MATROID THEORY

D. J. A. Welsh

MATROID THEORY

D. J. A. WELSH
Merton College
and
The Mathematical Institute,
University of Oxford

1976

ACADEMIC PRESS
LONDON NEW YORK SAN FRANCISCO
A Subsidiary of Harcourt Brace Jovanovich, Publishers

ACADEMIC PRESS INC. (LONDON) LTD.
24/28 Oval Road,
London NW1

United States Edition published by
ACADEMIC PRESS INC.
111 Fifth Avenue
New York, New York 10003

Library of Congress Catalog Card Number: 76–10493
ISBN: 0 12 744050 X

PRINTED IN GREAT BRITAIN BY
PAGE BROS (NORWICH) LTD, NORWICH

Preface

This book is an attempt to show the unifying and central role which matroids have played in combinatorial theory over the past decade. This is not to say that all aspects of combinatorial theory can be covered by the matroid umbrella; however, many parts of graph theory, transversal theory, block designs and combinatorial lattice theory can be more clearly understood by the use of matroids. Furthermore, since matroids are closely related to classical linear algebra and geometry they serve as a link between combinatorics and the more mainstream areas of mathematics.

The first half of this book can be regarded as a basic introduction to matroid theory. Most theorems are proved or an exact reference is given. The second half is an attempt to place the reader at the frontier of the subject. At this level I have found it impossible to prove every result. However I have, I hope, treated in some detail the more central and important topics, others I have set as exercises. Those exercises which are followed by a reference to some paper will usually be non-routine.

I have lectured on most of this book at various universities; the first half is the core of a course on combinatorics that I have given to third year undergraduates at Oxford. The other chapters have been covered at various times in M.Sc. level courses at Oxford and Waterloo.

I take this opportunity to acknowledge a deep sense of gratitude to a number of friends who in different ways helped in the production of this book.

C. St. J. A. Nash-Williams first introduced me to the subject with a most stimulating seminar on the applications of matroids in 1966. I am also very grateful to him for making it possible for me to visit the University of Waterloo where an early draft of the first half was prepared. F. Harary encouraged me to write this book and enabled me to try out a very preliminary version at the University of Michigan, Ann Arbor. The bulk of the book in its present form was drafted in the very happy and stimulating atmosphere of the mathematics department of the University of Calgary. I am deeply grateful to the department there and in particular to E. C. Milner for his unfailing kindness and patience in listening to my problems and queries.

I began to make a list of the people who had helped me over the last seven years either in discussion or by correspondence—it came to almost half the names listed in the bibliography. However, I do need to say that special thanks are due to D. W. T. Bean, A. W. Ingleton, C. J. H. McDiarmid, L. R. Mathews and J. G. Oxley, each of whom read substantial parts of the manuscript and had many helpful discussions on various points that have arisen.

Finally I would like to thank Clare Bass, Sheila Robinson and my wife Bridget for their help in preparing the final manuscript.

Merton College
and
The Mathematical Institute, Oxford
July 1975

Dominic Welsh

Contents

Chapter 4. Submatroids

Chapter 5. Matroid Connection

Chapter 6. Matroids, Graphs and Planarity

Chapter 7. Transversal Theory

Chapter 8. Covering and Packing

Chapter 9. The Vector Representation of Matroids

Chapter 10. Binary Matroids

Chapter 11. Matroids from Fields and Groups

Chapter 12. Block Designs and Matroids

Chapter 13. Menger's Theorem and Linkings in Graphs

Chapter 14. Transversal Matroids and Related Topics

Preliminaries

1. BASIC NOTATION

A reference to "item k" refers to item k of the same section; ($j.k$) refers to the same chapter; ($i.j.k$) refers to item k of section j of chapter i.

A reference $[k]$ refers to item k of the bibliography. References are by author's name and the last two digits of the year of publication, with additional letters to distinguish publications of the same author in the same year.

There are exercises at the end of most sections; the open problems are marked $^\circ$.

2. SET THEORY NOTATION

Throughout we adopt the usual set theoretic conventions: set-union, set-intersection, set inclusion and proper inclusion are denoted by the familiar symbols $\cup$, $\cap$, $\subseteq$, $\subset$, respectively.

For the most part we shall be considering structures on a finite set S. Elements of S will be denoted by lower case italic letters and subsets of S by italic capital letters. The *empty* set is denoted by $\emptyset$; $A\backslash B$ denotes the *set difference* of A and B; $A \triangle B$ denotes the *symmetric difference* of A and B,

$$A \triangle B = (A\backslash B) \cup (B\backslash A).$$

Two sets A, B are *incomparable* if neither is a subset of the other. As usual $\{x_1, \ldots, x_k\}$ denotes the set with elements $x_1, \ldots, x_k$ and when it is clear from the context that we are referring to a set rather than an element we abbreviate $\{x\}$ to x. For example $X \cup x$ means $X \cup \{x\}$, $X\backslash x$ means $X\backslash\{x\}$.

$|A|$ denotes the *cardinality* of the set A, and we write X is a *k-set* (*k-subset*) if X is a set (subset) of cardinality k. Suppose that we have a set A_i for each i in a non-empty *indexing set* I. We use $A(I)$ to denote the union of the A_i; $i \in I$. That is

$$A(I) = \{x : x \in A_i \text{ for some } i \in I\}.$$

A *function* or *map* from S to T is denoted by $f: S \to T$. If x belongs to the domain of f, $f(x)$ is called the image of x, and for $A \subseteq S$, the image of A, denoted by $f(A) = \{y: y \in T, f(x) = y \text{ for some } y \in A\}$.
If U is a subset of S we denote the *restriction* of f to U by $f|_U$.

The *power set* 2^S of S is the collection of subsets of S and a map $\phi: S \to T$ defines in the obvious way a map

$$2^\phi: 2^S \to 2^T$$

where for $X \subseteq S$,

$$2^\phi X = \{y: y = \phi x \quad \text{for some} \quad x \in X\}.$$

As usual we normally write ϕX rather than $2^\phi X$.

If S and I are sets and $\phi: I \to S$ is a map with $\phi(i) = x_i$ for all $i \in I$ we will often denote this map ϕ by the symbol $(x_i: i \in I)$ and call it a *family* of elements of S *indexed* by I or with *index set I*. A family is thus a map not a set, though loosely speaking it can often be thought of as a collection of labelled objects of S. A subset X of S is a *maximal* (*minimal*) subset of S possessing a given property P if X possesses property P and no set properly containing X (contained in X) possesses P.

The set of integers is denoted by $\mathbb{Z}$. The set of real numbers by $\mathbb{R}$. The sets of non-negative integers and real numbers are denoted respectively by $\mathbb{Z}^+$ and $\mathbb{R}^+$.

3. ALGEBRAIC STRUCTURES

I shall assume familiarity with the basic algebraic structures such as a group, field, or vector space.

The finite field with q elements will be denoted by $GF(q)$ and I use $F(x_1, \ldots, x_n)$ to denote the minimal extension field of the field F generated by $x_1, \ldots, x_n$. $V_n(F)$ denotes the vector space of dimension n over the field F, $V_n(q)$ denotes the vector space of dimension n over the field $GF(q)$.

A typical element v of a vector space will be denoted by v or $(v_1, \ldots, v_n)$, where n is the dimension of the space. The zero vector is denoted by 0.

Now for any field F consider the vector space V of all vectors $(a_0, \ldots, a_n)$, $a_i \in F$. If u, v are two members of $V\backslash 0$ we write $u \sim v$ if there exists some non-zero member b of F such that $u = bv$. It is easy to check that $\sim$ is an equivalence relation on $V\backslash 0$. The equivalence classes under this relation are the points of the *projective geometry of dimension n* over F. When F is the finite field $GF(q)$ we denote this projective geometry by $PG(n, q)$.

For a further discussion of projective geometries we refer to Chapter 12 (where we study them in more detail), or to the recent book of Bumcrot [69].

Unless specified a vector will mean a row vector and if x is a vector, x' is its transpose and xy' will denote the *scalar product* of x and y. Similarly A' will denote the *transpose* of the matrix A.

4. GRAPH THEORY

We assume familiarity with the concepts of a *graph* and a directed or oriented graph which we call a *digraph*. We denote a graph G by a pair $(V(G), E(G))$ where $V = V(G)$ is the *vertex* set and $E = E(G)$ is the set of *edges*.

The edge $e = (u, v)$ is said to *join* the vertices u and v. If $e = (u, v)$ is an edge of G, then u and v are *adjacent* vertices while u and v are called the *endpoints* of the edge $e = (u, v)$. If two edges e_1, e_2 have a common endpoint they are said to be *incident*. We often denote the edge $e = (u, v)$ by uv or vu.

A *loop* of a graph is an edge of the type (x, x). Two edges are *parallel* if they have common endpoints and are not loops.

A graph is *simple* if it has no loops or parallel edges.

The *degree* of a vertex v is the number of edges having G as an endpoint, and is denoted by $\deg(v)$. A graph is *regular* if all its vertices have the same degree.

Two graphs G_1, G_2 are *isomorphic* if there is a bijection $\phi: V(G_1) \to V(G_2)$ such that if $u, v \in V(G)$ the number of edges joining u, v in G_1 equals the number of edges joining $\phi(u)$ and $\phi(v)$ in G_2.

A vertex u of G is an *isolated* vertex if $\deg(u) = 0$. An edge uv of G is a *pendant* edge if either u or v, but not both, has degree 1 in G.

If G is a graph with vertex set $\{v_1, \ldots, v_n\}$ the *adjacency matrix* of G corresponding to the given labelling of the vertex set is the $n \times n$ matrix $A = (a_{ij})$, in which a_{ij} is the number of edges of G joining v_i and v_j.

A *complete graph* is a simple graph in which an edge joins each pair of vertices. The complete graph on n vertices is denoted by K_n.

If the vertex set of a graph can be divided into two disjoint sets V_1, V_2 in such a way that every edge of the graph joins a vertex of V_1 to a vertex of V_2 the graph is said to be a *bipartite graph*. We often denote such a graph by $\Delta(V_1, V_2; E)$ if we wish to specify the two sets involved, and where Δ signifies that the graph in question is bipartite.

If a bipartite graph $\Delta(V_1, V_2; E)$ has the property that every vertex of V_1 is joined to every vertex of V_2, and it is simple then it is called a *complete bipartite graph* and is usually denoted by $K_{m,n}$ where $m = |V_1|$ and $n = |V_2|$.

Figure 1 shows the complete graph K_6 and the complete bipartite graph $K_{3,2}$.

A *path* in G is a finite sequence of distinct edges of the form (v_0, v_1), (v_1, v_2), $\ldots$, (v_{m-1}, v_m). The *length* of this path is m and it is said to *connect* v_0 and v_m.

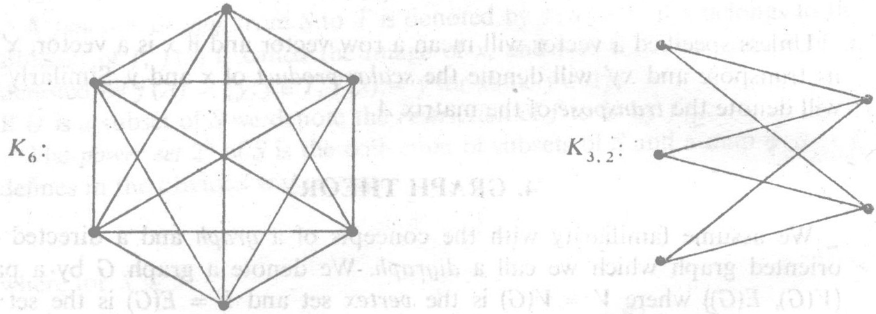

Figure 1

The vertices v_0 and v_m are called respectively the *initial* and *terminal* vertices of this path. The vertices v_i, $i \neq 0$, $i \neq m$ are *interior* vertices of this path. A *cycle* is a path in which $v_i \neq v_j$ for $i \neq j$ except that $v_0 = v_m$.

If we define a relation $\sim$ on $V(G)$ by $x \sim y$ if $x = y$ or there is a path in G joining x and y then it is easy to verify that $\sim$ is an equivalence relation on $V(G)$. The distinct equivalence classes are called the *connected components* of G. If there is one component G is *connected*.

A *subgraph* of a graph $G = (V, E)$ is a pair (U, F) where $U \subseteq V$ and $F \subseteq E$, with the proviso that if $e = (u, v) \in F$ then u and v are members of U.

If A is any set of edges of G we let $V(A)$ denote those vertices of G which are endpoints of some edge of A and then call $(V(A), A)$ the *subgraph generated* by A. We will use $G|A$ to denote the subgraph generated by A, though often we abbreviate this to A when it is clear from the context.

Thus for example if P is the set of edges of some path in G and $e \notin P$ is an edge of G, the statement "$e \cup P$ is a path" will mean e is incident with either the initial or terminal vertex of P and is not incident with any interior vertex of P. Similarly if $A \subseteq E(G)$ the statement "A is isomorphic to the complete graph K_4" means that the subgraph generated by A is isomorphic to K_4. If $X \subseteq V(G)$, we let $G \backslash X$ denote the subgraph obtained by deleting X and all edges incident with X from G.

A subgraph of G is a *spanning subgraph* if it has vertex set $V(G)$.

A *tree* is a graph which has no cycles and is connected. A *forest* is a graph which has no cycles. A *spanning forest* of G is union of spanning trees of its connected components. A *spanning tree* is a spanning subgraph which is a tree. It is easy to prove that G is connected if and only if it has a spanning tree, and that such a spanning tree must have exactly $|V(G)| - 1$ edges.

If $U \subseteq V(G)$ we let $G \backslash U$ denote the subgraph of G obtained by removing U and all its incident edges. A connected graph is *n-connected* for some positive integer n if there exists no set $U \subseteq V(G)$ with $|U| < n$ such that $G \backslash U$ is

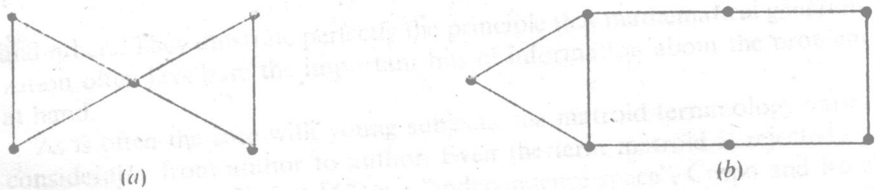

Figure 2

disconnected or a single vertex. Figures 2(a) and (b) show respectively a 1-connected and 2-connected graph.

A vertex u of a connected graph G such that $G\backslash\{u\}$ is disconnected is called a *cut vertex* of G.

More technical terms such as planarity, homeomorphism and so on are defined as they arise in the text. Moreover we often redefine graph theory terms as they are used to save the reader not too familar with graphs having to look back.

In a digraph $G = (V, E)$ we often denote an edge directed from the vertex u to the vertex v by (u, v) and call $u(v)$ respectively the *initial* (*terminal*) vertices of the edge. A *path* in a digraph is a finite sequence of distinct edges of the form $(v_0, v_1), (v_1, v_2), \ldots, (v_{m-1}, v_m)$ where the v_i are distinct vertices. Such a path is said to *pass through* the vertices v_i. Two paths are *vertex disjoint* if they do not pass through a common vertex. Other terms for digraphs are defined by obvious analogy with the corresponding terms for graphs.

CHAPTER 1

Fundamental Concepts and Examples

1. INTRODUCTION

Matroid theory dates from the 1930's when van der Waerden in his "Moderne Algebra" first approached linear and algebraic dependence axiomatically and Whitney in his basic paper [35] first used the term matroid. As the word suggests Whitney conceived a matroid as an abstract generalization of a matrix, and much of the language of the theory is based on that of linear algebra. However Whitney's approach was also to some extent motivated by his earlier work in graph theory and as a result some of the matroid terminology has a distinct graphical flavour.

Apart from isolated papers by Birkhoff [35], MacLane [36], [38], and Dilworth [41], [41a], [44], on the lattice theoretic and geometric aspects of matroid theory, and two important papers by Rado on the combinatorial applications of matroids [42] and infinite matroids [49], the subject lay virtually dormant until Tutte [58], [59], published his fundamental papers on matroids and graphs and Rado [57] studied the representability problem for matroids. Since then interest in matroids and their applications in combinatorial theory has accelerated rapidly. This is probably due to the discovery independently by Edmonds and Fulkerson [65] and Mirsky and Perfect [67] of a new, important class of matroids called transversal matroids. It is in the field of transversal theory that matroids seem so far to have had the most effect (measured in terms of new results obtained or easier proofs found of known results). In graph theory the main benefit of a matroid treatment seems to be a much more natural understanding of dual concepts such as the structure of the set of cocycles or the effect of contraction of a set of edges of a graph. The beauty and importance of matroids is perhaps best appreciated by the study of two covering and packing theorems of Edmonds [65], [65a]. These results give as easy corollaries, earlier very difficult, and intricate theorems of graph theory due to Tutte [61], and Nash-Williams [61], [64] a theorem about vector spaces due to Horn [55] and several results in transversal theory proved earlier by Higgins [59], Ore [55] and others. They illustrate perfectly the principle that mathematical generalization often lays bare the important bits of information about the problem at hand.

As is often the case with young subjects, the matroid terminology varies considerably from author to author. Even the term matroid is rejected by many. Mirsky and Perfect [67] use "independence space", Crapo and Rota in their monograph [70] on combinatorial geometries use "pregeometry" for "matroid"; Rado's work is in terms of "independence functions"; Cohn [65] uses the term "transitive dependence relation".

2. AXIOM SYSTEMS FOR A MATROID

As will be seen, a matroid may be defined in many different but equivalent ways, several of which were described in Whitney's original paper. Deciding which set of axioms would be the most natural to start with was difficult. I have eventually settled on "independence axioms" because I think they will be the most natural to the average reader.

Matroid theory has exactly the same relationship to linear algebra as does point set topology to the theory of real variable. That is, it *postulates* certain sets to be "independent" (=linearly independent) and develops a fruitful theory from certain axioms which it demands hold for this collection of independent sets.

A *matroid* M is a finite set S and a collection $\mathscr{I}$ of subsets of S (called *independent* sets) such that (I1)–(I3) are satisfied.

(I1) $\emptyset \in \mathscr{I}$.
(I2) If $X \in \mathscr{I}$ and $Y \subseteq X$ then $Y \in \mathscr{I}$.
(I3) If U, V are members of $\mathscr{I}$ with $|U| = |V| + 1$ there exists $x \in U \backslash V$ such that $V \cup x \in \mathscr{I}$.

A subset of S not belonging to $\mathscr{I}$ is called *dependent*.

Example. Let V be a finite vector space and let $\mathscr{I}$ be the collection of linearly independent subsets of vectors of V. Then $(V, \mathscr{I})$ is a matroid.

Following the analogy with vector spaces we make the following definitions.

A *base* of M is a maximal independent subset of S, the collection of bases is denoted by $\mathscr{B}$ or $\mathscr{B}(M)$.

The *rank function* of a matroid is a function $\rho: 2^S \to \mathbb{Z}$ defined by

$$\rho A = \max(|X| : X \subseteq A, X \in \mathscr{I}) \qquad (A \subseteq S).$$

The *rank of the matroid, M* sometimes denoted by ρM, is the rank of the set S.