)$ $(i = r + 1, \ldots, n)$ with respect to $\{\underline{e}_1, \ldots, \underline{e}_r\}$. Consequently, the number of non-isomorphic matroids cannot be greater than $d^{r(n - r)}$. Summing over r and applying Lemma 8 we obtain a bound $k_2 \cdot d^{n^2/4}$ with $k_2 = \sqrt{(\Pi/\log_e 2)} + 1$.

Secondly, we prove the lower bound. With $V_r(F)$ and $\{e_1, \ldots, e_r\}$ as above, let $\underline{U} = (U_{r+1}, \ldots, U_n)$ be a family of subsets of $I = \{1, 2, \ldots, r\}$. For $U_k \subseteq I$ put

$$\underline{e}_k = \sum_{i \in U_k} \underline{e}_i .$$

Then any family $\underline{U}$ determines a matroid on the set $S = \{s_1, \ldots, s_n\}$ intrinsically through the representation $s_k \to \underline{e}_k$ $(k = 1, \ldots, n)$.

Different families $\underline{U}$ give rise to non-equal matroids, since the set U_k determines the fundamental circuit of s_k with respect to $\{s_1, \ldots, s_r\}$. Thus we have $2^{r(n - r)}$ non-equal representable matroids of rank r, which must contain at least $2^{r(n - r)}/n!$ non-isomorphic matroids. Summing over r and applying Lemma 8 we obtain a bound $k_1 \cdot 2^{n^2/4} / n!$ with $k_1 = 2^{-1/4}$.

We observe that our lower bound is better than that obtained by Bollobas, because of the insignificance of the $n!$ term compared with $2^{n^2/4}$.

Also, with $d = 2$, the two bounds are roughly comparable. A general lower bound of the order of $d^{n^2/4}$ would appear to be difficult to obtain.

The number of transversal matroids.

Theorem 9 The number $w(n)$ of non-isomorphic fundamental transversal matroids on an n-set S satisfies

$$k_1 \cdot 2^{n^2/4} / n! < w(n) < k_2 \cdot 2^{n^2/4}$$

for some $k_1, k_2 > 0$.

Proof Let $\underline{A} = (A_i : i = 1, \ldots, r)$ be a family of subsets of $S = \{s_1, \ldots s_n\}$, where $r \leqslant n$, and $A_i = \{s_i\} \cup B_i$ $(i = 1, \ldots, r)$, with $B_i \subseteq S_1 = \{s_{r+1}, \ldots, s_n\}$. For fixed r, if $\underline{A}$ and $\underline{A}'$ are different families, then $\underline{M}(\underline{A}) \neq \underline{M}(\underline{A}')$. Thus, since the number of distinct families $\underline{A}$ for fixed r is $2^{r(n - r)}$, the number of distinct fundamental transversal matroids of rank r is at least $2^{r(n - r)}/n!$ Summing over r and applying Lemma 8, we obtain the desired lower bound. The upper bound is obtained directly as an upper bound for the number of families $\underline{A}$.

Theorem 9 gives a lower bound for the number $t(n)$ of non-isomorphic transversal matroids. A. P. Heron has obtained an upper bound $2^{2n^2/3}$ for $t(n)$.

The bound in Theorem 9 is also a lower bound for the number of strict gammoids, by duality.

REFERENCES

1 J. E. Blackburn, H. Crapo and D. A. Higgs, A catalogue of combinatorial geometries, Univ. Waterloo (1969), (unpublished).

2 B. Bollobas, A lower bound for the number of non-isomorphic matroids, J. Comb. Th. 7 (1969), 366 - 8.

3 J. A. Bondy, Transversal matroids, base-orderable matroids and graphs, (to appear).

4 J. A. Bondy and D. J. A. Welsh, Some results on transversal matroids and constructions of identically self-dual matroids, Quart. J. Math. Oxford (2) 22 (1971), 435 - 51.

5 R. A. Brualdi, Admissible mappings between dependence structures, (to appear).

6 R. A. Brualdi and E. B. Scringer, Exchange systems, matchings and transversals, (to appear).

7 H. H. Crapo, Single element extensions of matroids, J. Res. N. B. S. 69B (1965), 55 - 65.

8 H. H. Crapo and G-C. Rota, Combinatorial geometries, M.I.T. Press, (1971).

9 J. Edmonds, Systems of distinct representatives and linear algebra, J. Res. N. B. S. 71B (1965), 241 - 5.

10 R. Frucht, Herstellung von Graphen mit vorgegebener abstrakten Gruppe, Compositio Math. 6 (1938), 239 - 50.

11 F. Harary, Graph Theory, Addison-Wesley (1969).

12 F. Harary and E. M. Palmer, The groups of the small digraphs. J. Indian Statist. Assoc. 4(1966), 155 - 169.

13 F. Harary, M. J. Piff and D. J. A. Welsh, On the automorphism group of a matroid, J. Disc. Math. (to appear).

14 F. Harary and D. Welsh, "Matroids versus graphs", The many facets of graph theory, Springer-Verlag (1969), 155 - 170.

15 A. P. Heron, Transversal matroids, Dissertation, Oxf. Univ (1969).

16 A. W. Ingleton, Representation of matroids, Combinatorial Mathematics and its applications, Ac. Press, (1971).

17 A. W. Ingleton and M. J. Piff, Gammoids and transversal matroids, (to appear).

18 I. N. Kagno, Linear graphs of degree ≤ 6 and their groups, A. J. M. 68 (1946), 505 - 20; 69 (1947), 872; 77 (1955), 392.

19 S. Lang, Algebra, Addison-Wesley (1965).

20 T. Lazarson, The representation problem for independence functions, J. L. M. S. 33 (1958), 21 - 5.

21 J. H. Mason, Representations of independence spaces, Ph.D. Thesis, Univ. Wisconsin, (1969).

22 J. H. Mason, A characterization of transversal independence spaces Théorie des Matroides, ed. C. P. Bruter, Springer (1971), 86 - 94.

23 J. H. Mason, On a class of matroids arising from graphs, Proc. L.M.S. (3), (to appear).

24 G. J. Minty, On the axiomatic foundations of the theories of directed linear graphs, etc, J. Math. Mech. 15 (1966), 485 - 520.

25 L. Mirsky and H. Perfect, Applications of the notion of independence to problems of combinatorial analysis, J. Comb. Th. 2 (1967), 327 - 57.

26 H. Perfect, Applications of Menger's graph theorem, J. Math. Anal. Applic. 22 (1968), 96 - 110.

27 M. J. Piff, The representability of matroids, Dissertation. Oxf. Univ., (1969).

28 M. J. Piff, Properties of finite character of independence spaces, Mathematika, 18 (1971), 201 - 8.

29 M. J. Piff and D. J. A. Welsh, On the vector representation of matroids, J. L. M.S. (2) 2 (1970), 284 - 8.

30 M. J. Piff and D. J. A. Welsh, On the number of combinatorial geometries, Bull. L. M. S. 3 (1971), 55 - 6.

31 J. S. Pym, A proof of the linkage theorem, J. Math. Anal. Applic. 27 (1969), 636 - 8.

32 R. Rado, Axiomatic treatment of rank in infinite sets, Can. J. Math. 1 (1949), 337 - 43.

33 R. Rado, Note on independence functions, Proc. L. M. S. (3) 7 (1957), 306 - 20.

34 G. Sabidussi, Graphs with given group and given graph-theoretical properties, Can. J. M. 9 (1957), 515 - 25.

35 G. Sabidussi, Graphs with given infinite group, Mon. Math. 64 (1960), 64 - 7.

36 W. T. Tutte, Lectures on matroids, J. Res. N. B. S., 69B (1965), 1 - 47.

37 P. Vamos, A necessary and sufficient condition for a matroid to be linear, (to appear).

38 D. J. A. Welsh, A bound for the number of matroids, J. Comb. Th. 6 (1969), 313 - 16.

39 D. J. A. Welsh, On matroid theorems of Edmonds and Rado, J. L. M. S. (2) 2 (1970), 251 - 6.

40 D. J. A. Welsh, Matroids and block designs, Théorie des matroides, ed. C. P. Bruter, Springer (1971), 95 - 105.

41 H. Whitney, Congruent graphs and the connectivity of graphs, A. J. M. 54 (1932), 150 - 68.

42 H. Whitney, On the abstract properties of linear dependence, A. J. M. 57 (1935), 509 - 33.

ERRATA

8.9	... $X \neq \emptyset \}$
9.10	co-dependent
14.4	Brualdi and Scringer [6] or Heron [15].
14.13	$\underline{A} = (A_v : v \in V)$
15.8	... for some k ...
45	The obvious generalization of Theorem 2 to GF(3), namely, that $\underline{M}$ is ternary if and only if it does not contain as a minor the smallest non-ternary matroid, is false.
46.-1	... disjoint (possibly vacuous) union ...
50.12	We are here defining the term 'sufficiently large'. We have restricted it to mean 'but finite'. See, however, p.53.
50.18	the subspaces of V ...
51.8	sufficiently
52.7	transversal
52.8	... sufficiently large field.
56.7	algebraic
65.4	a transversal geometry which is not fundamental
68.13	permutation of V for $n \geq 3$.
83.8	The bar denotes closure, of course!
83.-4	$\lvert C_{i,j} \cap C_{i,k} \rvert < i$ follows from the fact that otherwise $C_{i,j}$ and $C_{i,k}$ would have the same closure.
87.-8	'Different' and 'non-equal' mean 'non-identical'.