Lecture Notes in Economics and Mathematical Systems

(Vol. 1–15: Lecture Notes in Operations Research and Mathematical Economics, Vol. 16–59: Lecture Notes in Operations Research and Mathematical Systems)

Vol. 1: H. Bühlmann, H. Loeffel, E. Nievergelt, Einführung in die Theorie und Praxis der Entscheidung bei Unsicherheit. 2. Auflage, IV, 125 Seiten. 1969. DM 16,–

Vol. 2: U. N. Bhat, A Study of the Queueing Systems M/G/1 and GI/M1. VIII, 78 pages. 1968. DM 16,–

Vol. 3: A. Strauss, An Introduction to Optimal Control Theory. VI, 153 pages. 1968. DM 16,–

Vol. 4: Branch and Bound: Eine Einführung. 2., geänderte Auflage. Herausgegeben von F. Weinberg. VII, 174 Seiten. 1972. DM 18,–

Vol. 5: Hyvärinen, Information Theory for Systems Engineers. VIII, 205 pages. 1968. DM 16,–

Vol. 6: H. P. Künzi, O. Müller, E. Nievergelt, Einführungskursus in die dynamische Programmierung. IV, 103 Seiten. 1968. DM 16,–

Vol. 7: W. Popp, Einführung in die Theorie der Lagerhaltung. VI, 173 Seiten. 1968. DM 16,–

Vol. 8: J. Teghem, J. Loris-Teghem, J. P. Lambotte, Modèles d'Attente M/G/1 et GI/M/1 à Arrivées et Services en Groupes. IV, 53 pages. 1969. DM 16,–

Vol. 9: E. Schultze, Einführung in die mathematischen Grundlagen der Informationstheorie. VI, 116 Seiten. 1969. DM 16,–

Vol. 10: D. Hochstädter, Stochastische Lagerhaltungsmodelle. VI, 269 Seiten. 1969. DM 18,–

Vol. 11/12: Mathematical Systems Theory and Economics. Edited by H. W. Kuhn and G. P. Szegö. VIII, IV, 486 pages. 1969. DM 34,–

Vol. 13: Heuristische Planungsmethoden. Herausgegeben von F. Weinberg und C. A. Zehnder. II, 93 Seiten. 1969. DM 16,–

Vol. 14: Computing Methods in Optimization Problems. Edited by A. V. Balakrishnan. V, 191 pages. 1969. DM 16,–

Vol. 15: Economic Models, Estimation and Risk Programming: Essays in Honor of Gerhard Tintner. Edited by K. A. Fox, G. V. L. Narasimham and J. K. Sengupta. VIII, 461 pages. 1969. DM 24,–

Vol. 16: H. P. Künzi und W. Oettli, Nichtlineare Optimierung: Neuere Verfahren, Bibliographie. IV, 180 Seiten. 1969. DM 16,–

Vol. 17: H. Bauer und K. Neumann, Berechnung optimaler Steuerungen, Maximumprinzip und dynamische Optimierung. VIII, 188 Seiten. 1969. DM 16,–

Vol. 18: M. Wolff, Optimale Instandhaltungspolitiken in einfachen Systemen. V, 143 Seiten. 1970. DM 16,–

Vol. 19: L. Hyvärinen Mathematical Modeling for Industrial Processes. VI, 122 pages. 1970. DM 16,–

Vol. 20: G. Uebe, Optimale Fahrpläne. IX, 161 Seiten. 1970. DM 16,–

Vol. 21: Th. Liebling, Graphentheorie in Planungs- und Tourenproblemen am Beispiel des städtischen Straßendienstes. IX, 118 Seiten. 1970. DM 16,–

Vol. 22: W. Eichhorn, Theorie der homogenen Produktionsfunktion. VIII, 119 Seiten. 1970. DM 16,–

Vol. 23: A. Ghosal, Some Aspects of Queueing and Storage Systems. IV, 93 pages. 1970. DM 16,–

Vol. 24: Feichtinger Lernprozesse in stochastischen Automaten. V, 66 Seiten. 1970. DM 16,–

Vol. 25: R. Henn und O. Opitz, Konsum- und Produktionstheorie. I. II, 124 Seiten. 1970. DM 16,–

Vol. 26: D. Hochstädter und G. Uebe, Ökonometrische Methoden. XII, 250 Seiten. 1970. DM 18,–

Vol. 27: I. H. Mufti, Computational Methods in Optimal Control Problems. IV, 45 pages. 1970. DM 16,–

Vol. 28: Theoretical Approaches to Non-Numerical Problem Solving. Edited by R. B. Banerji and M. D. Mesarovic. VI, 466 pages. 1970. DM 24,–

Vol. 29: S. E. Elmaghraby, Some Network Models in Management Science. III, 177 pages. 1970. DM 16,–

Vol. 30: H. Noltemeier, Sensitivitätsanalyse bei diskreten linearen Optimierungsproblemen. VI, 102 Seiten. 1970. DM 16,–

Vol. 31: M. Kühlmeyer, Die nichtzentrale t-Verteilung. II, 106 Seiten. 1970. DM 16,–

Vol. 32: F. Bartholomes und G. Hotz, Homomorphismen und Reduktionen linearer Sprachen. XII, 143 Seiten. 1970. DM 16,–

Vol. 33: K. Hinderer, Foundations of Non-stationary Dynamic Programming with Discrete Time Parameter. VI, 160 pages. 1970. DM 16,–

Vol. 34: H. Störmer, Semi-Markoff-Prozesse mit endlich vielen Zuständen. Theorie und Anwendungen. VII, 128 Seiten. 1970. DM 16,–

Vol. 35: F. Ferschl, Markovketten. VI, 168 Seiten. 1970. DM 16,–

Vol. 36: M. P. J. Magill, On a General Economic Theory of Motion. VI, 95 pages. 1970. DM 16,–

Vol. 37: H. Müller-Merbach, On Round-Off Errors in Linear Programming. VI, 48 pages. 1970. DM 16,–

Vol. 38: Statistische Methoden I. Herausgegeben von E. Walter. VIII, 338 Seiten. 1970. DM 22,–

Vol. 39: Statistische Methoden II. Herausgegeben von E. Walter. IV, 155 Seiten. 1970. DM 16,–

Vol. 40: H. Drygas, The Coordinate-Free Approach to Gauss-Markov Estimation. VIII, 113 pages. 1970. DM 16,–

Vol. 41: U. Ueing, Zwei Lösungsmethoden für nichtkonvexe Programmierungsprobleme. VI, 92 Seiten. 1971. DM 16,–

Vol. 42: A. V. Balakrishnan, Introduction to Optimization Theory in a Hilbert Space. IV, 153 pages. 1971. DM 16,–

Vol. 43: J. A. Morales, Bayesian Full Information Structural Analysis. VI, 154 pages. 1971. DM 16,–

Vol. 44: G. Feichtinger, Stochastische Modelle demographischer Prozesse. XIII, 404 Seiten. 1971. DM 28,–

Vol. 45: K. Wendler, Hauptaustauschschritte (Principal Pivoting). II, 64 Seiten. 1971. DM 16,–

Vol. 46: C. Boucher, Leçons sur la théorie des automates mathématiques. VIII, 193 pages. 1971. DM 18,–

Vol. 47: H. A. Nour Eldin, Optimierung linearer Regelsysteme mit quadratischer Zielfunktion. VIII, 163 Seiten. 1971. DM 16,–

Vol. 48: M. Constam, FORTRAN für Anfänger. 2. Auflage. VI, 148 Seiten. 1973. DM 16,–

Vol. 49: Ch. Schneeweiß, Regelungstechnische stochastische Optimierungsverfahren. XI, 254 Seiten. 1971. DM 22,–

Vol. 50: Unternehmensforschung Heute – Übersichtsvorträge der Züricher Tagung von SVOR und DGU, September 1970. Herausgegeben von M. Beckmann. VI, 133 Seiten. 1971. DM 16,–

Vol. 51: Digitale Simulation. Herausgegeben von K. Bauknecht und W. Nef. IV, 207 Seiten. 1971. DM 18,–

Vol. 52: Invariant Imbedding. Proceedings of the Summer Workshop on Invariant Imbedding Held at the University of Southern California, June–August 1970. Edited by R. E. Bellman and E. D. Denman. IV, 148 pages. 1971. DM 16,–

Vol. 53: J. Rosenmüller, Kooperative Spiele und Märkte. IV, 152 Seiten. 1971. DM 16,–

Vol. 54: C. C. von Weizsäcker, Steady State Capital Theory. III, 102 pages. 1971. DM 16,–

Vol. 55: P. A. V. B. Swamy, Statistical Inference in Random Coefficient Regression Models. VIII, 209 pages. 1971. DM 20,–

Vol. 56: Mohamed A. El-Hodiri, Constrained Extrema. Introduction to the Differentiable Case with Economic Applications. III, 130 pages. 1971. DM 16,–

Vol. 57: E. Freund, Zeitvariable Mehrgrößensysteme. VII, 160 Seiten. 1971. DM 18,–

Vol. 58: P. B. Hagelschuer, Theorie der linearen Dekomposition. VII, 191 Seiten. 1971. DM 18,–

continuation on page 110

Lecture Notes in Economics and Mathematical Systems

Managing Editors: M. Beckmann and H. P. Künzi

Mathematical Economics

109

Rabe von Randow

Introduction to the Theory of Matroids

Springer-Verlag
Berlin · Heidelberg · New York 1975

Author

Dr. Rabe von Randow
Institut für Ökonometrie
und Operations Research
Universität Bonn
Abt. Operations Research
Nassestraße 2
53 Bonn 1
BRD

Library of Congress Cataloging in Publication Data

Randow, Rabe von.
Introduction to the theory of matroids.

(Mathematical economics) (Lecture notes in economics and mathematical systems ; 109)
Bibliography: p.
Includes index.
1. Matroids. I. Title. II. Series. III. Series: Lecture notes in economics and mathematical systems ; 109.
QA166.6.R36 512'.5 75-16380

AMS Subject Classifications (1970): 05B35, 90A99, 90B10, 90C05, 94A20

ISBN-13: 978-3-540-07177-8 e-ISBN-13: 978-3-642-48292-2
DOI: 10.1007/978-3-642-48292-2

Offsetdruck: Julius Beltz, Hemsbach/Bergstr.

Preface

Matroid theory has its origin in a paper by H. Whitney entitled "On the abstract properties of linear dependence" [35], which appeared in 1935. The main objective of the paper was to establish the essential (abstract) properties of the concepts of linear dependence and independence in vector spaces, and to use these for the axiomatic definition of a new algebraic object, namely the matroid. Furthermore, Whitney showed that these axioms are also abstractions of certain graph-theoretic concepts. This is very much in evidence when one considers the basic concepts making up the structure of a matroid: some reflect their linear-algebraic origin, while others reflect their graph-theoretic origin. Whitney also studied a number of important examples of matroids.

The next major development was brought about in the forties by R. Rado's matroid generalisation of P. Hall's famous "marriage" theorem. This provided new impulses for transversal theory, in which matroids today play an essential role under the name of "independence structures", cf. the treatise on transversal theory by L. Mirsky [26]. At roughly the same time R.P. Dilworth established the connection between matroids and lattice theory. Thus matroids became an essential part of combinatorial mathematics.

About ten years later W.T. Tutte [30] developed the fundamentals of matroids in detail from a graph-theoretic point of view, and characterised graphic matroids as well as the larger class of those matroids that are representable over any field.

More recently papers by Bondy, Brualdi, Crapo, Edmonds, Fulkerson, Ingleton, Lehman, Mason, Maurer, Minty, Nash-Williams, Piff, Rado, Rota, de Sousa, Tutte, Welsh, Woodall, and other combinatorialists have led to a widespread interest in matroids and to a rapid growth in the volume of literature on matroids.

As was mentioned above, matroids are defined axiomatically. However, their rich structure allows one to pick one of a number of axiomatic definitions, depending on which of the matroid properties is to play the dominant role (cf. the survey papers by Harary and Welsh [15] and Wilson [36]). Thus in practice each author uses the definition most suitable for his purposes. Whitney considered the equivalence of several of these different definitions in his fundamental paper, and the recent book by H.H. Crapo and G.-C. Rota [7] does so as well but treats the subject within a lattice-theoretic framework. Apart from these no general introduction to the theory of matroids, giving their various equivalent axiomatic definitions and the most important examples, is readily available.

The present monograph is an attempt to fill this gap. Its main objective is to provide an introduction to matroids and all the usual basic concepts associated with them without favouring any particular point of view, and to prove the equivalence of all the usual axiomatic definitions of matroids. Furthermore, we have collected together and proved all the commonly used properties of matroids involving the concepts introduced. Where proofs were taken from the literature, the source has been indicated in the usual way. Next we have discussed the common types of matroids - matrix-matroids, binary, graphic, cographic, uniform, matching and transversal matroids - in some detail, mentioning others such as orientable matroids and gammoids, as well as important characterisations of the above, in remarks. Much of the material on the examples can be read after the initial definition of a matroid. Two further chapters deal respectively with the greedy algorithm and its relation to matroids, and with the recent interesting results on exchange properties of matroid bases.

A number of omissions will however be immediately obvious. We have for example not developed the geometry of matroids involving minors and separators. For a treatment of this topic we refer the reader to the paper [30] and book [31] by Tutte and to the book by Crapo and Rota [7]. Furthermore, no mention is made of the recent work by Maurer [24] and Holzmann, Norton and Tobey [16] on the basis-graphic representation of matroids. These and other topics not considered here go beyond the scope of this monograph as a first introduction to matroid theory.

One of the most beautiful aspects of the matroid concept is its unifying nature - by specialisation it covers many apparently unrelated structures and thus reveals their essential nature as well as yielding clear and often easy proofs for results that are otherwise very tedious to derive (cf. Remark (8) at the end of Chapter III). Matroids have however also led to decisive advances in theories important for practical applications, for example in linear programming through the greedy algorithm (cf. the papers by Edmonds [10], [11], and Dunstan and Welsh [9]), and in network theory (cf. Minty [25]). Moreover, it is felt that matroids could well become a new and powerful tool in the mathematical theory of economics, and it is with this thought in mind that the present monograph is addressed in particular to mathematical economists and operations research specialists.

In conclusion, I wish to express my gratitude to Professor B. Korte for introducing me to matroid theory and encouraging me to write this monograph, and I extend my thanks to Professor M. Beckmann for accepting it for publication in the Lecture Notes Series.

University of Bonn
March 1975

R. von Randow

Contents

Chapter V. Exchange Properties for Bases of Matroids.

Basic Notation

$\mathbb{N}$	the set of non-negative integers,
$\mathbb{N}_+$	the set of positive integers,
$\mathbb{R}$	the field of real numbers,
$\mathbb{Z}_2$	the ring (field) of residue classes of integers modulo 2,
$\mathcal{P}(M)$	the power set of the set M, i.e. the set whose elements are precisely all the subsets of M,
$\lvert M \rvert$	the number of elements in the finite set M,
$\emptyset$	the empty set,
$\{a,b\}$	the set consisting of the elements a and b,
$\{x \in X : p(x)\}$	the set of elements of X having property p,
$X-Y$	the difference set $\{x \in X : x \notin Y\}$,
$\bigwedge$	the quantifier "for each",
$\exists$	the quantifier "there exist(s)",
$\wedge$	"and" (logical conjunction),
$\Longrightarrow$, $\Longleftarrow$	logical implications,
$\Longleftrightarrow$	logical equivalence,
$\mathrm{im}(\varphi)$	the image set $\{\varphi(x) : x \in X\} \subset Y$ of the mapping $\varphi: X \longrightarrow Y$.

Chapter I. Equivalent Axiomatic Definitions and Elementary Properties of Matroids.

§1.1. The First Rank-Axiomatic Definition of a Matroid.

Definitions.

(a) Let E be a finite set and r a function $r: \mathfrak{P}(E) \longrightarrow \mathbb{N}$.
Then the pair (E,r) is a matroid M(E,r), and r(S) is the rank of $S \subset E$, if the following conditions hold:

(R1) $\bigwedge S \subset E \quad r(S) \leqslant |S|$,

(R2) $\bigwedge S,S' \subset E \quad [\, S \subset S' \Longrightarrow r(S) \leqslant r(S') \,]$,

(R3) $\bigwedge S,S' \subset E$ the submodular inequality holds:
$$r(S \cup S') + r(S \cap S') \leqslant r(S) + r(S') .$$

(b) A matroid M(E,r) is normal if $\bigwedge e \in E \quad r(\{e\}) = 1$.

Remarks and Further Definitions. Let M(E,r) be a matroid.

(1) The rank of the matroid M(E,r) is r(E).

(2) In the above definition of a matroid, axiom (R1) can be replaced by the axioms: $r(\emptyset) = 0$, and $\bigwedge e \in E \quad r(\{e\}) \in \{0,1\}$, as these are clearly implied by (R1), and together with (R3) imply (R1) by induction over $|S|$.

(3) (M(E,r) is normal and axiom (R3) holds with equality) $\Longleftrightarrow$ $(\bigwedge S \subset E \quad r(S) = |S|\,)$.

Proof: $\Longleftarrow$: Follows because $|S \cup S'| = |S| + |S'| - |S \cap S'|$.
$\Longrightarrow$: By induction over $|S|$.

(4) The following properties follow readily from the definition of a matroid:

(i) $\bigwedge S \subset E \quad \bigwedge e \in E \quad [\ r(\{e\}) = 0 \implies r(S \cup \{e\}) = r(S)\ ]$,

(ii) $\bigwedge S \subset E \quad [\ (\bigwedge e \in S \quad r(\{e\}) = 0) \implies r(S) = 0\ ]$.

On account of these properties points of rank 0 are relatively uninteresting, and some authors (cf. Berge [1]) exclude such points in their definition of a matroid.

(5) Definition. Let X be a set, A a property of sets, and Y a subset of X with property A.

(a) (Y is a maximal subset of X with property A) $:\Longleftrightarrow$ $[(Y \subset Y' \subset X \wedge Y' \text{ has property A}) \implies Y' = Y\ ]$,

(b) (Y is a minimal subset of X with property A) $:\Longleftrightarrow$ $[(Y' \subset Y \subset X \wedge Y' \text{ has property A}) \implies Y' = Y\ ]$.

(6) A subset $S \subset E$ is called independent if $r(S) = |S|$. We shall denote by F the family of independent sets of M(E,r). Note that $\emptyset \in F$.

A basis of M(E,r) is a maximal independent subset of E. We shall denote by W the family of bases of M(E,r).

If $B \in W$, then E–B is called a cobasis of M(E,r). We shall denote by W* the family of cobases of M(E,r). This notation is motivated by properties of the "dual matroid" defined in §2.4.

(7) A subset $S \subset E$ is called dependent if $r(S) < |S|$, i.e. $S \notin F$. Note that if M(E,r) is normal, then S dependent implies $|S| \geq 2$.

A circuit of M(E,r) is a minimal dependent subset of E. We shall denote by Z the family of circuits of M(E,r).

(8) If $S \subset E$, then $M(S, r|_S)$ is a matroid, called the reduction matroid $M \times S$ of M(E,r).

<u>Theorem 1</u>. Let $M(E,r)$ be a matroid.

(a) $\bigwedge e \in E \quad \bigwedge S \subset E \quad (r(S \cup \{e\}) - r(S)) \in \{0,1\}$,

(b) $\bigwedge S,S' \subset E \quad [\ S \subset S' \Longrightarrow 0 \leqslant r(S') - r(S) \leqslant |S'-S|\ ]$,

(c) $\bigwedge S,S' \subset E \quad [\ S \subset S' \in F \Longrightarrow S \in F\ ]$,

(d) $\bigwedge S \subset E \quad [(\bigwedge e \in S \quad r(S-\{e\}) = |S|-1 = r(S)) \Longleftrightarrow S \in Z\ ]$,

(e) $\bigwedge e_1,e_2 \in E \quad \bigwedge S \subset E$

$[r(S \cup \{e_1\}) = r(S \cup \{e_2\}) = r(S) \Longrightarrow r(S \cup \{e_1,e_2\}) = r(S)]$,

<u>Corollary</u>. $\bigwedge S,S' \subset E$

$[(\bigwedge e \in S' \quad r(S \cup \{e\}) = r(S)) \Longrightarrow r(S \cup S') = r(S)]$,

(f) $\bigwedge S \subset E \quad r(S) = \max\{|S'| : S \supset S' \in F\} = \max\{|S \cap S'| : S' \in F\}$,

<u>Corollary</u>. $\bigwedge S \subset E \quad [S \in F \Longleftrightarrow (\bigwedge e \in S \quad r(S) - r(S-\{e\}) = 1)]$,

(g) $\bigwedge S,S_1,S_2 \subset E \quad [S_1$ and S_2 are maximal independent subsets of S (i.e. bases of the reduction matroid $M \times S$) $\Longrightarrow$

$|S_1| = |S_2|]$,

<u>in particular</u>, $B \in W \Longrightarrow r(B) = r(E)$,

(h) $\bigwedge B,B' \in W \quad \bigwedge e \in B \quad \exists\ e' \in B' : (B-\{e\}) \cup \{e'\} \in W$,

(i) $\bigwedge S \subset E$ (α) $S \in F \Longleftrightarrow (\bigwedge C \in Z \quad C - S \neq \emptyset)$,

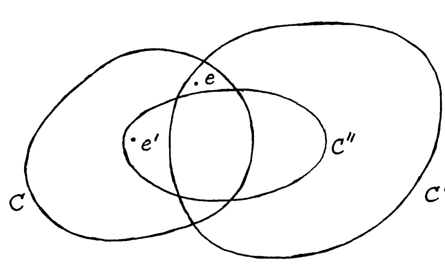
(β) $S \notin F \Longleftrightarrow (\bigwedge S' \in W^* \quad S \cap S' \neq \emptyset)$,

(j) $\bigwedge e,e' \in E \quad \bigwedge C,C' \in Z$

$[(e \in C \cap C' \wedge e' \in C-C') \Longrightarrow (\exists\ C'' \in Z : e' \in C'' \subset (C \cup C')-\{e\})]$,

<u>in particular</u>, $\bigwedge e \in E \quad \bigwedge C,C' \in Z$

$[(C \neq C' \wedge e \in C \cap C') \Longrightarrow (\exists\ C'' \in Z : C'' \subset (C \cup C')-\{e\})]$,



(k) $\bigwedge e \in E \quad \bigwedge S \subset E \quad [(S \in F \wedge S \cup \{e\} \notin F) \Longrightarrow (\exists$ unique $C \in Z : C \subset S \cup \{e\}$ (clearly $e \in C$))] .

Proof.

(a) $e \in S$ implies $r(S \cup \{e\}) = r(S)$.

Suppose $e \in E-S$. Then by axioms (R2), (R3), and Remark (2),

$r(S) + 1 \geqslant r(S) + r(\{e\}) \geqslant r(S \cup \{e\}) + r(\emptyset) = r(S \cup \{e\}) \geqslant r(S)$,

hence $0 \leqslant r(S \cup \{e\}) - r(S) \leqslant 1$.

(b) Trivial if $S = S'$. Let $S'-S =: \{e_1, e_2, \ldots, e_k\}$. Then by (a),

$$0 \leqslant r(S \cup \{e_1\}) - r(S) \leqslant 1$$
$$0 \leqslant r(S \cup \{e_1, e_2\}) - r(S \cup \{e_1\}) \leqslant 1$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$0 \leqslant r(S') - r(S'-\{e_k\}) \leqslant 1 ,$$

hence $0 \leqslant r(S') - r(S) \leqslant k = |S'-S|$.

(c) Let $S \subset S' \subset E$. Then by (b),

$r(S) < |S| \implies r(S') \leqslant r(S) + |S'-S| < |S| + |S'-S| = |S'|$

$\implies$ S' is dependent.

(d) $\Longleftarrow$: Follows from definitions and axiom (R2).

$\Longrightarrow$: Follows from definitions and (c).

(e) Trivial if $e_1 = e_2$. If $e_1 \neq e_2$, then

$2r(S) = r(S \cup \{e_1\}) + r(S \cup \{e_2\}) \geqslant r(S \cup \{e_1, e_2\}) + r(S)$,

hence $r(S) \leqslant r(S \cup \{e_1, e_2\}) \leqslant r(S)$, i.e. $r(S \cup \{e_1, e_2\}) = r(S)$.

Corollary: Follows by repeated application of (e).

(f) Trivial if $S \in F$. Suppose $S \notin F$, i.e. $r(S) < |S|$. Then

$S \supset S' \in F \implies r(S) \geqslant r(S') = |S'|$, hence

$r(S) \geqslant \max\{|S'| : S \supset S' \in F\} =: \sigma$. Clearly $\sigma < |S|$.

Let $S \supset \tilde{S} \in F$ with $r(\tilde{S}) = |\tilde{S}| = \sigma$.

($\underline{\underline{i}}$) $|S| = \sigma + 1$:- Let $S-\tilde{S} =: \{e\}$. Then by definition of σ, $r(\tilde{S}) = r(\tilde{S} \cup \{e\}) = r(S)$.

($\underline{\underline{ii}}$) $|S| > \sigma + 1$:- By definition of σ, $\bigwedge e \in S-\tilde{S}$ $r(\tilde{S} \cup \{e\}) = r(\tilde{S})$. Hence by the corollary of (e), $r(S) = r(\tilde{S} \cup (S-\tilde{S})) = r(\tilde{S})$.

Finally $\max\{|S'| : S \supset S' \in F\} = \max\{|S \cap S'| : S' \in F\}$ by (c).

Corollary: $\Longrightarrow$: Clear by definition of F.

$\Longleftarrow$: Let $S \supset S' \in F$ with $r(S) = |S'|$. If $S' \neq S$, let $e \in S-S'$. Then by (f) $r(S) = r(S-\{e\})$, contradiction.

(g) Clearly $S_1 \not\subset S_2$, i.e. $S_1 - S_2 \neq \emptyset$. Furthermore $\bigwedge e \in S_1 - S_2$ $r(S_2 \cup \{e\}) = r(S_2)$, hence by the corollary of (e), $r(S_1 \cup S_2) = r(S_2 \cup (S_1 - S_2)) = r(S_2)$. Similarly $r(S_1 \cup S_2) = r(S_1)$, hence $r(S_1) = r(S_2)$, i.e. $|S_1| = |S_2|$.

(h) $B-\{e\} \in F$, and $B-\{e\} \subset (B-\{e\}) \cup B'$. On the other hand, $|B-\{e\}| = |B'| - 1$, hence $B-\{e\}$ is not a maximal independent subset of $(B-\{e\}) \cup B'$, therefore $\exists$ $e' \in B'$ such that $(B-\{e\}) \cup \{e'\} \in W$.

(i) (α) S is independent $\Longleftrightarrow$ no subset of S is dependent $\Longleftrightarrow$ S does not contain a circuit.

(β) S is dependent $\Longleftrightarrow$ S is not contained in a basis $\Longleftrightarrow$ every cobasis intersects S.

(j) ($\underline{\underline{i}}$) Let $\sigma := r((C \cup C')-\{e\})$. We will show in ($\underline{\underline{ii}}$) below that $r((C \cup C')-\{e,e'\}) = \sigma$. This implies that $\exists$ $S \subset (C \cup C')-\{e,e'\}$ with $S \in F$ and $r(S) = \sigma$. Furthermore, $S \cup \{e'\} \notin F$, as $\sigma = r(S) \leqslant r(S \cup \{e'\}) \leqslant r((C \cup C')-\{e\}) = \sigma$ and thus $r(S \cup \{e'\}) = \sigma < \sigma+1 = |S \cup \{e'\}|$. Hence $\exists$ $C'' \in Z$ with $e' \in C'' \subset S \cup \{e'\} \subset (C \cup C')-\{e\}$.

($\underline{\underline{ii}}$) $r((C \cup C')-\{e,e'\}) = \sigma$:- Clearly $r((C \cup C')-\{e,e'\}) \in \{\sigma-1, \sigma\}$.

Let S be an independent subset of $(C\cup C')-\{e,e'\}$ with $C'-\{e\}\subset S$ and $r(S) = \sigma-1$, (note use of (g)). Suppose $\bigwedge \tilde{e}\in(C\cup C')-\{e,e'\}$ $r(S\cup\{\tilde{e}\}) = \sigma-1$. Note that $r(S\cup\{e\}) = \sigma-1$ as $C'\subset S\cup\{e\}\notin F$, so we have that $\bigwedge \tilde{e}\in(C\cup C')-\{e'\}$ $r(S\cup\{\tilde{e}\}) = \sigma-1$, hence by the corollary of (e), $r((C\cup C')-\{e'\}) = \sigma-1$. This implies that $r(C\cup C')\in\{\sigma-1,\sigma\}$; on the other hand $r(C\cup C') \geqslant r((C\cup C')-\{e\})=\sigma$, hence $r(C\cup C') = \sigma$. Therefore $\exists\ \tilde{S}\subset C\cup C'$ with $C-\{e'\}\subset\tilde{S}\in F$ and $r(\tilde{S}) = \sigma$, (note use of (g)), and furthermore $e'\in\tilde{S}$ as otherwise $\tilde{S}\subset(C\cup C')-\{e'\}$ and thus $r(\tilde{S}) \leqslant \sigma-1$. Hence $C\subset\tilde{S}$, contradiction. Therefore $\exists\ \tilde{e}\in(C\cup C')-\{e,e'\}$ such that $r(S\cup\{\tilde{e}\}) = \sigma$, i.e. $r((C\cup C')-\{e,e'\}) = \sigma$.

Short Proof of Special Case of (j):

$C\cap C' \neq C$ as $C\not\subset C'$, hence $C\cap C'\in F$. Then

$r((C\cup C')-\{e\}) \leqslant r(C\cup C') \leqslant r(C) + r(C') - r(C\cap C') =$

$= (|C|-1) + (|C'|-1) - |C\cap C'| = |C\cup C'| - 2 < |(C\cup C')-\{e\}|$,

hence $(C\cup C')-\{e\}\notin F$. Thus $\exists\ C''\in Z$ with $C''\subset(C\cup C')-\{e\}$.

(k) Suppose $\exists\ C,C'\in Z$ with $C\neq C'$ and $e\in C\subset S\cup\{e\}$, $e\in C'\subset S\cup\{e\}$. Then by the special case of (j) $\exists\ C''\in Z$ with $C''\subset(C\cup C')-\{e\}\subset S\in F$, contradiction.

The following theorem contains a result similar in structure to that of Theorem 1(h):

Theorem 2. $\bigwedge S\subset E \quad \bigwedge e\in E \quad \bigwedge B\in W$

$[(e\in B \wedge S\in F \wedge S\cup\{e\}\notin F) \Longrightarrow (\exists\ e'\in S-B : (S\cup\{e\})-\{e'\}\in F)]$.

<u>In particular</u>:

$\bigwedge B,B'\in W \quad \bigwedge e\in B-B' \quad \exists\ e'\in B'-B \ : \ (B'\cup\{e\})-\{e'\}\in W$,

<u>or equivalently</u>:

$\bigwedge S,S'\in W^* \quad \bigwedge\ e\in S' \quad \exists\ e'\in S \ : \ (S'-\{e\})\cup\{e'\}\in W^*$.

<u>Proof</u>: Trivial if $|S|\in\{0,1\}$. Let $|S| \geqslant 2$, and suppose that $\bigwedge\ \tilde{e}\in S-B \quad (S\cup\{e\})-\{\tilde{e}\}\notin F$. Then given $e'\in S-B$, $\exists\ C'\in Z$ with $e\in C'\subset (S\cup\{e\})-\{e'\}$ as $S-\{e'\}\in F$. Furthermore $C'\cap(S-B) \neq \emptyset$ as otherwise $C'\subset B$. Take $e''\in C'\cap(S-B)$, then as above $\exists\ C''\in Z$ with $e\in C''\subset (S\cup\{e\})-\{e''\}$. Hence by the special case of (j) $\exists\ C\in Z$ with $C\subset (C'\cup C'')-\{e\}\subset S$, contradiction.

§1.2. The Independence-Axiomatic Definition of a Matroid.

<u>Definitions</u>.

(a) Let E be a finite set and F a family of subsets of E. Then the pair (E,F) is a <u>matroid</u> M(E,F), and the elements of F are the <u>independent</u> sets of M(E,F), if the following conditions hold:

(F1) $\emptyset\in F$,

(F2) $\bigwedge S,S'\subset E \quad [S\subset S'\in F \Longrightarrow S\in F]$,

(F3) $\bigwedge S,S_1,S_2\subset E \quad [S_1$ and S_2 are maximal independent subsets of $S \Longrightarrow |S_1| = |S_2|]$.

(b) A matroid M(E,F) is <u>normal</u> if $\bigwedge e\in E \quad \{e\}\in F$.

(c) Let M(E,F) be a matroid. We define a mapping $r: \mathfrak{P}(E) \longrightarrow \mathbb{N}$ as follows: $\quad r(S) := \max\{|S'| : S\supset S'\in F\}$, $\quad S\subset E$.
r(S) is called the <u>rank</u> of S. Clearly

$$\bigwedge S\subset E \quad [S\in F \iff r(S) = |S|] . \qquad \ldots\ldots\ldots\ldots(*)$$

<u>Remarks</u>.

(1) We note that axiom (F1) is in fact a consequence of axiom (F2).

(2) It follows immediately that every matroid M(E,r) is a matroid M(E,F). The converse is established by the following theorem:

<u>Theorem 3</u>. The matroid M(E,F) satisfies the axioms (R1) - (R3).

<u>Proof</u>. Axioms (R1) and (R2) follow immediately.
Proof of Axiom (R3) (Berge [1]):- Suppose $S,S' \subset E$.
$\exists S_1 \in F$ with $S_1 \subset S \cap S'$ and $|S_1| = r(S_1) = r(S \cap S')$.
$\exists S_2 \in F$ with $S_1 \subset S_2 \subset S$ and $|S_2| = r(S_2) = r(S)$, (note use of Axiom (F3)).
$\exists S_3 \in F$ with $S_2 \subset S_3 \subset S \cup S'$ and $|S_3| = r(S_3) = r(S \cup S')$, (note use of axiom (F3)). As $S_2 \subset S_3 \cap S \in F$ and S_2 is maximal independent in S, it follows that $S_2 = S_3 \cap S$. Similarly $S_1 = S_2 \cap (S \cap S') = S_2 \cap S'$, hence $S_1 = S_3 \cap S \cap S'$. Thus

$$\begin{aligned} r(S \cup S') &= |S_3| = |(S_3 \cap S) \cup (S_3 \cap S')| = \\ &= |S_3 \cap S| + |S_3 \cap S'| - |S_3 \cap S \cap S'| \\ &\leqslant |S_2| + r(S') - |S_1| \text{ by (F2) and definition of } r, \\ &= r(S) + r(S') - r(S \cap S') . \end{aligned}$$

<u>Corollary 1</u>. By Theorem 3 and the statement (*) of Definition (c) it follows that the first rank-axiomatic and the independence-axiomatic definitions of a matroid are equivalent.

<u>Corollary 2</u>. Let E be a finite set, $F \subset \mathfrak{P}(E)$ with $\emptyset \in F$, and $r: \mathfrak{P}(E) \longrightarrow \mathbb{N}$ the mapping defined by

$$r(S) := \max\{|S'| : S \supset S' \in F\}, \quad S \subset E .$$

Then $\exists$ a matroid on E with family of independent sets F and rank function r, if and only if r satisfies the submodular inequality.

§1.3. The Second Rank-Axiomatic Definition of a Matroid.

Definitions.

(a) Let E be a finite set and r a function $r: \mathfrak{P}(E) \longrightarrow \mathbb{N}$.
Then the pair (E,r) is a matroid M'(E,r), and r(S) is the rank of $S \subset E$, if the following conditions hold:

(R'1) $r(\emptyset) = 0$,

(R'2) $\bigwedge e \in E \quad \bigwedge S \subset E \quad (r(S \cup \{e\}) - r(S)) \in \{0,1\}$,

(R'3) $\bigwedge e_1, e_2 \in E \quad \bigwedge S \subset E$

$$[r(S \cup \{e_1\}) = r(S \cup \{e_2\}) = r(S) \Longrightarrow r(S \cup \{e_1, e_2\}) = r(S)].$$

Remarks and Further Definitions. Let M'(E,r) be a matroid.

(1) (R'1) and (R'2) imply $\bigwedge e \in E \quad r(\{e\}) \in \{0,1\}$. A matroid M'(E,r) is normal if $\bigwedge e \in E \quad r(\{e\}) = 1$.

(2) (R'2) implies Theorem 1(b), i.e. $\bigwedge S, S' \subset E$
$[S \subset S' \Longrightarrow 0 \leqslant r(S') - r(S) \leqslant |S'-S|]$, (cf. proof of Theorem 1(b)), in particular
(i) (R2), i.e. $\bigwedge S, S' \subset E \quad [S \subset S' \Longrightarrow r(S) \leqslant r(S')]$, and
(ii) with (R'1) we get (R1), i.e. $\bigwedge S \subset E \quad r(S) \leqslant |S|$.
A subset $S \subset E$ is called independent if $r(S) = |S|$. We shall denote by F the family of independent sets of M'(E,r).

(3) The axioms (R'1) - (R'3) imply

$$\bigwedge S \subset E \quad r(S) = \max\{|S'| : S \supset S' \in F\} ,$$

(cf. proof of Theorem 1(f) and Remark (2)).

(4) It follows immediately that every matroid M(E,r) is a matroid M'(E,r). The following theorem establishes that every matroid M'(E,r) is a matroid M(E,F):

Theorem 4. The matroid M'(E,r) satisfies the axioms (F1) - (F3).

Proof. Axiom (F1) follows immediately.
Axiom (F2) is Theorem 1(c), which follows from axiom (R'2), (cf. proof of Theorem 1(c) and Remark (2)).
Axiom (F3) is Theorem 1(g), which follows from axioms (R'2) and (R'3), (cf. proof of Theorem 1(g)).

Corollary. By Theorem 4 and Remark (3) it follows that the two rank-axiomatic and the independence-axiomatic definitions of a matroid are pairwise equivalent.

§1.4. The Circuit-Axiomatic Definition of a Matroid.

Definitions.

(a) Let E be a finite set and Z a family of subsets of E. Then the pair (E,Z) is a matroid M(E,Z), and the elements of Z are the circuits of M(E,Z), if the following conditions hold:

(Z1) $\emptyset \notin Z$,

(Z2) $\bigwedge C,C' \in Z \quad [C \subset C' \Longrightarrow C = C']$,

(Z3) $\bigwedge e \in E \quad \bigwedge C,C' \in Z$
$[(C \neq C' \wedge e \in C \cap C') \Longrightarrow (\exists C'' \in Z : C'' \subset (C \cup C')-\{e\})]$.

(b) A matroid M(E,Z) is normal if $\bigwedge C \in Z \quad |C| \geqslant 2$.

Remarks and Further Definitions.

(1) Let M(E,Z) be a matroid. A subset $S \subset E$ is called independent if it contains no circuits. We shall denote by F the family of independent sets of M(E,Z). Clearly we have

$$C \in Z \iff C \notin F \wedge [(S \subset C \wedge S \neq C) \implies S \in F] \quad \ldots\ldots\ldots\ldots(*)$$

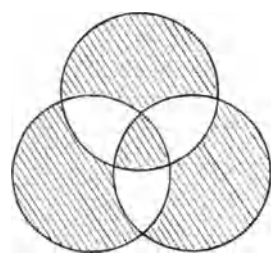
and Theorem 1(k) holds, (cf. proof of Theorem 1(k)), i.e.

$\bigwedge e \in E \quad \bigwedge S \subset E \quad [(S \in F \wedge S \cup \{e\} \notin F) \implies (\exists \text{ unique } C \in Z :$ $C \subset S \cup \{e\}$ (clearly $e \in C$))] .

(2) Definition. Let $S, S' \subset E$. The symmetric difference $S \Delta S'$ of S and S' is $S \Delta S' := (S-S') \cup (S'-S) = (S \cup S') - (S \cap S')$. It follows readily that the operator Δ is commutative and associative, and if $n \in \mathbb{N}$, $n>1$, and $\bigwedge i \in \{1,2,\ldots,n\}$ $S_i \subset E$ and $A_i := \{x \in \bigcup_{j=1}^{n} S_j : x \in \text{exactly } i \text{ of the } S_j\}$, then

$$S_1 \Delta S_2 \Delta \ldots \Delta S_n = \bigcup_{i=0}^{[\frac{n-1}{2}]} A_{2i+1} ,$$ and

$$\sum_{i=1}^{n} |S_i| \equiv |\mathop{\Delta}_{i=1}^{n} S_i| \pmod 2 .$$



(3) It follows immediately that every matroid M(E,r) is a matroid M(E,Z). The following theorem establishes that every matroid M(E,Z) is a matroid M(E,F):

Theorem 5. The matroid M(E,Z) satisfies the axioms (F1) - (F3).

Proof. Axioms (F1) and (F2) follow immediately.

Axiom (F3):- Let S_1 and S_2 be distinct maximal independent subsets of S. Then $S_1 - S_2 \neq \emptyset$ and $S_2 - S_1 \neq \emptyset$. Let $e \in S_2 - S_1$, then $S_1 \cup \{e\} \notin F$, hence $\exists\, C \in Z$ with $e \in C \subset S_1 \cup \{e\}$. Furthermore,

$C \cap (S_1 - S_2) \neq \emptyset$ as otherwise $C \subset S_2$. Let $\tilde{e} \in C \cap (S_1 - S_2)$ and $S_3 := (S_1 - \{\tilde{e}\}) \cup \{e\}$. Note that $|S_3| = |S_1|$.

(i) $S_3 \in F$: Clearly $S_1 - \{\tilde{e}\} \in F$. Suppose $S_3 \notin F$, then $\exists\ C' \in Z$ with $e \in C' \subset S_3 \subset S_1 \cup \{e\}$, and $C' \neq C$ as $\tilde{e} \notin C'$. This contradicts Theorem 1(k), (cf. Remark (1)).

(ii) S_3 is maximal independent in S: Suppose $\tilde{S}$ is a maximal independent subset of S with $S_3 \subset \tilde{S}$ and $|S_3| < |\tilde{S}|$. $\tilde{e} \notin \tilde{S}$ as otherwise $S_1 \subset \tilde{S}$ and $|S_1| < |\tilde{S}|$. Then $\tilde{S} \cup \{\tilde{e}\} \notin F$, hence $\exists\ \tilde{C} \in Z$ with $\tilde{e} \in \tilde{C} \subset \tilde{S} \cup \{\tilde{e}\}$, and furthermore, $\tilde{C} \cap (\tilde{S} - S_1) \neq \emptyset$ as otherwise $\tilde{C} \subset S_1$. Let $e' \in \tilde{C} \cap (\tilde{S} - S_1)$, then $(\tilde{S} - \{e'\}) \cup \{\tilde{e}\} \in F$: this follows as in (i). But $S_1 \subset (\tilde{S} - \{e'\}) \cup \{\tilde{e}\}$ and $|S_1| < |(\tilde{S} - \{e'\}) \cup \{\tilde{e}\}| = |\tilde{S}|$, contradiction.

(iii) S_3 and S_2 are maximal independent subsets of S, and if $S_3 = S_2$, then $|S_1| = |S_2|$. If $S_3 \neq S_2$, we note that $|S_3 \triangle S_2| < |S_1 \triangle S_2|$, (cf. Remark (2)). Repeating the above a finite number of times thus gives rise to a maximal independent subset S_n of S with $S_n = S_2$, hence $|S_1| = |S_2|$.

<u>Corollary</u>. By Theorem 5 and statement (*) of Remark (1) it follows that the circuit-axiomatic definition of a matroid is equivalent to the earlier axiomatic definitions.

§1.5. The Basis-Axiomatic Definition of a Matroid.

<u>Definitions</u>.

(a) Let E be a finite set and W a family of subsets of E. Then the pair (E,W) is a <u>matroid</u> M(E,W), and the elements of W are the <u>bases</u> of M(E,W), if the following conditions hold:

(W1) $\bigwedge S, S' \subset E \quad [(S \subset S' \in W \wedge S \neq S') \Longrightarrow S \notin W]$,

(W2) $\bigwedge B, B' \in W \quad \bigwedge e \in B \quad \exists\ e' \in B' : (B - \{e\}) \cup \{e'\} \in W$.

(b) A matroid $M(E,W)$ is <u>normal</u> if $\bigwedge e \in E \quad \exists\ B \in W$ with $e \in B$.

(c) Let $M(E,W)$ be a matroid. A subset $S \subset E$ is called <u>independent</u> if $\exists\ B \in W$ with $S \subset B$. We shall denote by F the family of independent sets of $M(E,W)$. Clearly the bases of $M(E,W)$ are the maximal independent sets of $M(E,W)$.

<u>Remarks</u>. It follows immediately that every matroid $M(E,r)$ is a matroid $M(E,W)$. The following theorem establishes that every matroid $M(E,W)$ is a matroid $M(E,F)$. We first prove a lemma.

<u>Lemma</u>. $\bigwedge B, B' \in W \qquad |B| = |B'|$.

<u>Proof</u>. Suppose $B \neq B'$, then $B-B' \neq \emptyset$ and $B'-B \neq \emptyset$ by axiom (W1). Let $e \in B-B'$. Then by axiom (W2) $\exists\ e' \in B'-B$ such that $B'' := (B-\{e\}) \cup \{e'\} \in W$. Note that $|B''| = |B|$. If $B'' \subset B'$, then $B'' = B'$ by axiom (W1). If $B'' \not\subset B'$, we note that $|B'' \Delta B'| < |B \Delta B'|$, (cf. Remark (2) of §1.4). Repeating the above a finite number of times thus gives rise to a basis $\tilde{B}$ with $\tilde{B} \subset B'$, i.e. $\tilde{B} = B'$, hence $|B| = |B'|$.

<u>Theorem 6</u>. The matroid $M(E,W)$ satisfies the axioms (F1) - (F3).

<u>Proof</u>. Axioms (F1) and (F2) follow immediately.

Axiom (F3):- Let S_1 and S_2 be distinct maximal independent subsets of S. Then $\exists\ B_i \in W$ such that $S_i = B_i \cap S$, $i=1,2$. Suppose $|S_1| < |S_2|$.

(<u>i</u>) $(B_1-B_2)-S \neq \emptyset$: Suppose not, i.e. $B_1 \subset S \cup B_2$. Then

$$|S_2-S_1| = |(B_2-B_1) \cap S| \leqslant |B_2-B_1| = |B_1-B_2| \text{ by the above lemma,}$$
$$= |(B_1-B_2) \cap S| = |S_1-S_2| ,$$

which contradicts $|S_1| < |S_2|$.

(ii) We now use axiom (W2) to replace every point of $(B_1-B_2)-S$ stepwise by a point of B_2-B_1 and thus obtain a basis $\tilde{B}$ with the properties $S_1 \subset \tilde{B} \cap S$ and $\tilde{B} \cap (S_2-S_1) \neq \emptyset$, for

$|S_1| < |S_2| \Longrightarrow |(B_1-B_2) \cap S| = |S_1-S_2| < |S_2-S_1| =$

$= |(B_2-B_1) \cap S| \Longrightarrow |(B_1-B_2) - S| > |(B_2-B_1) - S|$.

Hence $S_1 \neq \tilde{B} \cap S$, which contradicts the fact that S_1 is maximal independent in S.

<u>Corollary</u>. By Theorem 6 and Remark (c) it follows that the basis-axiomatic definition of a matroid is equivalent to the earlier axiomatic definitions.

Chapter II. Further Properties of Matroids.

§2.1. The Span Mapping $\mathcal{S}$.

Definitions. Let M be a matroid on the finite set E. The span mapping

$$\mathcal{S} : \mathfrak{P}(E) \longrightarrow \mathfrak{P}(E)$$

is defined as follows:

$$\mathcal{S}(S) := \{e \in E : r(S \cup \{e\}) = r(S)\} \quad , \quad S \subset E.$$

Clearly (a) $\bigwedge S \subset E \quad S \subset \mathcal{S}(S)$,

(b) $\mathcal{S}(\emptyset) = \{e \in E : r(\{e\}) = 0\}$,

(c) M is normal if and only if $\mathcal{S}(\emptyset) = \emptyset$.

$\mathcal{S}(S)$, which we shall also denote by $\overline{S}$, is called the span of S. A subset $S \subset E$ is called spanning if $\overline{S} = E$.

Theorem 7. Let M be a matroid on the finite set E.

(a) $\bigwedge S \subset E \quad r(\overline{S}) = r(S)$,

(b) $\bigwedge S \subset E \quad \overline{\overline{S}} = \overline{S}$,

(c) $\bigwedge S, S' \subset E \quad [S \subset S' \Longrightarrow \overline{S} \subset \overline{S'}]$,

in particular: $\bigwedge S, S' \subset E$

$[(S \subset S' \wedge S \text{ is spanning}) \Longrightarrow S' \text{ is spanning}]$,

Corollaries. (1) $\bigwedge S, S' \subset E \quad [S \subset \overline{S'} \Longrightarrow \overline{S} \subset \overline{S'}]$,

(2) $\bigwedge S \subset E \quad \overline{S} = \bigcap_{S \subset S' \in \operatorname{Im} \mathcal{S}} S'$,

(d) Let I be an index set and $S_i \subset E$, $i \in I$. Then

(1) $\overline{\bigcap_{i\in I} S_i} \subset \bigcap_{i\in I} \overline{S_i}$,

(2) $(\bigwedge i \in I \quad S_i \in \operatorname{Im}\varphi) \Longrightarrow \bigcap_{i\in I} S_i \in \operatorname{Im}\varphi$,

(3) $\overline{\bigcup_{i\in I} S_i} = \overline{\bigcup_{i\in I} \overline{S_i}}$,

(e) $\bigwedge S,S' \subset E \quad [(S \subset S' \wedge r(S) = r(S')) \Longrightarrow \overline{S} = \overline{S'}]$,

<u>Corollary</u>. $\bigwedge S \subset E \quad [S \text{ is spanning} \Longleftrightarrow r(S) = r(E)]$,

(f) $\bigwedge S \subset E \quad [S \in Z \Longleftrightarrow ((\bigwedge e \in S \quad e \in \overline{S-\{e\}}) \wedge r(S) = |S|-1)]$,

(g) $\bigwedge S \subset E \quad \bigwedge e \in E-S$

$[e \in \overline{S} \Longleftrightarrow (\exists\, C \in Z : e \in C \subset S \cup \{e\})$ or equivalently

$\Longleftrightarrow (\exists\, S' \in F : S' \subset S \wedge S' \cup \{e\} \notin F)]$, ††

<u>Corollary</u>. $\bigwedge S \subset E \quad \bigwedge e \in E-S$

$[(e \in \overline{S} \wedge \bigwedge e' \in S \quad e \notin \overline{S-\{e'\}}) \Longrightarrow S \cup \{e\} \in Z]$,

(h) $\bigwedge S \subset E \quad \bigwedge e,e' \in E$

$[(e \notin \overline{S} \wedge e \in \overline{S \cup \{e'\}}) \Longrightarrow e' \in \overline{S \cup \{e\}}]$,

(i) $\bigwedge S \subset E \quad [S \in F \Longleftrightarrow (\bigwedge e \in S \quad e \notin \overline{S-\{e\}})$ or equivalently

$\Longleftrightarrow$ (S is minimal† in $\{S' \subset E : \overline{S'} = \overline{S}\}$)] ,

---

† cf. Definition (5) of §1.1.

†† The implication $\Longleftarrow$ of the first equivalence is true for $e \in E$.

(j) $\bigwedge S, S' \subset E$

$[(S$ is a maximal independent subset of $S')$

$\Longleftrightarrow (S$ is minimal[†] in $\{S'' \subset S' : \overline{S''} = \overline{S'}\})$

$\Longleftrightarrow (S \in F \wedge S \subset S' \subset \overline{S})]$,

<u>in particular</u> $(S' = E)$:

$[(S$ is basis$) \Longleftrightarrow (S$ is a minimal spanning set$)$

$\Longleftrightarrow (S$ is independent and spanning$)]$,

<u>Corollary</u>. $\bigwedge S \subset E$

$[(S$ is spanning $) \Longleftrightarrow (\exists B \in W : B \subset S) \Longleftrightarrow (r(S) = r(E))]$,

(k) $\bigwedge S \in F \quad \bigwedge$ spanning set $S' \subset E$ with $S \subset S' \quad \exists \; B \in W$

with $S \subset B \subset S'$.

<u>Proof</u>.

(a) Trivial if $S = \overline{S}$. Suppose $S \neq \overline{S}$. Then $\bigwedge e \in \overline{S}-S$
$r(S \cup \{e\}) = r(S)$, hence by the corollary of Theorem 1(e),
$r(\overline{S}) = r(S \cup (\overline{S}-S)) = r(S)$.

(b) Let $e \in \overline{\overline{S}}$, i.e. $r(\overline{S} \cup \{e\}) = r(\overline{S})$. Then by (a)
$r(S) = r(\overline{S}) = r(\overline{S} \cup \{e\}) \geqslant r(S \cup \{e\}) \geqslant r(S)$,
hence $r(S \cup \{e\}) = r(S)$, i.e. $e \in \overline{S}$.

† cf. Definition (5) of §1.1.

(c) Let $e \in \overline{S}$, i.e. $r(S \cup \{e\}) = r(S)$. Then by the submodular inequality

$$r(S') + r(S \cup \{e\}) \geqslant r(S' \cup \{e\}) + [r(S \cup \{e\}) \text{ or } r(S)],$$

hence $r(S' \cup \{e\}) = r(S')$, i.e. $e \in \overline{S'}$.

Corollaries: (1) follows immediately from (b) and (c).

(2): $S \subset S' \in \mathrm{Im}(\varphi) \Longrightarrow \overline{S} \subset S'$ by Corollary (1). On the other hand $\overline{S} \in \{S' \subset E : S \subset S' \in \mathrm{Im}(\varphi)\}$.

(d) (1) $\bigwedge j \in I \quad \bigcap_{i \in I} S_i \subset S_j$, hence $\bigwedge j \in I \quad \overline{\bigcap_{i \in I} S_i} \subset \overline{S_j}$ by (c).

(2) $\overline{\bigcap_{i \in I} S_i} \subset \bigcap_{i \in I} \overline{S_i} = \bigcap_{i \in I} S_i$ by (1) and (b),

hence $\overline{\bigcap_{i \in I} S_i} = \bigcap_{i \in I} S_i$.

(3) $\bigwedge j \in I \quad S_j \subset \bigcup_{i \in I} S_i$, hence by (c) $\bigwedge j \in I \quad \overline{S_j} \subset \overline{\bigcup_{i \in I} S_i}$,

i.e. $\bigcup_{i \in I} \overline{S_i} \subset \overline{\bigcup_{i \in I} S_i}$, hence by Corollary (1) of (c),

$\overline{\bigcup_{i \in I} \overline{S_i}} \subset \overline{\bigcup_{i \in I} S_i}$. On the other hand $\bigcup_{i \in I} S_i \subset \bigcup_{i \in I} \overline{S_i}$, hence

by (c) $\overline{\bigcup_{i \in I} S_i} \subset \overline{\bigcup_{i \in I} \overline{S_i}}$.

(e) By (c) $\overline{S} \subset \overline{S'}$. Let $e \in \overline{S'}$, then

$r(S \cup \{e\}) \leqslant r(S' \cup \{e\}) = r(S') = r(S)$, hence

$r(S \cup \{e\}) = r(S)$, i.e. $e \in \overline{S}$.

(f) Follows immediately from Theorem 1(d) and the definition of φ.

(g) $\Longrightarrow$: $\exists\ S' \in F$ with $S' \subset S$ and $r(S) = r(S')$. As $e \in \overline{S}$,

$r(S) = r(S') \leqslant r(S' \cup \{e\}) \leqslant r(S \cup \{e\}) = r(S)$,

i.e. $r(S' \cup \{e\}) = r(S')$ or $S' \cup \{e\} \notin F$ as $e \notin S'$.

$\Longleftarrow$: $r(S' \cup \{e\}) = r(S')$, hence $e \in \overline{S'} \subset \overline{S}$ by (c).

Corollary: By (g) $\exists\ C \in Z$ with $e \in C \subset S \cup \{e\}$. Suppose $(S \cup \{e\}) - C \neq \emptyset$ and take $e' \in (S \cup \{e\}) - C$. Then $e' \neq e$, i.e. $e' \in S$, hence $e \in C \subset (S - \{e'\}) \cup \{e\}$ and thus by (g) $e \in \overline{S - \{e'\}}$, contradiction.

(h) Trivial if $e = e'$. Suppose $e \neq e'$. Clearly we need only consider the case $e' \notin S$. $e \notin S$ as $e \notin \overline{S}$, therefore $e \notin S \cup \{e'\}$, hence by (g) $\exists\ C \in Z$ with $e \in C \subset S \cup \{e, e'\}$. Furthermore, $e' \in C$ as otherwise $e \in C \subset S \cup \{e\}$ and thus by (g) $e \in \overline{S}$. Hence, again by (g), $e' \in \overline{S \cup \{e\}}$.

(i) Follows immediately by the corollary of Theorem 1(f).

(j) The first statement is equivalent to:
$(S \subset S' \wedge S \in F \wedge r(S) = r(S'))$.
By (a) and (e) the second statement is equivalent to:
$(S \subset S' \wedge r(S) = r(S') \wedge S$ is minimal in $\{S'' \subset E : \overline{S''} = \overline{S}\})$
or $(S \subset S' \wedge r(S) = r(S') \wedge S \in F)$ by (i).
By (a) - (c) and (e) the third statement is equivalent to
$(S \in F \wedge S \subset S' \wedge r(S) = r(S'))$.

(k) Let S'' be a maximal independent subset of S' with $S \subset S''$. Then $|S''| = r(S') = r(E)$ by the corollary of (j), i.e. $S'' \in W$.

§2.2. The Span-Axiomatic Definition of a Matroid.

Definitions.

(a) Let E be a finite set and $\mathcal{S}$ a mapping $\mathcal{S}: \mathfrak{P}(E) \longrightarrow \mathfrak{P}(E)$. Then the pair $(E,\mathcal{S})$ is a matroid $M(E,\mathcal{S})$, and $\overline{S} := \mathcal{S}(S)$ is the span of $S \subset E$, if the following conditions hold:

($\mathcal{S}$1) $\bigwedge S \subset E \quad S \subset \overline{S}$,

($\mathcal{S}$2) $\bigwedge S,S' \subset E \quad [S \subset \overline{S'} \Longrightarrow \overline{S} \subset \overline{S'}]$,

($\mathcal{S}$3) $\bigwedge S \subset E \quad \bigwedge e,e' \in E$
$[(e \notin \overline{S} \wedge e \in \overline{S \cup \{e'\}}) \Longrightarrow e' \in \overline{S \cup \{e\}}]$.

(b) A matroid $M(E,\mathcal{S})$ is normal if $\overline{\emptyset} = \emptyset$.

Remarks and Further Definitions. Let $M(E,\mathcal{S})$ be a matroid.

(1) Axioms ($\mathcal{S}$1) and ($\mathcal{S}$2) imply: $\bigwedge S,S' \subset E \quad [S \subset S' \Longrightarrow \overline{S} \subset \overline{S'}]$ and $\overline{\overline{S}} = \overline{S}$ (as $\overline{S} \subset \overline{S} \Longrightarrow \overline{\overline{S}} \subset \overline{S}$ by ($\mathcal{S}$2)).
Conversely, these two properties imply axiom ($\mathcal{S}$2), hence they can be substituted for ($\mathcal{S}$2) in the above definition.

(2) A subset $S \subset E$ is called independent if $\bigwedge e \in S \quad e \notin \overline{S - \{e\}}$.
We shall denote by F the family of independent sets of $M(E,\mathcal{S})$.
Note that $\emptyset \in F$.

(3) The axioms ($\mathcal{S}$1) - ($\mathcal{S}$3) imply the following lemma:

Lemma. $\bigwedge S,S' \subset E$
$[(S \text{ is a maximal independent subset of } S') \Longrightarrow \overline{S} = \overline{S'}]$.

Proof. Trivial if $S = S'$. Suppose $S \neq S'$. By Remark (1) $\overline{S} \subset \overline{S'}$. Now let $e \in S'-S$, then $S \cup \{e\} \notin F$. Hence by Remark (2) $\exists\ \tilde{e} \in S \cup \{e\}$ with $\tilde{e} \in \overline{(S \cup \{e\}) - \{\tilde{e}\}}$. If $\tilde{e} = e$, then $e \in \overline{S}$. If $\tilde{e} \neq e$, then $\tilde{e} \in S$, but $\tilde{e} \notin \overline{S-\{\tilde{e}\}}$ by Remark (2) as $S \in F$. Therefore $\tilde{e} \notin \overline{S-\{\tilde{e}\}}$, $\tilde{e} \in \overline{(S \cup \{e\}) - \{\tilde{e}\}}$, hence by ($\varphi$3) $e \in \overline{S}$. Thus $S' \subset \overline{S}$, hence by (φ2) $\overline{S'} \subset \overline{S}$.

(4) The axioms (φ1) - (φ3) imply: $\bigwedge S \subset E \quad \bigwedge e \in E-S$

$$[e \in \overline{S} \iff (\exists S' \in F : S' \subset S \wedge S' \cup \{e\} \notin F)] .$$

Proof. $\Longleftarrow$: Let $e \in E-S$ and $S \supset S' \in F$ with $S' \cup \{e\} \notin F$. Then by Remark (2) $\exists\ \tilde{e} \in S' \cup \{e\}$ with $\tilde{e} \in \overline{(S' \cup \{e\}) - \{\tilde{e}\}}$, and as in the proof of the lemma $e \in \overline{S'}$, and $\overline{S'} \subset \overline{S}$ by Remark (1), hence $e \in \overline{S}$.
$\Longrightarrow$: Let $e \in \overline{S}-S$ and S' a maximal independent subset of S. Then by the lemma $\overline{S'} = \overline{S}$. If $S' \cup \{e\} \in F$, then by Remark (2) $e \notin \overline{S'} = \overline{S}$, contradiction, hence $S' \cup \{e\} \notin F$.

(5) It follows immediately that every matroid $M(E,r)$ is a matroid $M(E,\varphi)$. The following theorem establishes that every matroid $M(E,\varphi)$ is a matroid $M(E,F)$:

Theorem 8. The matroid $M(E,\varphi)$ satisfies the axioms (F1) - (F3).

Proof. Axiom (F1) is clearly satisfied.

Axiom (F2):- Let $S \subset S' \in F$. Then by Remark (2) $\bigwedge e \in S'$, in particular $\bigwedge e \in S$, $e \notin \overline{S'-\{e\}}$. But $S-\{e\} \subset S'-\{e\}$, hence by Remark (1) $\overline{S-\{e\}} \subset \overline{S'-\{e\}}$ and thus $\bigwedge e \in S \quad e \notin \overline{S-\{e\}}$, i.e. $S \in F$.
Axiom (F3):- Let S_1 be a maximal independent subset of S and S' an independent subset of S with $S' \not\subset S_1$. Clearly $S_1 \not\subset S'$. Take $e \in S'-S_1$, then $S'-\{e\} \in F$ by axiom (F2). Now $\exists\ e' \in S_1 - S'$ such that $S'' := (S'-\{e\}) \cup \{e'\} \in F$, as otherwise $S'-\{e\}$ is maximal

independent in $(S'-\{e\})\cup S_1$, hence by the above lemma $\overline{S'-\{e\}} = \overline{(S'-\{e\})\cup S_1} \supset \overline{S_1} = \overline{S}$, i.e. $\overline{S'-\{e\}} = \overline{S}$, hence $e \in \overline{S'-\{e\}}$, i.e. $S' \notin F$, contradiction.

If $S'' \subset S_1$, then $|S'| = |S''| \leqslant |S_1|$. If $S'' \not\subset S_1$, we note that $|S'' \triangle S_1| < |S' \triangle S_1|$, (cf. Remark (2) of §1.4). Repeating the above a finite number of times thus gives rise to an independent subset $\tilde{S}$ of S with $\tilde{S} \subset S_1$, hence $|S'| = |\tilde{S}| \leqslant |S_1|$.
Now if S_2 is another maximal independent subset of S, then taking $S' = S_2$ gives $|S_2| \leqslant |S_1|$. Similarly $|S_1| \leqslant |S_2|$, hence $|S_1| = |S_2|$.

Corollary. By Theorem 8 and Remark (4) it follows that the span-axiomatic definition of a matroid is equivalent to the earlier axiomatic definitions.

§2.3. Hyperplanes and Cocircuits.

Definitions. Let M be a matroid on the finite set E.

(1) A subset $S \subset E$ is a hyperplane of M if $S = \overline{S}$ and $r(S) = r(E) - 1$.

(2) A subset $S \subset E$ is a cocircuit of M if E-S is a hyperplane of M. We shall denote by Z^* the family of cocircuits of M. Clearly $\emptyset \notin Z^*$. This notation is motivated by properties of the "dual matroid" defined in §2.4.

Theorem 9. Let M be a matroid on the finite set E.

(a) $\bigwedge S \subset E$

$[(S \text{ is hyperplane})$

$\Longleftrightarrow (\bigwedge e \in E-S \quad r(S \cup \{e\}) = r(S)+1 = r(E))$

$\Longleftrightarrow (S \text{ is not spanning but } \bigwedge e \in E-S \quad S \cup \{e\} \text{ is spanning})$

$\Longleftrightarrow (S \text{ is maximal}^{\dagger} \text{ in } \{S' \subset E : S' = \overline{S'} \neq E\})]$,

Corollaries. (1) $\bigwedge S, S' \in Z^* \quad [S \subset S' \Longrightarrow S = S']$,

(2) $\bigwedge S \subset E \quad [(\overline{S} \text{ is hyperplane}) \Longleftrightarrow (S \text{ is not spanning but}$

$\exists \; e \in E-S : S \cup \{e\} \text{ is spanning})]$,

(b) $\bigwedge S \subset E \quad \bigwedge e \in E$

$[e \notin S = \overline{S} \Longrightarrow (\exists \text{ hyperplane } S' \text{ with } S \subset S' \subset E-\{e\})]$,

Corollary. $\bigwedge S, S' \subset E$

$[(S = \overline{S} \wedge S' = \overline{S'} \wedge S' \subset S \wedge r(S)-r(S') = 1) \Longrightarrow$

$(\exists \text{ hyperplane } S'' \text{ with } S' = S \cap S'')]$,

(c) $\bigwedge S \subset E$

$[(S = \overline{S} \neq E)$

$\Longleftrightarrow (\exists \; n \in \mathbb{N}_+ \text{ and } \exists \text{ hyperplanes } S_1, S_2, \ldots, S_n \text{ with}$

$S = S_1 \cap S_2 \cap \ldots \cap S_n)$, <u>in particular</u>:

$\Longleftrightarrow (\exists \text{ distinct hyperplanes } S_1, S_2, \ldots, S_m, \text{ where}$

$m := r(E)-r(S), \text{ with } S = S_1 \cap S_2 \cap \ldots \cap S_m)]$,

(d) $\bigwedge S \subset E \quad [(S \text{ is spanning}) \Longleftrightarrow (\bigwedge S' \in Z^* \quad S \cap S' \neq \emptyset)]$,

---

† cf. Definition (5) of §1.1.

(e) $\bigwedge S \subset E \quad [(\exists\, S' \in Z^* \text{ with } S' \subset S) \Longleftrightarrow (\bigwedge B \in W \quad B \cap S \neq \emptyset)]$,

(f) $\bigwedge S \subset E \quad [S = \overline{S} \Longleftrightarrow (\bigwedge C \in Z \quad |C-S| \neq 1)]$,

<u>Corollary</u>. $\bigwedge S \subset E \quad [(\exists\, n \in \mathbb{N}_+ \text{ and } \exists\, S_1, S_2, \ldots, S_n \in Z^* \text{ with}$

$S = S_1 \cup S_2 \cup \ldots \cup S_n) \Longleftrightarrow (S \neq \emptyset \wedge \bigwedge C \in Z \quad |S \cap C| \neq 1)]$,

(g) $\bigwedge S \subset E$

$[S \in Z^*$

$\Longleftrightarrow (S \neq \emptyset \wedge (\bigwedge C \in Z \quad |S \cap C| \neq 1) \wedge (\bigwedge e, e' \in S \text{ with}$

$e \neq e' \quad \exists\, C \in Z : S \cap C = \{e, e'\}))$

$\Longleftrightarrow (S$ is minimal† in $\{S' \subset E : S' \neq \emptyset \wedge \bigwedge C \in Z \quad |S' \cap C| \neq 1\})$

$\Longleftrightarrow ((\bigwedge B \in W \quad B \cap S \neq \emptyset) \wedge (\bigwedge e \in S \quad \exists\, B \in W : B \cap S = \{e\}))$

$\Longleftrightarrow (S$ is minimal† in $\{S' \subset E : \bigwedge B \in W \quad B \cap S' \neq \emptyset\})]$,

(h) $\bigwedge S \subset E \quad \bigwedge e \in S$

$[(S$ is spanning and $S - \{e\}$ is not spanning$) \Longrightarrow$

$(\exists$ unique $S' \in Z^* : (S - \{e\}) \cap S' = \emptyset$ (clearly $e \in S'$))] ,

(i) (α) $\bigwedge B \in W \quad \bigwedge e \in E-B \quad \exists$ unique $C \in Z : C \subset B \cup \{e\}$,

(clearly $e \in C$). Then $\bigwedge b \in B$

$[(B - \{b\}) \cup \{e\} \in W \Longleftrightarrow b \in C]$,

(β) $\bigwedge B \in W \quad \bigwedge b \in B \quad \exists$ unique $S \in Z^* : (B - \{b\}) \cap S = \emptyset$,

(clearly $b \in S$). Then $\bigwedge e \in E-B$

$[(B - \{b\}) \cup \{e\} \in W \Longleftrightarrow e \in S]$,

---

† cf. Definition (5) of §1.1.

(j) Axiom (G-II) of Minty [25]: $\bigwedge S \subset E \quad \bigwedge e \in E-S$

either $\exists\ C \in Z$ with $e \in C \subset S \cup \{e\}$,

or $\exists\ S' \in Z^*$ with $e \in S'$ and $S \cap S' = \emptyset$.

<u>Proof</u>.

(a) The first equivalence is clear. The second and third statements are equivalent by the corollary of Theorem 7(e).

Fourth statement: let $A := \{S' \subset E : S' = \overline{S'} \neq E\}$ and take $S' \in A$ and $e \in E-S'$. Then by the corollary of Theorem 7(e) $r(S') \leqslant r(E)-1$, and $r(S' \cup \{e\}) = r(S')+1 \leqslant r(E)$, hence $\overline{S' \cup \{e\}} \in A$ if

$r(S') < r(E)-1$, and S' is maximal in A if $r(S') = r(E)-1$. Thus

(S is maximal in A) $\Longleftrightarrow$ (S is hyperplane).

Corollaries: (1) Clear.
(2) $\Longrightarrow$: Follows by (a) and Theorem 7(b), (d(3)).
$\Longleftarrow$: By the corollary of Theorem 7(e) $r(S) < r(E)$ and $r(S \cup \{e\}) = r(E) = r(S)+1$, hence by Theorem 7(a)
$r(\overline{S}) = r(S) = r(E)-1$.

(b) Let S' be maximal in $B := \{S'' \subset E-\{e\} : \overline{S''} = S''\}$. Note that $B \neq \emptyset$ as $S \in B$. Then S' is also maximal in $\{S'' \subset E : S'' \neq E \wedge \overline{S''} = S''\}$, i.e. S' is a hyperplane by (a), for (S' maximal in B) $\Longrightarrow$
$(\bigwedge e' \in E-(S' \cup \{e\}) \quad e \in \overline{S' \cup \{e'\}}) \Longrightarrow$ with Theorem 7(h)
$(\bigwedge e' \in E-(S' \cup \{e\}) \quad e' \in \overline{S' \cup \{e\}})$, i.e. $\overline{S' \cup \{e\}} = E$, hence
$\bigwedge e' \in E-S' \quad \overline{S' \cup \{e'\}} = E$ (because $\bigwedge e' \in E-(S' \cup \{e\})$
$e \in \overline{S' \cup \{e'\}}$, hence $E = \overline{S' \cup \{e\}} \subset \overline{S' \cup \{e'\}}$).

Corollary: Clearly $S' \neq S$ and $\exists\ e \in S-S'$ such that

$r(S' \cup \{e\}) = r(S)$. Then by (b) $\exists$ hyperplane S'' with

$S' \subset S'' \subset E-\{e\}$. Clearly $S' \subset S \cap S''$. By the submodular inequality

$r(S) + (r(E)-1) = r(S) + r(S") \geqslant r(E) + r(S \cap S")$, i.e.
$r(S \cap S") \leqslant r(S')$, hence $r(S \cap S") = r(S')$, and thus by Theorem 7 (d(2)), (e) $S' = S \cap S"$.

(c) $\Longleftarrow$: Follows immediately by Theorem 7(d(2)).
$\Longrightarrow$: Let $E-S =: \{e_1, e_2, \ldots, e_n\}$. By (b) $\bigwedge i \in \{1,\ldots,n\}$ $\exists$ hyperplane S_i with $S \subset S_i \subset E-\{e_i\}$. Then $S = S_1 \cap \ldots \cap S_n$.
Special Case: (Welsh [33]) $\exists$ $S' \in F$ with $S' \subset S$ and $r(S') = r(S)$, and $\exists$ $B \in W$ with $S' \subset B$. Let $B-S' =: \{e_1, e_2, \ldots, e_m\}$, $A_1 := S$, and $\bigwedge i \in \{1,\ldots,m-1\}$ $A_{i+1} := \overline{S' \cup \{e_1,\ldots,e_i\}}$. Clearly $A_m = \overline{B-\{e_m\}}$ is a hyperplane S_m. By the corollary to (b) $\bigwedge i \in \{1,\ldots,m-1\}$ $\exists$ hyperplane S_i with $A_i = A_{i+1} \cap S_i$. Thus $A_1 = \bigcap_{i=1}^{m} S_i$, and the S_i are distinct as $\bigwedge i \in \{1,\ldots,m-1\}$ $e_i \notin S_i$ but $e_i \in S_{i+1}, S_{i+2}, \ldots, S_m$.

(d) S is spanning $\Longleftrightarrow$ by (b) no hyperplane contains S $\Longleftrightarrow$ every cocircuit intersects S.

(e) E-S contains a basis $\Longleftrightarrow$ E-S is spanning by the corollary of Theorem 7(j) $\Longleftrightarrow$ by (d) every cocircuit intersects E-S $\Longleftrightarrow$ S contains no cocircuits.

(f) Follows immediately by Theorem 7(g).
Corollary: Follows immediately by (c) and (f).

(g) By the corollary of (f) and Corollary (1) of (a) the first and third statements are equivalent.
By (e) and Corollary (1) of (a) the first and fifth statements are equivalent.

The fourth statement $\Longleftrightarrow$ $((\bigwedge B \in W \quad B \cap S \neq \emptyset) \wedge (\bigwedge e \in S \; \exists \; B \in W :$ $B \cap (S-\{e\}) = \emptyset))$ $\Longleftrightarrow$ the fifth statement.

If $|S| = 1$, the second and third statements are trivially equivalent. Suppose now that $|S| \geq 2$.

The second statement $\Longrightarrow$

$$(S \neq \emptyset \wedge (\bigwedge C \in Z \quad |S \cap C| \neq 1) \wedge (\bigwedge e \in S \; \exists \; C \in Z : |(S-\{e\}) \cap C| = 1)),$$

which is equivalent to the third statement. It remains to prove the reverse implication.

Let S be minimal in $\{S' \subset E : S' \neq \emptyset \wedge \bigwedge C \in Z \quad |S' \cap C| \neq 1\}$ and let $T \subset E$ be maximal in

$D := \{S' \subset S : \bigwedge e,e' \in S'$ with $e \neq e' \; \exists \; C \in Z : S \cap C = \{e,e'\}\}$.

$D \neq \emptyset$ as for $\tilde{e} \in S \; \exists \; \tilde{C} \in Z$ and $\exists \; \tilde{e}' \in E$ such that $(S-\{\tilde{e}\}) \cap \tilde{C} = \{\tilde{e}'\}$ by the minimality of S, hence $S \cap \tilde{C} = \{\tilde{e}, \tilde{e}'\}$, i.e. $\{\tilde{e}, \tilde{e}'\} \in D$.

Suppose $S-T \neq \emptyset$. As $S-T \neq S$, $\exists \; C \in Z$ and $\exists \; e \in E$ such that $(S-T) \cap C = \{e\}$ by the minimality of S, but $S \cap C \neq \{e\}$, thus $\exists \; e_1, e_2, \ldots, e_k \in T$, $k \geq 1$, with $S \cap C = \{e, e_1, \ldots, e_k\}$.

Let $i \in \{1, \ldots, k-1\}$, then as $T \in D \; \exists \; C_i \in Z : S \cap C_i = \{e_i, e_k\}$, hence by Theorem 1(j) applied to C and C_i, $\exists \; \tilde{C}_i \in Z$: $e \in S \cap \tilde{C}_i \subset \{e, e_1, \ldots, e_{k-1}\}$, and $|S \cap \tilde{C}_i| \geq 2$. We repeat this step with $\tilde{C}_i$ instead of C and continue in this way until we have a $\tilde{C} \in Z$ and a $j \in \{1, \ldots, k-1\}$ with $S \cap \tilde{C} = \{e, e_j\}$.

Now let $e' \in T-\{e_j\}$, then as $T \in D \; \exists \; C' \in Z : S \cap C' = \{e', e_j\}$, hence by Theorem 1(j) applied to $\tilde{C}$ and C' $\exists \; C'' \in Z$: $e \in S \cap C'' \subset \{e, e'\}$, i.e. $S \cap C'' = \{e, e'\}$. Thus $T \cup \{e\} \in D$, contradicting the maximality of T in D.

(h) By Corollary (2) of (a) $\overline{S-\{e\}}$ is a hyperplane. Let $S' := E - \overline{S-\{e\}}$, then $S' \in Z^*$ and $(S-\{e\}) \cap S' = \emptyset$. Suppose $\tilde{S}$ is a hyperplane containing $S-\{e\}$, then $\overline{S-\{e\}} \subset \tilde{S}$, hence $\tilde{S} = \overline{S-\{e\}}$ by (a).

(i) (α): The initial statement follows by Theorem 1(k) applied to B and e.

$\Longrightarrow$: $(B-\{b\})\cup\{e\}\in F$ but $B\cup\{e\} = ((B-\{b\})\cup\{e\})\cup\{b\}\notin F$, hence $\exists\ C'\in Z : b\in C'\subset B\cup\{e\}$. By the initial statement $C' = C$, i.e. $b\in C$.

$\Longleftarrow$: $(B-\{b\})\cup\{e\}\in F$ (and hence $\in W$ as $|(B-\{b\})\cup\{e\}| = |B|$), as otherwise $\exists\ C'\in Z : C'\subset(B-\{b\})\cup\{e\}\subset B\cup\{e\}$ and $C'\neq C$ as $b\notin C'$, which contradicts the uniqueness of C.

(β): The initial statement follows by the special case of Theorem 7(j) and by (h) applied to B and b.

$\Longrightarrow$: $(B-\{b\})\cup\{e\}$ is spanning but $B-\{b\} = ((B-\{b\})\cup\{e\})-\{e\}$ is not, hence by (d) $\exists\ S'\in Z^* : (B-\{b\})\cap S' = \emptyset$ and $e\in S'$. By the initial statement $S' = S$, i.e. $e\in S$.

$\Longleftarrow$: $(B-\{b\})\cup\{e\}$ is spanning (and hence contains a basis by the corollary of Theorem 7(j), and is thus itself a basis as $|(B-\{b\})\cup\{e\}| = |B|$), as otherwise by (d) $\exists\ S'\in Z^*$: $((B-\{b\})\cup\{e\})\cap S' = \emptyset$, hence $(B-\{b\})\cap S' = \emptyset$, and $S'\neq S$ as $e\notin S'$, which contradicts the uniqueness of S.

(j) Either $e\in\overline{S}$ or $e\notin\overline{S}$. The result then follows by Theorem 7(g) and Theorem 9(b).

§2.4. The Dual Matroid.

Theorem 10. Let M be a matroid on the finite set E. Then the pair (E,W^*) satisfies the axioms (W1) and (W2) and is thus a matroid $M^* := M(E,W^*)$, the dual matroid of M. The bases of M^* are the elements of W^*, i.e. the cobases of M.

Proof. Axiom (W1): We have for M : $\bigwedge S \subset E \quad \bigwedge B \in W$ $[(B \subset S \wedge B \neq S) \Longrightarrow S \notin W]$, or equivalently: $\bigwedge S' \subset E \quad \bigwedge S'' \in W^*$ $[(S' \subset S'' \wedge S' \neq S'') \Longrightarrow S' \notin W^*]$, i.e. (E,W^*) satisfies axiom (W1).
Axiom (W2): Follows from Theorem 2.

Theorem 11. Let M be a matroid on the finite set E and M* its dual matroid.

(a) $\bigwedge S \subset E$

[S is an independent set of M*

$\Longleftrightarrow$ E-S is spanning in M] ,

The family of independent sets of M* is

$$F^* = \{S \subset E : E-S \text{ is spanning in } M\}$$
$$= \{S \subset E : \exists\ B \in W : B \subset E-S\}$$
$$= \{S \subset E : r(E-S) = r(E)\},$$

(b) The rank function r^* of M* is: $\bigwedge S \subset E$

$$r^*(S) = |S| - r(E) + r(E-S) ,$$

in particular, $r(E) + r^*(E) = |E|$,

(c) $\bigwedge S \subset E$ [S is a circuit of M* $\Longleftrightarrow$ $S \in Z^*$] ,

(d) The span mapping $\mathcal{S}^*$ of M* is: $\bigwedge S \subset E$

$$\mathcal{S}^*(S) = S \cup \{e \in E-S : r(E-S) = r((E-S)-\{e\}) + 1\}$$
$$= S \cup \{e \in E-S : e \notin \overline{(E-S)-\{e\}}\} ,$$

in particular, $\bigwedge S \subset E$ [S is spanning in M* $\Longleftrightarrow$ $E-S \in F$] ,

(e) $M^{**} = M$,

(f) $\bigwedge e \in E \quad \bigwedge S, S' \subset E-\{e\}$ with $S \cup S' = E-\{e\}$ and $S \cap S' = \emptyset$, $e \in \varphi(S) \triangle \varphi^*(S')$ (cf. Remark (2) of §1.4).

<u>Proof</u>.

(a) (S independent in M*) $\Longleftrightarrow$ (S is contained in a basis of M*) $\Longleftrightarrow$ (E-S contains a basis of M) $\Longleftrightarrow$ (E-S is spanning in M) $\Longleftrightarrow$ $(r(E-S) = r(E))$.

(b) $\bigwedge S \subset E \quad r^*(S) = \max\{|S \cap S'| : S' \in F^*\}$. Take $S' \in F^*$, then by (a) $\exists\ B \in W : B \subset E-S'$, i.e. $S' \subset E-B$, thus
$|S \cap S'| \leqslant |S \cap (E-B)| = |S| - |S \cap B|$. But
$r(E-S) \geqslant r((E-S) \cap B) = |(E-S) \cap B| = |B| - |S \cap B|$. Hence
$|S \cap S'| \leqslant |S| - |B| + r(E-S) = |S| - r(E) + r(E-S)$. Thus
$r^*(S) \leqslant |S| - r(E) + r(E-S)$.
On the other hand $\exists\ B' \in W : r(E-S) = |(E-S) \cap B'| = |B'-S|$,
and clearly $E-B' \in F^*$. Hence $r^*(S) \geqslant |S \cap (E-B')| = |S| - |S \cap B'| =$
$= |S| - (|B'| - |B'-S|) = |S| - r(E) + r(E-S)$.

(c) By Theorem 9(a) we have $\bigwedge S \subset E$:
$(S \in Z^*) \Longleftrightarrow (\bigwedge e \in S \ \ r((E-S) \cup \{e\}) = r(E-S) + 1 = r(E))$
$\Longleftrightarrow (\bigwedge e \in S \ \ r^*(S-\{e\}) = |S| - 1 = r^*(S)) \Longleftrightarrow$ (S is a circuit of M*) by Theorem 1(d).

(d) $\bigwedge S \subset E \quad \varphi^*(S) := \{e \in E : r^*(S \cup \{e\}) = r^*(S)\} =$
$= S \cup \{e \in E-S : r(E-S) = r((E-S)-\{e\}) + 1\} =$
$= S \cup \{e \in E-S : e \notin \overline{(E-S)-\{e\}}\ \}$.
Special Case: Follows by Theorem 7(i).

(e) Follows immediately from the definition of M**.

(f) By Theorem 7(g) we have: $e \in \mathcal{P}(S) \cap \mathcal{P}^*(S') \Longrightarrow$
$(\exists C \in Z : e \in C \subset S \cup \{e\}) \wedge (\exists \tilde{S} \in Z^* : e \in \tilde{S} \subset S' \cup \{e\}) \Longrightarrow$
$|C \cap \tilde{S}| = 1$, which contradicts Theorem 9(g).
$e \notin \mathcal{P}^*(S') \Longrightarrow e \in \overline{(E-S')-\{e\}} = \overline{S} = \mathcal{P}(S)$.

<u>Theorem 12</u>. Let M be a matroid on the finite set E and M* its dual matroid. Then

$$(M^* \text{ is normal}) \Longleftrightarrow (\bigwedge e \in E \ \exists\ B \in W : e \notin B)$$
$$\Longleftrightarrow (\bigwedge e \in E \ \exists\ C \in Z : e \in C)$$
$$\Longleftrightarrow (\bigwedge e \in E \ \ \{e\} \notin Z^*)$$
$$\Longleftrightarrow (\bigwedge e \in E \ \ E-\{e\} \text{ is spanning in } M) ,$$

i.e. M* is normal if and only if M has one of these four equivalent properties.

<u>Proof</u>. $(M^* \text{ is normal}) \Longleftrightarrow (\bigwedge e \in E \ \exists\ S \in W^* : e \in S) \Longleftrightarrow$ (first property), and
(first property) $\Longrightarrow (\bigwedge e \in E \ \exists\ B \in W : B \cup \{e\} \notin F) \Longrightarrow$
(second property) $\Longrightarrow$ (third property by Theorem 9(g)) $\Longrightarrow$
(fourth property by Theorem 9(d)) $\Longrightarrow$ (first property by the corollary of Theorem 7(j)).

<u>Remarks</u>. The following relations:

S is independent in M* $\Longleftrightarrow$ E-S is spanning in M,

S is a basis in M* $\Longleftrightarrow$ S is a cobasis in M,

S is a circuit in M* $\Longleftrightarrow$ S is a cocircuit in M, together with the formula for r*, enable us to dualise every statement about M, e.g.

the special case of Theorem 7(c)	is dual to	Theorem 1(c),
the special case of Theorem 2	is dual to	Theorem 1(h),
the corollary of Theorem 7(e)	is dual to	the definition of an independent set,
Theorem 9(d)	is dual to	Theorem 1(i(α)),
the corollary of Theorem 7(j) and Theorem 9(e)	are dual to	Theorem 1(i(β)),
Theorem 9(h)	is dual to	Theorem 1(k),
Theorem 9(i(α))	is dual to	Theorem 9(i(β)),

while the special case of Theorem 7(j) and Theorem 7(k) are self-dual.

Chapter III. Examples.

§3.1. Linear Algebraic Examples (Whitney [35]).

Let $\mathbb{F}$ be a field, e.g. the real numbers $\mathbb{R}$ or the ring $\mathbb{Z}_2$ of residue classes of integers modulo 2.

Example 1. Let A be an $(m \times n)$-matrix with coefficients in $\mathbb{F}$ and columns a_i, i.e. $A = (a_1\ a_2\ \dots\ a_n)$. If we put

$E := \{a_1, a_2, \dots, a_n\}$ and $\bigwedge S \subset E$

$r(S) :=$ $\mathbb{F}$-rank of the corresponding submatrix of A,

we have a matroid by the second rank-axiomatic definition, namely the matrix-matroid $M_{\mathbb{F}}(A)$ associated with A.

$M_{\mathbb{F}}(A)$ is normal if and only if $\bigwedge i \in \{1, \dots, n\}$ $a_i \neq 0 \in \mathbb{F}^m$.

Example 2. Let X be a vector space over $\mathbb{F}$. If we put

$E :=$ finite non-empty set of not necessarily distinct vectors $\in X$,

and $\bigwedge S \subset E$ $r(S) := \dim_{\mathbb{F}}(\text{span}_{\mathbb{F}}(S))$,

we have a matroid by the second rank-axiomatic definition, which is normal if and only if $0 \notin E$.

If $X = \mathbb{F}^m$ and $|E| =: n$, $m, n \in \mathbb{N}_+$, we can take E to be the set of columns of an $(m \times n)$-matrix and thus obtain Example 1.

Example 3. Let $n \in \mathbb{N}_+$, and let $e_1, e_2, \dots, e_n$ be the canonical basis of the vector space $\mathbb{F}^n$ and $Y \neq \{0\}$ a vector subspace of $\mathbb{F}^n$. If we put

$E := \{1, 2, \dots, n\}$ and $\bigwedge S \subset E$

$r(S) := \dim_{\mathbb{F}}(\text{projection of } Y \text{ onto } \text{span}_{\mathbb{F}}(\{e_i : i \in S\}))$,

we have a matroid, namely the matroid M_Y associated with Y.

M_Y is normal if and only if Y has the following property:

$\bigwedge i \in \{1, \dots, n\}$ $\dim_{\mathbb{F}}(\text{projection of } Y \text{ onto } \text{span}_{\mathbb{F}}(\{e_i\})) = 1$,

i.e. Y is not contained in a canonical vector subspace $\mathbb{F}^q$, $q < n$, of $\mathbb{F}^n$.

If $Y =: \mathrm{span}_{\mathbb{F}}(\{b_1,b_2,\dots,b_m\})$, $m \in \mathbb{N}_+$, $\bigwedge i \in \{1,\dots,m\}$ $b_i \in \mathbb{F}^n$, and we consider the $(m \times n)$-matrix $\begin{pmatrix} b_1^T \\ \vdots \\ b_m^T \end{pmatrix}$, then we obtain Example 1.

<u>Theorem 13</u>. Let $n \in \mathbb{N}_+$ and X, Y be vector subspaces of $\mathbb{F}^n$ with $\dim_{\mathbb{F}} X =: p \in \{1,2,\dots,n-1\}$ and $\dim_{\mathbb{F}} Y = n-p$. If $Y = X^{\perp}$, then the matroids associated with X and Y are dual.

<u>Proof</u>.

Let $a_1,a_2,\dots,a_p$ be a basis of the vector space X,

and $b_1,b_2,\dots,b_{n-p}$ be a basis of the vector space Y,

i.e. $a_1,\dots,a_p,b_1,\dots,b_{n-p}$ is a basis of the vector space $X \oplus Y = \mathbb{F}^n$. We can suppose without loss of generality (we need only renumber the e_i) that $\{1,2,\dots,p\} \subset E$ is a matroid basis of the matroid M_X associated with X, i.e.

$$p = r_X(\{1,\dots,p\}) = r_X(E) = \dim X \;. \qquad \dots\dots\dots\dots\dots\dots\dots (*)$$

We need to show that $\{p+1,p+2,\dots,n\} \subset E$ is a matroid basis of M_Y.

Let
$$A := \begin{pmatrix} a_1^T \\ \vdots \\ a_p^T \end{pmatrix}_{p\times n} =: \Big(\underset{p\times p}{\tilde{A}} \;\Big|\; \underset{p\times(n-p)}{\tilde{\tilde{A}}} \Big) \;,$$

and
$$B := \begin{pmatrix} b_1^T \\ \vdots \\ b_{n-p}^T \end{pmatrix}_{(n-p)\times n} =: \Big(\underset{(n-p)\times p}{\tilde{B}} \;\Big|\; \underset{(n-p)\times(n-p)}{\tilde{\tilde{B}}} \Big) \;.$$

We have $\bigwedge i,j$ $a_i \perp b_j$ or $\langle a_i, b_j \rangle = 0$, hence

$$0 = AB^T = \big(\tilde{A} \;\big|\; \tilde{\tilde{A}} \big) \begin{pmatrix} \tilde{B}^T \\ \hline \tilde{\tilde{B}}^T \end{pmatrix} = \tilde{A}\tilde{B}^T + \tilde{\tilde{A}}\tilde{\tilde{B}}^T \;,$$

i.e. $\tilde{A}\tilde{B}^T = -\tilde{\tilde{A}}\tilde{\tilde{B}}^T$. By (*) it follows that $\tilde{A}$ is nonsingular, hence $\tilde{B}^T = -\tilde{A}^{-1}\tilde{\tilde{A}}\tilde{\tilde{B}}^T$ or $\tilde{B} = \tilde{\tilde{B}}C$, where $C := -\tilde{\tilde{A}}^T(\tilde{A}^T)^{-1}$, i.e. the columns of $\tilde{B}$ are linear combinations of the columns of $\tilde{\tilde{B}}$, hence $\tilde{\tilde{B}}$ is nonsingular as rank(B) = n-p.

Example 4. Let A be an (m×n)-matrix with coefficients in $\mathbb{F}$ and columns a_i, i.e. $A = (a_1\ a_2\ \dots\ a_n)$, and $M_{\mathbb{F}}(A)$ be the associated matrix-matroid. Let $S := \{a_{i_1}, a_{i_2}, \dots, a_{i_p}\} \subset E$. Then it follows readily that:

$S \in Z_{\mathbb{F}}(A)$ (i.e. S is a circuit in $M_{\mathbb{F}}(A)$)

$\Longleftrightarrow$ $\exists\ b \in \mathbb{F}^n$ which is uniquely determined up to a factor $\in \mathbb{F} - \{0\}$, such that: (i) $\bigwedge_{i \in \{i_1, i_2, \dots, i_p\}} \ b_i \neq 0$,

(ii) $\bigwedge_{i \in \{1,\dots,n\} - \{i_1,\dots,i_p\}} \ b_i = 0$,

(iii) $\sum_{i=1}^{n} b_i a_i = 0 \in \mathbb{F}^m$.

Let $Z_{\mathbb{F}}(A) =: \{S_1, S_2, \dots, S_q\}$. Then the (q × n)-matrix

$$B := \begin{pmatrix} b_1^T \\ b_2^T \\ \vdots \\ b_q^T \end{pmatrix}$$ is called the circuit-matrix of $M_{\mathbb{F}}(A)$.

Theorem 14. Let A and B be as in Example 4. If we identify the columns of A canonically with the columns of B (i.e. E is essentially the index set $\{1,2,\dots,n\}$), then the associated matrix-matroids $M_{\mathbb{F}}(A)$ and $M_{\mathbb{F}}(B)$ are dual.

<u>Proof</u>. We shall make use of Theorem 13: let $X :=$ span of the rows of A in $\mathbb{F}^n$, and $Y :=$ span of the rows of B in $\mathbb{F}^n$, i.e. $Y = \mathrm{span}(\{b_1,\ldots,b_q\})$. Thus $M_{\mathbb{F}}(A) = M_X$ and $M_{\mathbb{F}}(B) = M_Y$. The j^{th} column of AB^T is $\sum_{i=1}^{n} b_{ji}a_i = 0 \in \mathbb{F}^m$ by definition of B, hence $BA^T = 0$ or $\bigwedge i,j \ \langle a_i, b_j\rangle = 0$, i.e. $X \perp Y$. It remains to show that $\mathrm{rank}(B) = n - \mathrm{rank}(A)$. Let $p := \mathrm{rank}(A)$. We can suppose without loss of generality that the p^{th} leading principal submatrix $\tilde{A}$ of A is nonsingular, and we shall write

$$A := \begin{pmatrix} \tilde{A} & \tilde{\tilde{A}} \\ \hline \ldots & \ldots \end{pmatrix}, \qquad B := (\underset{q\times p}{\tilde{B}} \mid \underset{q\times(n-p)}{\tilde{\tilde{B}}}) \quad .$$

Then as $AB^T = 0$ we have $0 = (\tilde{A} \mid \tilde{\tilde{A}}) \begin{pmatrix} \tilde{B}^T \\ \hline \tilde{\tilde{B}}^T \end{pmatrix} = \tilde{A}\tilde{B}^T + \tilde{\tilde{A}}\tilde{\tilde{B}}^T$,

or $\tilde{B}^T = -\tilde{A}^{-1}\tilde{\tilde{A}}\tilde{\tilde{B}}^T$, or $\tilde{B} = \tilde{\tilde{B}}C$, where $C := -\tilde{\tilde{A}}^T(\tilde{A}^T)^{-1}$, i.e. the columns of $\tilde{B}$ are linear combinations of the columns of $\tilde{\tilde{B}}$, hence $\mathrm{rank}(B) = \mathrm{rank}(\tilde{\tilde{B}}) \leqslant n-p$.

On the other hand we have, as $\{a_1,a_2,\ldots,a_p\}$ is a matroid basis in $M_{\mathbb{F}}(A)$, $\bigwedge i \in \{p+1,p+2,\ldots,n\}$ $\exists$ circuit $C_{(i)}$ in $M_{\mathbb{F}}(A)$ with $a_i \in C_{(i)} \subset \{a_1,\ldots,a_p,a_i\}$. Hence for the associated vector $b_{(i)}$ we have $b_{(i)i} \neq 0$, $b_{(i)j} = 0$ for $j \in \{p+1,\ldots,n\}-\{i\}$. Thus the $n-p$ rows $b_{(i)}^T$ of B are linearly independent, i.e. $\mathrm{rank}(B) \geqslant n-p$.

§3.2. Binary Matroids.

Definitions (Crapo and Rota [7]). Let E be a finite set and $\bigwedge S, S' \subset E$ $S \triangle S'$ the symmetric difference of S and S' (cf. Remark (2) of §1.4). Then $(\mathcal{P}(E), \triangle)$ is an abelian group. Let G be a subgroup of $(\mathcal{P}(E), \triangle)$ and $\mathcal{S}_G : \mathcal{P}(E) \longrightarrow \mathcal{P}(E)$ the mapping defined by

$$\mathcal{S}_G(S) := \bigcap_{\substack{S'' \in G \\ S \subset E-S''}} (E-S'') = E - \bigcup_{\substack{S'' \in G \\ S \cap S'' = \emptyset}} S'' , \quad S \subset E .$$

Remark. We note that $S \in G \Longrightarrow \mathcal{S}_G(E-S) = E-S$.

Theorem 15. The pair $(E, \mathcal{S}_G)$ satisfies the axioms $(\mathcal{S}1) - (\mathcal{S}3)$ and is thus a matroid, namely the binary matroid $M(E,G)$. $M(E,G)$ is normal if and only if G has the property $\bigcup_{S \in G} S = E$.

Proof. Axiom $(\mathcal{S}1)$ is trivial.
Axiom $(\mathcal{S}2)$: As before we shall write $\overline{S}$ instead of $\mathcal{S}_G(S)$. Let $e \in \overline{S}$ and $S'' \in G$ with $S' \subset E-S''$. As $S \subset \overline{S'}$, we have $S \subset E-S''$, hence $e \in E-S''$ as $e \in \overline{S}$. Thus $e \in \overline{S'}$.
Axiom $(\mathcal{S}3)$: Let $S'' \in G$ with $S \cup \{e\} \subset E-S''$. As $e \notin \overline{S}$, $\exists$ $S' \in G$ with $e \in S' \subset E-S$. As $e \in \overline{S \cup \{e'\}}$, it follows that $e' \in S'$, because $e' \notin S' \Longrightarrow (S \cup \{e'\}) \cap S' = \emptyset \Longrightarrow e \in E-S'$, contradiction.
It then follows that $e' \in E-S''$, because
$e' \in S'' \Longrightarrow e' \notin S' \triangle S'' \Longrightarrow S \cup \{e'\} \subset E-(S' \triangle S'') \Longrightarrow$
$e \in E-(S' \triangle S'')$ as $e \in \overline{S \cup \{e'\}}$, contradiction, as $e \in S' \triangle S''$.

Lemma. Let $M(E,G)$ be a binary matroid. Then $Z^* \subset G$.

Proof. Let $S \in Z^*$, then

$$E\text{-}S = \overline{E\text{-}S} = E - \bigcup_{\substack{S'' \in G \\ S'' \subset S}} S'' \quad , \quad \text{i.e.} \quad S = \bigcup_{\substack{S'' \in G \\ S'' \subset S}} S'' \neq \emptyset \ ,$$

hence $\{S'' \in (G\text{-}\{\emptyset\}) : S'' \subset S\} \neq \emptyset$. However,
$\{S'' \in (G\text{-}\{\emptyset\}) : S'' \subsetneqq S\} = \emptyset$, i.e. $S \in G$, because
$(\exists\, S'' \in (G\text{-}\{\emptyset\}) \text{ with } S'' \subsetneqq S) \Longrightarrow (\overline{E\text{-}S} = E\text{-}S \subsetneqq E\text{-}S'' = \overline{E\text{-}S''})$,
contradicting the maximality of E-S in $\{S' \subset E : S' = \overline{S'} \neq E\}$ by Theorem 9(a).

Theorem 16. A matroid is binary if and only if the symmetric difference of any family of cocircuits is the union of a family of pairwise disjoint cocircuits.

Proof (Crapo and Rota [7]).
$\Longrightarrow$: Let M(E,G) be a binary matroid and suppose that the theorem does not hold for M(E,G). Let S be minimal in $\{S' \subset E : S'$ is the symmetric difference of cocircuits but not the union of pairwise disjoint cocircuits$\}$. Note that this family of sets does not contain $\emptyset$, hence $S \neq \emptyset$. By the above lemma $S \in G$, hence by the remark before Theorem 15, $\overline{E\text{-}S} = E\text{-}S \neq E$ and thus by Theorem 9(a) $\exists$ cocircuit $\tilde{S}$ with $\tilde{S} \subset S$. By the definition of S, $S \neq \tilde{S}$. Then $S \triangle \tilde{S} = S\text{-}\tilde{S} \subsetneqq S$ and $S \triangle \tilde{S} \neq \emptyset$ and $S \triangle \tilde{S}$ is the union of pairwise disjoint cocircuits by the minimality of S. But $S = (S \triangle \tilde{S}) \cup \tilde{S}$ and $(S \triangle \tilde{S}) \cap \tilde{S} = \emptyset$, hence S is the union of pairwise disjoint cocircuits, contradiction.

$\Longleftarrow$: Let $\tilde{M}$ be a matroid on E with the property that any symmetric difference of cocircuits is the union of pairwise disjoint cocircuits. Let G be the subgroup of $(\mathfrak{P}(E), \triangle)$ generated by the family $\tilde{Z}^*$ of cocircuits of $\tilde{M}$. Then $\tilde{M} = M(E,G)$:-
$S \in \tilde{Z}^* \Longrightarrow S \in G \Longrightarrow \mathcal{P}_G(E\text{-}S) = E\text{-}S \neq E \Longrightarrow S$ contains a cocircuit of M(E,G) by Theorem 9(a).

On the other hand: $S \in Z^* \Longrightarrow$ by the lemma $S \in G \Longrightarrow$ S is the symmetric difference of cocircuits of $\tilde{M} \Longrightarrow$ by the definition of $\tilde{M}$ that S is the union of pairwise disjoint cocircuits of $\tilde{M} \Longrightarrow$ S contains a cocircuit of $\tilde{M}$.

Then by Corollary 1 of Theorem 9(a) $\tilde{Z}^* = Z^*$, hence $\tilde{M}^* = (M(E,G))^*$ and thus $\tilde{M} = M(E,G)$ (or without duality: $\tilde{M}$ and $M(E,G)$ have the same hyperplanes and thus $\tilde{\mathcal{S}} = \mathcal{S}_G$ by Theorem 9(c) and Corollary 2 of Theorem 7(c)).

<u>Corollary</u>. Let $\tilde{M}$ be a binary matroid on E and G the subgroup of $(\mathfrak{P}(E),\Delta)$ generated by the family $\tilde{Z}^*$ of cocircuits of $\tilde{M}$. Then $\tilde{M} = M(E,G)$. In fact, if $\tilde{M} = M(E,G')$, then $G' = G$.

<u>Proof</u>. The first part follows because $\tilde{M}$ has the property given in Theorem 16 and $\tilde{\mathcal{S}} = \mathcal{S}_G$ by the second half of the proof of the theorem.

Second part: By the lemma $G \subset G'$. Let $S \in (G'-\{\emptyset\})$. Then as

$$\tilde{\mathcal{S}} = \mathcal{S}_G = \mathcal{S}_{G'}, \quad E-S = \overline{E-S} = E - \bigcup_{\substack{S'' \in G \\ S'' \subset S}} S'' ,$$

i.e. $S = \bigcup_{\substack{S'' \in G \\ S'' \subset S}} S'' \neq \emptyset$, and as in the lemma $S \in G$.

<u>Definitions</u>.

(1) Let M be a matroid on the finite set E and M' a matroid on the finite set E'. Then M and M' are <u>isomorphic</u> if there exists a bijection $E \longrightarrow E'$ preserving the matroid structure in both directions.

(2) Let M be a matroid and $\mathbb{F}$ a field. M is <u>representable</u> over $\mathbb{F}$ if there exists a vector space X over $\mathbb{F}$ such that M is isomorphic to the matroid associated with a finite subset of X, cf. Example 2 of §3.1. Note that we do not require the elements of this finite subset of X to be distinct, i.e. in the matrix representation of this matroid there may be vanishing columns and equal columns.

<u>Theorem 17</u>. A matroid on E is binary if and only if it is representable over the field $\mathbb{Z}_2$.

<u>Proof</u>. If $n := |E|$, we identify E with the canonical basis of the vector space $(\mathbb{Z}_2)^n$ over $\mathbb{Z}_2$. This generates a bijection $\mathfrak{P}(E) \longrightarrow (\mathbb{Z}_2)^n$ under which a subgroup G of $(\mathfrak{P}(E), \triangle)$ corresponds to a vector subspace V of $(\mathbb{Z}_2)^n$ and vice versa. Then M(E,G) is isomorphic to the matroid M_V associated with V, cf. Example 3 of §3.1 :-

Let $V =: \operatorname{span}_{\mathbb{Z}_2}(b_1, b_2, \ldots, b_m)$, $m \in \mathbb{N}_+$, where $\bigwedge i \in \{1, \ldots, m\}$ $b_i \in (\mathbb{Z}_2)^n$, (e.g. $V = \operatorname{span}_{\mathbb{Z}_2}(Z^*)$, cf. corollary of Theorem 16), and $B := \begin{pmatrix} b_1^T \\ \vdots \\ b_m^T \end{pmatrix}$. Then clearly $M_V = M_{\mathbb{Z}_2}(B)$ (cf. Example 1 of §3.1).

Let $S \subset E$ and $S =: \{e_{i_1}, e_{i_2}, \ldots, e_{i_k}\}$. Then:

(S is independent in M(E,G))

$\Longleftrightarrow$ by Theorem 7(i) $(\bigwedge j \in \{1, \ldots, k\} \quad e_{i_j} \notin \varphi_G(S - \{e_{i_j}\}))$

$\Longleftrightarrow$ $(\bigwedge j \in \{1, \ldots, k\}$ $\exists$ row $(c_1 \ldots c_n)$ in the row-space of B

over $\mathbb{Z}_2$ with $c_\ell := \begin{cases} 0 \text{ if } \ell \in \{i_1, \ldots, \hat{i}_j, \ldots, i_k\} \\ 1 \text{ if } \ell = i_j \end{cases}$

$\Longleftrightarrow$ ($\bigwedge j \in \{1,\ldots,k\}$ $\exists$ row $(\underbrace{0,\ldots,0,\overset{\uparrow}{\underset{j^{th}}{1}},0,\ldots,0}_{k})$ in the row-space over $\mathbb{Z}_2$ of the submatrix of B corresponding to S)

$\Longleftrightarrow$ (the $\mathbb{Z}_2$-rank of the submatrix of B corresponding to S is $k = |S|$)

$\Longleftrightarrow$ (S is independent in $M_{\mathbb{Z}_2}(B)$).

<u>Theorem 18</u>. Let M be a matroid. Then:

M is binary $\Longleftrightarrow$ ($\bigwedge S \in Z \quad \bigwedge S' \in Z^* \quad |S \cap S'| \equiv 0 \pmod 2$) .

<u>Proof</u>.

$\Longrightarrow$: Let G be the subgroup of $(\mathfrak{P}(E), \Delta)$ generated by Z^*. By the corollary of Theorem 16 $M = M(E,G)$, and by Theorem 17 and the bijection introduced in the proof of Theorem 17, $M(E,G) = M_V$, where $V = \text{span}(Z^*)$. Let B be as defined in the proof of Theorem 17, i.e. the rows of B are the cocircuits of M_V, and let C be the circuit-matrix of $M_{\mathbb{Z}_2}(B)$ (cf. Example 4 of §3.1). Then we have by the definition of C: if S is a circuit of M_V, then the row of C corresponding to S is the vector $\in (\mathbb{Z}_2)^n$ giving S, and clearly $BC^T \equiv 0 \pmod 2$.

$\Longleftarrow$: (Lehman [21]). We will use the characterisation of binary matroids given in Theorem 16. Suppose M is not binary. Let S ($\neq \emptyset$, cf. proof of Theorem 16) be minimal in $\{S' \subset E : S'$ is the symmetric difference of cocircuits but not the union of pairwise disjoint cocircuits}, and $S := \overset{n}{\underset{i=1}{\triangle}} S_i$, where $\bigwedge i \in \{1,...,n\}$ $S_i \in Z^*$. Let $C \in Z$. Then $\bigwedge i \in \{1,...,n\}$ $|C \cap S_i| \equiv 0 \pmod 2$, hence $|C \cap S| = |\overset{n}{\underset{i=1}{\triangle}} (C \cap S_i)| \equiv \sum_{i=1}^{n} |C \cap S_i| \equiv 0 \pmod 2$ by Remark(2) of §1.4. Thus $\bigwedge C \in Z$ $|C \cap S| \neq 1$, hence by the corollary of Theorem 9(f) S is the union of cocircuits, so $\exists\ \tilde{S} \in Z^*$ with $\tilde{S} \subset S$. We can now deduce a contradiction as in the first part of the proof of Theorem 16.

<u>Theorem 19</u>. For a matroid M the following seven properties are equivalent:

(a) M is binary,

(b) M* is binary,

(c) $\bigwedge S \in Z \quad \bigwedge S' \in Z^* \quad |S \cap S'| \equiv 0 \pmod 2$,

(d) the symmetric difference of any family of cocircuits is the union of a family of pairwise disjoint cocircuits,

(e) the symmetric difference of any family of circuits is the union of a family of pairwise disjoint circuits,

(f) M is representable over the field $\mathbb{Z}_2$,

(g) M* is representable over the field $\mathbb{Z}_2$.

<u>Corollary</u>. Let M be a binary matroid. Then:

$\bigwedge S \subset E \quad [S \in Z \iff$ (S is minimal in $\{S' \subset E : S' \neq \emptyset \wedge S'$ is the symmetric difference of a family of circuits$\})]$, and dually:

$\bigwedge S \subset E \quad [S \in Z^* \iff$ (S is minimal in $\{S' \subset E : S' \neq \emptyset \wedge S'$ is the symmetric difference of a family of cocircuits$\})]$.

<u>Proof</u>. The theorem follows by Theorems 16 - 18 and the symmetry of (c). The corollary follows by (d) and (e) of Theorem 19.

<u>Definitions</u>. Let M be a matroid on the finite set E.

(1) Let $B \in W$. $\bigwedge e \in E-B$ the unique $C \in Z$ with $e \in C \subset B \cup \{e\}$ which exists by Theorem 1(k) is called the <u>fundamental</u> <u>circuit</u> corresponding to e with respect to B.

(2) Let $S \in W^*$, i.e. $B := E-S \in W$. $\bigwedge e \in B$ the unique $S' \in Z^*$ with $e \in S' \subset S \cup \{e\}$ (i.e. $e \in S'$ and $(B-\{e\}) \cap S' = \emptyset$) which exists by Theorem 9(h) is called the <u>fundamental</u> <u>cocircuit</u> corresponding to e with respect to S.

<u>Theorem 20</u>. Let M be a matroid and $B \in W$. Then:

M is binary

$\Longleftrightarrow$ ($\bigwedge C \in Z$ $\quad C = \underset{e \in C-B}{\triangle} C_e$, where C_e is the fundamental circuit corresponding to e with respect to B) ,

$\Longleftrightarrow$ ($\bigwedge S \in Z^*$ $\quad S = \underset{e \in S \cap B}{\triangle} S_e$, where S_e is the fundamental cocircuit corresponding to e with respect to E-B) .

<u>Proof</u>. The third statement is just the dual of the second, hence the first equivalence implies the second by Theorem 19.

The second statement $\Longrightarrow$ M is binary:- We will use the characterisation of binary matroids given in Theorem 18. Let $C \in Z$ and $S \in Z^*$. Take $\tilde{e} \in S$. By Theorem 9(g) $\exists$ $B \in W$ such that $B \cap S = \{\tilde{e}\}$.

Then $C = \underset{e \in C-B}{\triangle} C_e$, and $\bigwedge e \in C-B$ $\quad S \cap C_e = \begin{Bmatrix} \{e,\tilde{e}\} \text{ if } e \in S \\ \emptyset \text{ if } e \notin S \end{Bmatrix}$ as

$|S \cap C_e| \neq 1$ by Theorem 9(g). Hence $|S \cap C| = |\underset{e \in C-B}{\triangle}(S \cap C_e)| =$

$$= |\underset{e \in (S \cap C)-B}{\triangle}(S \cap C_e)| \equiv \sum_{e \in (S \cap C)-B} |S \cap C_e| = 2|(S \cap C)-B| \equiv$$

$\equiv 0 \pmod 2$ by Remark (2) of §1.4.

M is binary $\Longrightarrow$ the second statement: (Minty [25]).

(a) Let $B \in W$ and $C \in Z$ with $C-B =: \{e_1, e_2\}$. We will use the characterisation of binary matroids given in Theorem 18. Let C_i be the fundamental circuit corresponding to e_i with respect to B, i=1,2.

(i) $C \subset C_1 \triangle C_2$: We need to show $C \subset C_1 \cup C_2$ and $C \cap (C_1 \cap C_2) = \emptyset$.

$C \subset C_1 \cup C_2$: Clearly $C-B = \{e_1, e_2\} \subset C_1 \cup C_2$. Suppose $\exists\ e \in C \cap B$ with $e \notin C_1 \cup C_2$. Let $S \in Z^*$ be the fundamental cocircuit corresponding to e with respect to E-B. By Theorem 9(g) $|S \cap C| \neq 1$, hence e_1 or $e_2 \in S$. But then $|S \cap C_1| = 1$ or $|S \cap C_2| = 1$, contradiction.

$C \cap (C_1 \cap C_2) = \emptyset$: Suppose $\exists\ e \in C \cap C_1 \cap C_2$. Then clearly $e \in B$. Let $S \in Z^*$ be the fundamental cocircuit corresponding to e with respect to E-B. By Theorem 9(g) $|S \cap C_i| \neq 1$, i=1,2, hence $\{e_1, e_2\} \subset S$. But then $S \cap C = \{e, e_1, e_2\}$, i.e. $|S \cap C| = 3 \not\equiv 0 \pmod 2$, contradiction.

(ii) $C_1 \triangle C_2 \subset C$: By Theorem 19 $C_1 \triangle C_2$ is the union of pairwise disjoint circuits, and this union representation can be chosen to contain C: by (i) $C \subset C_1 \triangle C_2$, hence $(C_1 \triangle C_2) - C = C \triangle C_1 \triangle C_2$, and this set is again the union of pairwise disjoint circuits by Theorem 19. Hence it follows that if there is another circuit C" in the union representation of $C_1 \triangle C_2$, then $C'' \subset B$, contradiction, therefore $C_1 \triangle C_2 = C$.

(b) We will prove the theorem by induction over $m := |C-B|$. The case m=1 is trivial and the case m=2 follows by (a). Suppose the theorem holds for m-1. Let $B \in W$ and $C \in Z$ with $C-B =: \{e_1, e_2, \ldots, e_m\}$, and let C_i be the fundamental circuit corresponding to e_i with respect to B, $i \in \{1,\ldots,m\}$. Clearly $C_m \not\subset C$. Take $\tilde{e} \in C_m - C$. Then by Theorem 9(i(α))
$B' := (B-\{\tilde{e}\}) \cup \{e_m\} \in W$, and $C-B' = \{e_1,\ldots,e_{m-1}\}$, hence by the induction hypothesis

$$C = \mathop{\triangle}_{i=1}^{m-1} C_i' , \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (*)$$

where C_i' is the fundamental circuit corresponding to e_i with respect to B', $i \in \{1,\ldots,m-1\}$. Clearly $\bigwedge i \in \{1,\ldots,m-1\}$ $C_i'-B = \{e_i\}$ or $\{e_i, e_m\}$. In the former case $C_i' = C_i$, and in the latter $C_i' = C_i \triangle C_m$ by (a). Substituting in (*) and simplifying using the formulae $S \triangle S = \emptyset$ and $\emptyset \triangle S = S$ clearly leads to

$C = \mathop{\triangle}_{i=1}^{m} C_i$, because C_m must appear on the right as $e_m \in C$.

<u>Theorem 21</u>. (Whitney [35]).

(i) Let M be a binary matroid.

(a) $|\{S' \subset E : S'$ is the symmetric difference of a family of circuits$\}| = 2^{|E|-r(E)}$. These sets can be obtained by taking all possible symmetric differences of the fundamental circuits with respect to a basis of M.

(b) The family of fundamental circuits with respect to a basis of M determines M.

(ii) Let $E =: \{e_1, e_2, \ldots, e_n\}$ be a set and let $P_1, P_2, \ldots, P_m$, where $m \in \{1,2,\ldots,n\}$, be subsets of E such that

$\bigwedge i \in \{1,2,\ldots,m\} \qquad e_{n-m+i} \in P_i \subset \{e_1, e_2, \ldots, e_{n-m}, e_{n-m+i}\}$.

Then there is a unique binary matroid M having $P_1, \ldots, P_m$ as fundamental circuits with respect to the basis $\{e_1, \ldots, e_{n-m}\}$.

(iii) A matroid is binary if and only if it is determined by the family of fundamental circuits with respect to a basis.

(iv) The duals of the above statements hold as well.

Proof.

(i) (a) Clearly there are exactly $2^{|E|-r(E)}$ distinct symmetric differences of the fundamental circuits with respect to $B \in W$. Let $S \subset E$ be the symmetric difference of a family of circuits and let $S-B := \{e_1, e_2, \ldots, e_m\}$. If C_i is the fundamental circuit corresponding to e_i with respect to B, $i \in \{1,\ldots,m\}$, then

$$S \triangle \Big(\mathop{\triangle}_{i=1}^{m} C_i \Big) \subset B \; . \qquad \ldots\ldots\ldots\ldots\ldots\ldots (*)$$

By Theorem 19 $S \triangle (\mathop{\triangle}_{i=1}^{m} C_i)$ is the union of a family of pairwise disjoint circuits, which contradicts (*) unless this family is empty, i.e. $S \triangle (\mathop{\triangle}_{i=1}^{m} C_i) = \emptyset$ or $S = \mathop{\triangle}_{i=1}^{m} C_i$.

(i) (b) This follows by (a) and the corollary of Theorem 19, or directly by Theorem 20.

(ii) We form the family of 2^m-1 possible distinct non-empty symmetric differences of $P_1,\dots,P_m$ and call the minimal among these, in particular $P_1,\dots,P_m$, circuits. These define a matroid M, in which $\{e_1,\dots,e_{n-m}\}$ is clearly a basis and $P_1,\dots,P_m$ are the fundamental circuits with respect to this basis. M is binary by Theorem 20, and the uniqueness follows by (i)(b).

(iii) This follows by (i)(b) and (ii).

(iv) This follows by Theorem 19.

Definitions. Let M be a binary matroid, $E := \{e_1,e_2,\dots,e_n\}$, $m := n-r(E)$, and $B := \{e_1,e_2,\dots,e_{n-m}\} \in W$.

(1) Let C_i be the fundamental circuit corresponding to e_{n-m+i} with respect to B, $i \in \{1,\dots,m\}$. Then the $(m \times n)$-matrix C defined by
$$c_{ij} := \begin{cases} 1 & \text{if } e_j \in C_i \\ 0 & \text{otherwise} \end{cases}$$
is called the fundamental circuit matrix of M with respect to B. We note that C is of the form $(P \mid I_m)$.

(2) Let S_i be the fundamental cocircuit corresponding to e_i with respect to E-B, $i \in \{1,\dots,n-m\}$. Then the $((n-m) \times n)$-matrix S defined by
$$s_{ij} := \begin{cases} 1 & \text{if } e_j \in S_i \\ 0 & \text{otherwise} \end{cases}$$
is called the fundamental cocircuit matrix of M with respect to E-B. We note that S is of the form $(I_{n-m} \mid Q)$.

<u>Remarks</u>. By Theorem 9(g) $CS^T \equiv 0 \pmod 2$; in fact, by Theorem 20 and the proof of Theorem 17,

$$M = M_{\mathbb{Z}_2}(S) \quad \text{and} \quad M^* = M_{\mathbb{Z}_2}(C)$$

under the identification $e_j \longmapsto j^{th}$ column of the matrix, and C is part of the circuit-matrix of $M_{\mathbb{Z}_2}(S)$.

Thus $$0 \equiv CS^T \equiv (P \mid I_m)\begin{pmatrix} I_{n-m} \\ \hline Q^T \end{pmatrix} \equiv P + Q^T \pmod 2,$$

i.e. $Q \equiv P^T$.

A graph-theoretic example is given in §5.2.

<u>Theorem 22</u>. (Whitney [35]). Let M be a binary matroid, $E =: \{e_1, e_2, \ldots, e_n\}$, $m := n - r(E)$, and $B := \{e_1, e_2, \ldots, e_{n-m}\} \in W$.

(a) If A is a matrix with coefficients in $\mathbb{Z}_2$ and n-m columns and $\mathbb{Z}_2$-rank n-m, then there is a unique set K of m columns which when adjoined to A gives a matrix $A' := (A \mid K)$ such that $M_{\mathbb{Z}_2}(A') = M$ under the identification $e_j \longmapsto j^{th}$ column of A'.

If in particular A is taken to be S^T, i.e. $A = S^T = \begin{pmatrix} I_{n-m} \\ \hline Q^T \end{pmatrix}$,

then $$A' = \left(\begin{array}{c|c} I_{n-m} & Q \\ \hline Q^T & * \end{array}\right) = \begin{pmatrix} S \\ \hline * \ * \end{pmatrix}.$$

(b) If A is a matrix with coefficients in $\mathbb{Z}_2$ and m columns and $\mathbb{Z}_2$-rank m, then there is a unique set K of n-m columns which when adjoined to A gives a matrix $A' := (K \mid A)$ such that $M_{\mathbb{Z}_2}(A') = M^*$ under the identification $e_j \longmapsto j^{th}$ column of A'.

If in particular A is taken to be C^T, i.e. $A = C^T = \begin{pmatrix} P^T \\ \hline I_m \end{pmatrix}$,

then $$A' = \left(\begin{array}{c|c} * & P^T \\ \hline P & I_m \end{array}\right) = \begin{pmatrix} * \ * \\ \hline C \end{pmatrix}.$$

Proof.

(a) Let a_j be the j^{th} column of A, i.e. $A = (a_1\ a_2\ \dots\ a_{n-m})$, and let C_i be the fundamental circuit corresponding to e_{n-m+i} with respect to B, $i \in \{1,\dots,m\}$. If $C_i \cap B = \emptyset$, we put $a_{n-m+i} := 0$, and if $C_i \cap B =: \{e_{i_1}, e_{i_2}, \dots, e_{i_k}\}$, $k \leqslant n-m$, we take a_{n-m+i} to be the vector with coefficients in $\mathbb{Z}_2$ satisfying $a_{n-m+i} \equiv \sum_{j=1}^{k} a_{i_j}$ (mod 2). This representation of a_{n-m+i} as a $\mathbb{Z}_2$-linear combination of the $\mathbb{Z}_2$-linearly independent vectors $a_1,\dots,a_{n-m}$ is unique, hence by Example 4 of §3.1 $\{a_{i_1}, a_{i_2}, \dots, a_{i_k}, a_{n-m+i}\}$ is a circuit in $M_{\mathbb{Z}_2}(A')$. Furthermore, $\{a_1, a_2, \dots, a_{n-m}\}$ is a basis in $M_{\mathbb{Z}_2}(A')$ and the circuits $\{a_{i_1}, a_{i_2}, \dots, a_{i_k}, a_{n-m+i}\}$ are the fundamental circuits in $M_{\mathbb{Z}_2}(A')$ with respect to this basis, and $M_{\mathbb{Z}_2}(A')$ is binary by Theorem 17. Hence by (ii) of Theorem 21 M and $M_{\mathbb{Z}_2}(A')$ are isomorphic under the identification $e_j \longmapsto j^{th}$ column of A'.

Suppose now that $A = S^T$. By Theorem 18 we have that

$$e_j \in C_i \cap B \quad \Longleftrightarrow \quad e_{n-m+i} \in S_j - B ,$$

hence for $1 \leqslant j \leqslant n-m$,

$$a_{j,n-m+i} = \begin{cases} 1 \text{ if } e_j \in C_i \cap B \\ 0 \text{ otherwise} \end{cases} = \begin{cases} 1 \text{ if } e_{n-m+i} \in S_j \\ 0 \text{ otherwise} \end{cases} = S_{j,n-m+i} .$$

(b) This follows by dualising (a) and using the relation $r(E) + r^*(E) = n$.

Remark.

A further characterisation of binary matroids related to the one given in Theorem 19(e) was established by Bixby [38] using ℓ-matrices.

§3.3. Elementary Definitions and Results from Graph Theory.

(Berge and Ghouila-Houri [2]).

A (directed) graph G is defined to be a triple (X,E,f), where X is a finite non-empty set of elements called the vertices of G, E is a finite set of elements called the edges of G, and $f: E \longrightarrow X^2$ is the incidence-mapping: if $f(e) = (a,b)$, then we say that the edge e is directed from the vertex a to the vertex b. We note that there may be more than one edge joining two vertices - these form a multiple edge, and that an edge can start and end in the same vertex - it is then called a loop. A graph with neither multiple edges nor loops is called simple. We shall drop explicit reference to f below and write G = (X,E).

If $Y \subset X$ and $E' := \{e \in E : f(e) \in Y^2\}$, then the graph (Y,E') is called the subgraph of G generated by Y. If $E'' \subset E$, the graph (X,E") is called a partial graph of G.

A simple chain k is a finite sequence $(e_1, e_2, \ldots, e_p)$ of distinct edges such that $\bigwedge\ i \in \{2,3,\ldots,p-1\}$ e_i has one end in common with e_{i-1} and the other with e_{i+1}.

A graph G = (X,E) is called connected if any two distinct vertices can be connected by a simple chain. A subset Y of X is called a connected component of G if the subgraph generated by Y is a maximal connected subgraph of G.

A simple chain is closed if it begins and ends in the same vertex. Let k be a simple closed chain. Then we define

$\mu^+(k)$:= the set of edges in k whose orientation agrees with that of k, including any loops in k, and

$\mu^-(k)$:= the set of edges in k whose orientation is opposite to that of k.

Let $\mu, \mu^+, \mu^- \subset E$ with $\mu \neq \emptyset$, $\mu = \mu^+ \cup \mu^-$, $\mu^+ \cap \mu^- = \emptyset$. Then μ is called a cycle of G if $\exists$ a simple closed chain k with $\mu^+(k) = \mu^+$, $\mu^-(k) = \mu^-$. A cycle μ is elementary if k traverses each of its vertices exactly once, and is minimal if no proper subset of μ is a cycle. It can be shown that a cycle is minimal if and only if it is elementary.

Let $Y \subset X$, $Y \neq \emptyset$. Then we define

$\omega^+(Y) := \{e \in E : f(e) = (a,b) \wedge a \in Y \wedge b \notin Y\}$, and

$\omega^-(Y) := \{e \in E : f(e) = (a,b) \wedge a \notin Y \wedge b \in Y\}$.

Let $\omega, \omega^+, \omega^- \subset E$ with $\omega \neq \emptyset$, $\omega = \omega^+ \cup \omega^-$, $\omega^+ \cap \omega^- = \emptyset$. Then ω is called a cocycle of G if $\exists$ $Y \subset X$ with $Y \neq \emptyset$ and $\omega^+(Y) = \omega^+$, $\omega^-(Y) = \omega^-$, in brief $\omega(Y) = \omega$. A cocycle ω is elementary if $\exists$ $Y \subset X$ such that $\omega(Y) = \omega$ and the subgraph generated by Y is connected and, letting C denote the connected component of G containing Y, $C-Y \neq \emptyset$ and the subgraph generated by C-Y is connected. A cocycle ω is minimal if no proper subset of ω is a cocycle. It can be shown that a cocycle is minimal if and only if it is elementary.

We note that if μ is a cycle in a partial or subgraph of G, then μ is a cycle of G, and if ω is a cocycle of G, then ω induces a cocycle in a partial or subgraph of G.

Let $|X| =: m$ and $|E| =: n$. If $E =: \{e_1, e_2, \ldots, e_n\}$, then a cycle μ and a cocycle ω can be represented uniquely as vectors $\in \mathbb{R}^n$:

$$\mu_i := \begin{cases} 1 \text{ if } e_i \in \mu^+, \\ -1 \text{ if } e_i \in \mu^-, \\ 0 \text{ if } e_i \notin \mu, \end{cases} \qquad \omega_i := \begin{cases} 1 \text{ if } e_i \in \omega^+, \\ -1 \text{ if } e_i \in \omega^-, \\ 0 \text{ if } e_i \notin \omega. \end{cases}$$

It is easy to see that $\langle \mu, \omega \rangle = \sum_{i=1}^{n} \mu_i \omega_i = 0$ (If $\omega = \omega(Y)$, then $\omega = \sum_{y \in Y} \omega(\{y\})$ and for each $y \in Y$ $\langle \mu, \omega(\{y\}) \rangle = 0$.)

If μ is a cycle of G and $k =: (e_1, e_2, \ldots, e_p)$ an associated simple closed chain, then the chain $-k := (e_p, e_{p-1}, \ldots, e_2, e_1)$, obtained by changing the orientation of k, uniquely determines a cycle which we denote $-\mu$, as we have $(-\mu)^+ = \mu^-$, $(-\mu)^- = \mu^+$. Furthermore, if μ is elementary, so is $-\mu$.

If ω is a cocycle of G and $Y \subset X$ such that $\omega = \omega(Y)$, and if $C_1, C_2, \ldots, C_q$ are those connected components of G that intersect Y, then the set $\bigcup_{i=1}^{q} (C_i - Y) \subset X$ uniquely determines a cocycle which we denote $-\omega$, as we have $(-\omega)^+ = \omega^-$, $(-\omega)^- = \omega^+$. (Note that X-Y also determines $-\omega$.) Furthermore, if ω is elementary, so is $-\omega$.

It can be shown that every cycle is the sum of pairwise disjoint elementary cycles, and similarly for cocycles.

The <u>cyclomatic number</u> $k(G)$ of G is the dimension of the vector subspace Φ of $\mathbb{R}^n$ generated by the cycles of G. The <u>cocyclomatic number</u> $\ell(G)$ of G is the dimension of the vector subspace Θ of $\mathbb{R}^n$

generated by the cocycles of G. It can be shown that

$$k(G) = n - m + p \ , \qquad \ell(G) = m - p \ ,$$

where p is the number of connected components of G. Clearly the two subspaces Φ and Θ are orthogonal complements of one another.

A graph which contains no cycles is called a <u>forest</u>, and a connected forest is called a <u>tree</u>. Thus forests and trees are simple graphs, and for a tree (X,E), $n = m-1$. A <u>spanning tree</u> of a connected graph G = (X,E) is a partial graph G' := (X,E') of G such that G' is a tree. Equivalently, a spanning tree of G is a minimal connected partial graph, or a maximal partial graph containing no cycles of G. Furthermore, a partial graph (X,E') of a connected graph G = (X,E) is connected if and only if (X,E-E') contains no cocycles of G, and is a spanning tree if and only if (X,E-E') is a maximal partial graph containing no cocycles of G.

We now have the following important results: let G = (X,E) be a connected graph, $E =: \{e_1,\dots,e_n\}$, and G' = (X,E') a spanning tree of G.

(a) If $e_i \notin E'$, then the addition of e_i to G' gives rise to an elementary cycle μ^i of G in G', which is uniquely determined up to sign. The k(G) elementary cycles obtained in this way form a cycle-basis of G.

(b) If $e_i \in E'$, then the addition of e_i to G" := (X,E-E') gives rise to an elementary cocycle ω^i of G in G", which is uniquely determined up to sign. The $\ell(G)$ elementary cocycles obtained in this way form a cocycle-basis of G.

Let G = (X,E) be a connected graph and $E =: \{e_1,e_2,\dots,e_n\}$. We now define the concepts of flow and tension on G. A vector $\varphi \in \mathbb{R}^n$ is a <u>flow</u> on G and φ_i is the flow in e_i, if for all cocycles ω

of G $\langle \varphi, \omega \rangle = 0$, or equivalently if for all $x \in X$

$$\sum_{e_i \in \omega^-(\{x\})} \varphi_i = \sum_{e_i \in \omega^+(\{x\})} \varphi_i .$$ Clearly every cycle of G is a flow on G, and it can be shown that if φ is a flow on G and $(X, \{e_1, e_2, \ldots, e_{m-1}\})$ is a spanning tree of G and $(\mu^1, \mu^2, \ldots, \mu^{n-m+1})$ is the corresponding cycle-basis of G such that $e_{m-1+i} \in (\mu^i)^+$, $1 \leqslant i \leqslant n-m+1$, then $\varphi = \sum_{i=1}^{n-m+1} \varphi_{m-1+i} \mu^i$.

Thus the vector subspace in $\mathbb{R}^n$ of all flows on G is precisely Φ .

A vector $\theta \in \mathbb{R}^n$ is a <u>tension</u> or <u>potential difference</u> on G and θ_i is the tension in e_i, if for all cycles μ of G $\langle \theta, \mu \rangle = 0$, or alternatively, if $\exists$ function $t: X \longrightarrow \mathbb{R}$ such that $\bigwedge e_i \in E$ $\theta_i = t(b_i) - t(a_i)$, where $(a_i, b_i) := f(e_i)$. The function t is called a <u>potential function</u> of the tension θ, and (as G is connected) t is uniquely determined up to addition of a constant. Clearly every cocycle of G is a tension on G, and it can be shown that if θ is a tension on G and $(\omega^1, \omega^2, \ldots, \omega^{m-1})$ is the cocycle-basis of G determined by the above spanning tree of G such that $e_i \in (\omega^i)^+$, $1 \leqslant i \leqslant m-1$, then $\theta = \sum_{i=1}^{m-1} \theta_i \omega^i$. Thus the vector subspace in $\mathbb{R}^n$ of all tensions on G is precisely Θ .

A matrix A with coefficients in $\mathbb{R}$ is called a <u>cyclomatic matrix</u> of the connected graph G if:

(1) A has n columns,

(2) the rows of A are $\in \Phi$,

(3) the $\mathbb{R}$-rank of A is $k(G) = n-m+1$.

Taking $\mu^1, \mu^2, \ldots, \mu^{n-m+1}$ as above, the matrix $\tilde{C} := (\mu^1 \mu^2 \ldots \mu^{n-m+1})^T$ is a cyclomatic matrix of G and is called a <u>fundamental cycle matrix</u> of G. We note that $\tilde{C}$ is of the form $(P \mid I_{n-m+1})$.

A matrix B with coefficients in $\mathbb{R}$ is called a <u>cocyclomatic</u> <u>matrix</u> of the connected graph G if:

(1) B has n columns,

(2) the rows of B are $\in \Theta$,

(3) the $\mathbb{R}$-rank of B is $\ell(G) = m-1$.

Clearly if A is a cyclomatic and B a cocyclomatic matrix of G, then $AB^T = 0$.

If $X =: \{x_1,x_2,\dots,x_m\}$, the <u>incidence</u> <u>matrix</u> $(\omega(\{x_1\}),\omega(\{x_2\}),\dots,\omega(\{x_m\}))^T$ is a cocyclomatic matrix of G. Furthermore, taking $\omega^1,\omega^2,\dots,\omega^{m-1}$ as above, the matrix $\tilde{S} := (\omega^1\,\omega^2\dots\,\omega^{m-1})^T$ is a cocyclomatic matrix of G and is called a <u>fundamental</u> <u>cocycle</u> <u>matrix</u> of G. We note that $\tilde{S}$ is of the form $(I_{m-1} \mid Q)$, and that

$$0 = \tilde{C}\tilde{S}^T = (P \mid I_{n-m+1}) \begin{pmatrix} I_{m-1} \\ \hline Q^T \end{pmatrix} = P + Q^T \;, \quad \text{i.e.} \quad Q = -P^T \,.$$

§3.4. Graph-Theoretic Examples.

<u>Example 1</u>. Let $G = (X,E)$ be a connected graph, $m := |X|$, $n := |E|$. The <u>graphic</u> <u>matroid</u> M(G) on E is defined by taking $Z := \{S \subset E : S \text{ is the set of edges of an elementary cycle of } G\}$. Clearly the pair (E,Z) satisfies the circuit axioms (Z1) - (Z3), cf. §1.4, and is thus a matroid. We then have:

(a) M(G) is normal if and only if G contains no loops.

(b) $S \in F \iff$ (the partial graph (X,S) contains no cycles)

$\iff$ (for every connected component X_i^S of (X,S) we have: the subgraph (X_i^S, S_i) of (X,S) generated by X_i^S is a tree)

$\iff$ (the partial graph (X,S) is a forest).

(c) $\bigwedge S' \subset S \subset E$ [(S' is a maximal independent subset of S)

$\iff$ (for every connected component X_i^S of (X,S) we have: the subgraph (X_i^S, S_i') of (X,S') generated by X_i^S is a tree)],

in particular: S is a basis $\iff$ (X,S) is a spanning tree.

(d) $\bigwedge S \subset E$ $r(S) = m - p_S$ = the cocyclomatic number ℓ_S of the partial graph (X,S), where p_S is the number of connected components of (X,S), for: if S' is a maximal independent subset of S, then $\bigwedge i \in \{1,2,\dots,p_S\}$ $|S_i'| = |X_i^S| - 1$, hence

$$|S'| = \sum_{i=1}^{p_S} |S_i'| = \sum_{i=1}^{p_S} |X_i^S| - p_S = |X| - p_S = m - p_S .$$

(e) $\bigwedge S \subset E$ $\bar{S}$ = the union $\bigcup_i E_i$ of the sets of edges occurring in the subgraphs (X_i^S, E_i) of G generated by the connected components X_i^S of (X,S),

in particular: S is spanning $\iff$ (X,S) is connected.

(f) $S \in Z^* \iff$ S is the set of edges of an elementary cocycle of G.

(g) $S \in W^*$ $\Longleftrightarrow$ $(X, E-S)$ is a spanning tree

$\Longleftrightarrow$ (X,S) is a maximal partial graph containing no cocycles of G.

(h) As for every cycle μ and cocycle ω of G $\langle \mu, \omega \rangle = 0$, it follows that $\bigwedge C \in Z \quad \bigwedge S \in Z^* \quad |C \cap S| \equiv 0 \pmod 2$. Hence M(G) is binary. See Remark (8) at the end of §3.4.

(i) Let B be a cocyclomatic matrix of G and $E =: \{e_1, e_2, \ldots, e_n\}$. Then $M(G) = M_{\mathbb{R}}(B)$ under the identification $e_j \longmapsto j^{th}$ column of B, i.e. M(G) is representable over $\mathbb{R}$.

<u>Proof</u>. Let $S \subset E$. (S dependent in $M_{\mathbb{R}}(B)$) $\Longleftrightarrow$

$\Longleftrightarrow$ (the columns of B corresponding to S are linearly dependent)

$\Longleftrightarrow$ ($\exists$ vector $\varphi \in \mathbb{R}^n$ with $\varphi \neq 0$ and $\bigwedge e_i \in E-S \quad \varphi_i = 0$ and $B\varphi = 0$)

$\Longleftrightarrow$ ($\exists$ nonvanishing flow φ on G with $\bigwedge e_i \in E-S \quad \varphi_i = 0$, i.e. $\exists$ nonvanishing flow on (X,S))

$\Longleftrightarrow$ ((X,S) contains cycles) $\Longleftrightarrow$ $S \notin F$.

<u>Example 2</u>. Let $G = (X,E)$ be a connected graph, $m := |X|$, $n := |E|$. The <u>cographic</u> <u>matroid</u> $M^*(G)$ on E is defined to be the dual matroid of M(G). In particular, we then have:

(a) ($S \subset E$ is a circuit of $M^*(G)$) $\Longleftrightarrow$

$\Longleftrightarrow$ (S is the set of edges of an elementary cocycle of G)

$\Longleftrightarrow$ $S \in Z^*$.

(b) ($S \subset E$ is an independent set of $M^*(G)$, i.e. $S \in F^*$) $\Longleftrightarrow$

$\Longleftrightarrow$ (the partial graph (X,S) contains no cocycles of G)

$\Longleftrightarrow$ (the partial graph $(X,E-S)$ is connected).

(c) $M^*(G)$ is normal if and only if for every edge $e \in E$ there is a cycle containing e, or equivalently, no edge is a cocycle of G.

(d) (S is a basis in $M^*(G)$) $\Longleftrightarrow$

$\Longleftrightarrow$ ((X,S) is a maximal partial graph containing no cocycles of G)

$\Longleftrightarrow$ ($(X,E-S)$ is a spanning tree of G) $\Longleftrightarrow$ $S \in W^*$.

(e) $\bigwedge S \subset E \quad r^*(S) = |S| - p_{E-S} + 1$, where p_{E-S} is the number of connected components of $(X,E-S)$, in particular:

$r^*(E) = |E| - |X| + 1 = n - m + 1 =$ the cyclomatic number $k(G)$ of G,

for: if S' is a maximal independent subset of S, then $(X,E-S')$ is connected, but $\bigwedge e \in S-S' \quad (X,E-(S' \cup \{e\}))$ is not connected. This implies that the number of edges that the graphs $(X,E-S')$ and (X,S) have in common is the least number necessary to connect all the components of $(X,E-S)$, i.e. $|S \cap (E-S')| = p_{E-S} - 1$.

Hence $r^*(S) = |S'| = |S| - |S \cap (E-S')| = |S| - p_{E-S} + 1$.

(f) $\bigwedge S \subset E \quad \varphi^*(S) - S = \{e \in E-S : p_{E-(S \cup \{e\})} = p_{E-S} + 1\}$, in particular: S is spanning in $M^*(G)$ $\Longleftrightarrow$ the partial graph $(X,E-S)$ contains no cycles.

(g) ($S \subset E$ is a cocircuit of $M^*(G)$) $\Longleftrightarrow$

$\Longleftrightarrow$ (S is the set of edges of an elementary cycle of G)

$\Longleftrightarrow$ $S \in Z$.

(h) $M^*(G)$ is binary. See Remark (8) at the end of §3.4.

(i) Let A be a cyclomatic matrix of G and $E =: \{e_1, e_2, \ldots, e_n\}$. Then $M^*(G) = M_{\mathbb{R}}(A)$ under the identification $e_j \longmapsto j^{th}$ column of A, i.e. $M^*(G)$ is representable over $\mathbb{R}$.

Proof. Let $S \subset E$. (S dependent in $M_{\mathbb{R}}(A)$) $\Longleftrightarrow$
$\Longleftrightarrow$ (the columns of A corresponding to S are linearly dependent)
$\Longleftrightarrow$ ($\exists$ vector $\theta \in \mathbb{R}^n$ with $\theta \neq 0$ and $\bigwedge e_i \in E-S$ $\theta_i = 0$ and $A\theta = 0$)
$\Longleftrightarrow$ ($\exists$ nonvanishing tension θ on G with $\bigwedge e_i \in E-S$ $\theta_i = 0$)
$\Longleftrightarrow$ ((X,E−S) is not connected, see below) $\Longleftrightarrow$ $S \notin F^*$.

If $\exists$ nonvanishing tension θ on G with $\bigwedge e_i \in E-S$ $\theta_i = 0$, and (X,E−S) is connected, then $\exists$ $e_j \in S$ such that $\theta_j \neq 0$, hence e_j is not a loop. Suppose $f(e_j) = (a,b)$. Then $\exists$ a simple chain k in (X,E−S) from a to b. But θ vanishes on all the edges of k, hence $\theta_j = 0$ as k and e_j together form a cycle, contradiction.

If (X,E−S) is not connected, define a function $t: X \longrightarrow \mathbb{R}$ by taking t to be constant on each connected component of (X,E−S) but not constant on all of X. It follows immediately that t is the potential function of a nonvanishing tension θ on G with $\bigwedge e_i \in E-S$ $\theta_i = 0$.

Example 3. A graph $G = (X,E)$ is called planar if it can be represented on a plane in such a way that its vertices are distinct points and its edges are simple curves that do not cross one another. The regions into which the edges of a planar graph G divide the plane are called the faces of G. For a connected planar graph G the dual graph $G^* = (X^*,E^*)$ is the connected planar graph defined as follows: to every face of G there corresponds a vertex of G^*, and to every edge e of G there corresponds an edge of G^* joining the vertices of G^* corresponding to the faces of G that e bounds - if e bounds only one face, then the corresponding edge in G^* is a loop, and vice versa. The edges of G^* are oriented in the following way: we represent G on a plane and place each vertex of G^* inside the corresponding face of G and draw each edge e^* of G^* so that it crosses the corresponding edge e of G, and no other edge of G, exactly once, and orient e^* in such a way that the directed angle $\sphericalangle(e,e^*)$ satisfies $0 < \sphericalangle(e,e^*) < \pi$. Furthermore, $G^{**} = -G$, i.e. G with all its edge-orientations reversed.

It follows readily that under the bijection $\begin{matrix} E \longrightarrow E^* \\ e \longmapsto e^* \end{matrix}$ elementary cycles in G correspond to elementary cocycles in G^*, and vice versa. Hence defining a matroid to be <u>planar</u> if it is isomorphic to a graphic and also to a cographic matroid, we have that if G is a connected planar graph, then $M(G)$ and $M(G^*)$ are planar matroids, because under the identification $\begin{matrix} E \longrightarrow E^* \\ e \longmapsto e^* \end{matrix}$ we have $M(G) = M^*(G^*)$ and $M(G^*) = M^*(G)$. Clearly the dual of a planar matroid is again planar.

<u>Remarks</u>.

(1) Let M be a matroid on E and $S \subset E$. Clearly the reduction matroid $M \times S$ (cf. §1.1, Remark (8)) of M is the matroid on S whose circuits are precisely those circuits of M which are contained in S. Analogously we define the <u>contraction matroid</u> $M \cdot S$ of M to be the matroid on S whose cocircuits are precisely those cocircuits of M which are contained in S. Clearly we then have:

$$M \cdot S = (M^* \times S)^* ,$$

and $\bigwedge S' \subset S$ $\quad r_{ctr}(S') = |S'| - r^*(S) + r^*(S-S')$

$$= r(S' \cup (E-S)) - r(E-S) .$$

The operations of reduction and contraction of a matroid generalise the operations on a graph of deleting and contracting edges. In fact, if $G = (X,E)$ is a connected graph and $S \subset E$, and we put

$G \times S$:= partial graph (X,S) of G, and

$G \cdot S$:= graph obtained by contracting all edges not in S,

then $M(G \times S) = M(G) \times S$ and $M(G \cdot S) = M(G) \cdot S$.

A minor of M is a matroid on $S \subset E$ obtained by a succession of reductions and/or contractions of M. This topic has been extensively developed by Tutte [31], and is also covered in the book by Crapo and Rota [7]. See also Remark (12) of §3.5.

(2) In analogy to the fundamental circuit matrix of a binary matroid we can define the circuit matrix of a general matroid. Let M be a matroid on E and $E =: \{e_1, e_2, \ldots, e_n\}$. If $C_1, C_2, \ldots$ $\ldots, C_m$ are the circuits of M, then the circuit matrix $C(M)$ of M is defined as follows:

$$(C(M))_{ij} := \begin{Bmatrix} 1 \text{ if } e_j \in C_i \\ 0 \text{ otherwise} \end{Bmatrix} .$$

The cocircuit matrix $S(M)$ is defined similarly.

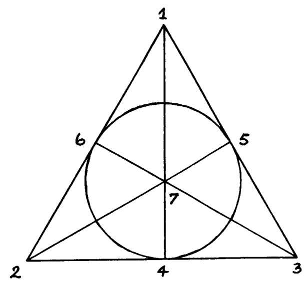
We then call M orientable if one can assign positive and negative signs to the non-zero entries of $C(M)$ and $S(M)$ such that for the resultant matrices $C_o(M)$, $S_o(M)$, $C_o(M)(S_o(M))^T = 0$.
Clearly graphic and cographic matroids are orientable.

(3) The <u>Fano matroid</u> F is defined as follows:

$E := \{1,2,\ldots,7\}$,

$W := \{S \subset E : |S| = 3\} - \{\{1,2,6\},\{1,4,7\},\{1,3,5\},\{2,3,4\},$
$\{2,5,7\},\{3,6,7\},\{4,5,6\}\}$.

The exceptional triples are those that are collinear in the Fano configuration

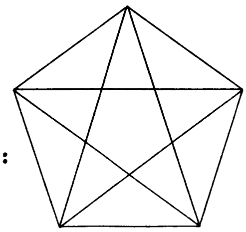


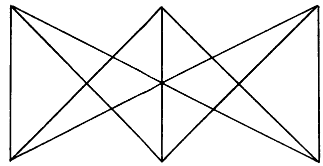
F can be shown to be representable over any field of characteristic 2, but not over any other field (cf. Whitney [35], Wilson [36]). In particular F is binary.

(4) Minty [25] has proved:
A matroid is representable over any field if and only if it is orientable.
In particular, the matroid F is not orientable, hence neither graphic nor cographic.
Tutte [30] has proved:
A matroid is representable over any field (or equivalently, orientable) if and only if it is binary and contains no minor isomorphic to F or F*.

(5) The classic characterisation of planar graphs proved by Kuratowski [20] is:

A connected graph is planar if and only if it cannot be reduced to the graphs K_5 or $K_{3,3}$ (shown below) by a succession of the operations of deleting or contracting edges (cf. Remark (1)).

K_5: 

$K_{3,3}$: 

Tutte [30] has proved the following generalisation for matroids: A matroid is graphic if and only if it is orientable and contains no minor isomorphic to $M^*(K_5)$ or $M^*(K_{3,3})$.

As corollaries we have:

(a) A matroid is cographic if and only if it is orientable and contains no minor isomorphic to $M(K_5)$ or $M(K_{3,3})$.

(b) A matroid is planar if and only if it is orientable and contains no minor isomorphic to $M(K_5)$ or $M(K_{3,3})$ or their duals.

(6) Similarly the characterisation of planar graphs given by MacLane [22] has been generalised to matroids by Welsh [33].

(7) A detailed discussion of the representability of matroids is contained in the paper by Ingleton [17].

(8) Let G be a connected graph, X the incidence matrix of G, and $\tilde{S}$ a fundamental cocycle matrix of G (cf. §3.3). Let X_0 be the matrix obtained from X by reducing mod 2, i.e. X_0 is the (0,1)-matrix with $X_0 \equiv X \pmod 2$. Doing the same with $\tilde{S}$ yields a fundamental cocircuit matrix $\tilde{S}_0$ of M(G) (cf. §3.2). By (i) of Example 1 above, $M(G) = M_{\mathbb{R}}(X) = M_{\mathbb{R}}(\tilde{S})$.

If ω is an elementary cocycle of G and $\omega = \omega(Y)$ (cf. §3.3), then $\omega = \sum_{y \in Y} \omega(\{y\})$, hence $\omega_o = \Delta_{y \in Y} \omega_o(\{y\})$, where the subscripts o denote that we ignore the directions of the edges. On the other hand, every cocycle is the sum of pairwise disjoint elementary cocycles. Thus $\text{span}_{\mathbb{Z}_2}(\text{rows of } X_o) = \text{span}_{\mathbb{Z}_2}(Z^*)$ (cf. Proof of Theorem 17). Hence $M(G) = M_{\mathbb{Z}_2}(X_o)$.
Furthermore, by the Remark after Theorem 21, $M(G) = M_{\mathbb{Z}_2}(\tilde{S}_o)$.
Clearly $\text{rank}_{\mathbb{R}}(X) = \text{rank}_{\mathbb{R}}(\tilde{S}) = \text{rank}_{\mathbb{Z}_2}(X_o) = \text{rank}_{\mathbb{Z}_2}(\tilde{S}_o) =$
$= r(M(G)) = m-1$.
Similar considerations hold for $M^*(G)$ and a fundamental cycle matrix of G.

§3.5. Combinatorial Examples.

Example 1. Let E be a finite set and $k \in \mathbb{N}$. The k-uniform matroid on E is defined by taking the family W of bases to be $\{S \subset E : |S| = k\}$. It then follows that $r(S) = \min\{|S|, k\}$, $S \subset E$. Special cases are the 0-uniform matroid which is called the trivial matroid, and the $|E|$-uniform matroid called the discrete matroid. The k-uniform matroid on a set of 2k elements is readily seen to be self-dual and non-binary.

Example 2. Let $G = (X,U)$ be a graph without loops (cf. §3.3, we denote the edge set by U here) and $A \subset U$, $A \neq \emptyset$. (The orientation of the edges of G does not play a role here.) Then A is called a matching in G if no two edges of A meet in the same vertex of G.

Clearly: $(\emptyset \neq A' \subset A$ and A is a matching in $G) \Longrightarrow (A'$ is a matching in $G)$.

If A is a matching in G, let

$V(A) := \{x \in X : \exists\ e \in A$ with $e \in$ cocycle $\omega(\{x\})\}$, cf. §3.3.

Lemma. Let A_1, A_2 be matchings in G. Then the subgraphs of the partial graph $(X, A_1 \triangle A_2)$ generated by the connected components of $(X, A_1 \triangle A_2)$ are of the following three types:

(a) an isolated vertex,

(b) a simple closed chain k traversing each of its vertices exactly once (i.e. the edge set of k is an elementary cycle), with an even number of edges and such that alternate edges of k belong to A_1 and A_2 respectively,

(c) a simple non-closed chain traversing each of its vertices exactly once and such that alternate edges belong to A_1 and A_2 respectively, and whose ends are not both in $V(A_1)$ or both in $V(A_2)$.

Proof. (Berge [1]). Let $x \in X$.

(a) If $x \notin V(A_1-A_2)$ and $x \notin V(A_2-A_1)$, then x is an isolated vertex of the partial graph $(X, A_1 \triangle A_2)$.

(b) Let $x \in V(A_1-A_2)$ and $x \notin V(A_2-A_1)$. Then exactly one edge $e \in A_1-A_2$ meets x, and no edge of A_2-A_1 meets x. Hence $x \notin V(A_2)$, for if $x \in V(A_2)$, then an edge $e' \in A_2$ meets x. Clearly $e' \neq e$, hence $e' \in A_2-A_1$ for otherwise there would be two distinct edges $e, e' \in A_1$ meeting x. But this contradicts the fact that no edge of A_2-A_1 meets x.

(c) Let $x \in V(A_1-A_2)$ and $x \in V(A_2-A_1)$. Then exactly one edge of A_1-A_2 meets x and exactly one edge of A_2-A_1 meets x.

<u>Definition</u>. Let G be as above and $E \subset X$. Then the <u>matching matroid</u> M(G,E) is the matroid on E obtained by taking the family F of independent sets to be

$F := \{S \subset E : \exists$ matching A in G with $S \subset V(A)\}$.

Axioms (F1) and (F2) are clearly satisfied.

Axiom (F3) (Edmonds and Fulkerson [12]): Let S_1 and S_2 be maximal independent subsets of $S \subset E$, and suppose that $|S_1| < |S_2|$, i.e.

$$0 \neq |S_1 - S_2| < |S_2 - S_1|. \quad \text{..................(*)}$$

By the maximality of S_1 and S_2 $\exists$ matchings A_1, A_2 in G such that $S_1 = S \cap V(A_1)$ and $S_2 = S \cap V(A_2)$.

The subgraphs of the partial graph $(X, A_1 \triangle A_2)$ generated by the connected components of $(X, A_1 \triangle A_2)$ are of types (a) - (c) given in the above lemma, and by the assumption (*) there is one of type (c), which moreover must have the property that one end is a vertex $e \in S_2 - S_1$ and the other end a vertex $\notin S_1 - S_2$. Let A' be the edge set of this chain. Then $A := A_1 \triangle A'$ is clearly a matching in G, and $S_1 \cup \{e\} \subset V(A)$, contradicting the maximality of S_1.

<u>Remarks</u>.

(1) M(G,E) is normal if and only if E contains no isolated vertices of G.

(2) If $S \subset E$, the reduction matroid $M(G,E) \times S$ is the matching matroid M(G,S).

<u>Example 3</u>. Let $A_1, A_2, \ldots, A_m$ be non-empty subsets of a finite set E. A subset $T \subset E$ with $|T| =: k \geq 1$ and $T =: \{e_{i_1}, e_{i_2}, \ldots, e_{i_k}\}$ is called a <u>partial transversal</u> of E if $\exists$ injection $j: \{1,2,\ldots,k\} \longrightarrow \{1,2,\ldots,m\}$ such that $\bigwedge q \in \{1,2,\ldots,k\}$ $e_{i_q} \in A_{j(q)}$. T is called a <u>transversal</u> or a <u>system of distinct representatives</u> of E if $k = m$.

The <u>transversal matroid</u> of the family $\{A_1, A_2, \ldots, A_m\}$ is the matroid on E obtained by taking the family F of independent sets as follows:

$F - \{\emptyset\}$:= the set of partial transversals of E.

To show that this is a matroid, we proceed as follows (Berge [1]): Let $I := \{1,2,\ldots,m\}$ and G be the graph (X,U) with vertex set $X := E \cup I$ and edge set $U := \{(e,i) \in E \times I : e \in A_i\}$. Then the set of partial transversals of E is equal to the set of nonvanishing independent subsets of the matching matroid M(G,E), in other words, every transversal matroid is a matching matroid.

<u>Remarks</u>.

(1) The maximum number of edges comprising a matching in the above graph (X,U) is given by the Theorem of König (cf. Berge [1]) to be $\min_{J \subset I}\{|I-J| + |\text{cocycle } \omega(J)|\}$, and clearly $\omega(J) = \bigcup_{j \in J} A_j$.

Hence the rank function r of the above transversal matroid is given by

$$r(S) = \min_{J \subset I}\{|I-J| + |(\bigcup_{j \in J} A_j) \cap S|\}, \quad S \subset E.$$

(2) The above transversal matroid is normal if and only if

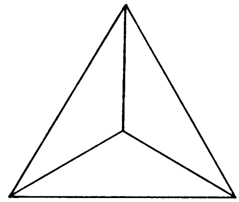
$$\bigcup_{i=1}^{m} A_i = E .$$

(3) We saw above that every transversal matroid is a matching matroid. The converse was proved by Edmonds and Fulkerson [12]. Thus the two classes of matroids are abstractly the same.

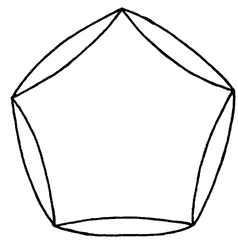
(4) The k-uniform matroid on E (cf. Example 1) is seen to be transversal by taking $k = m$ and $A_i = E$ for all $i \in \{1,...,k\}$.

(5) The following result was proved by de Sousa and Welsh [29]: A transversal matroid is binary if and only if it is graphic. Hence in particular the Fano matroid F (cf. §3.4, Remark (3)) is not transversal.

(6) A related result was proved by Bondy [3]:
The graphic matroid M(G) of a connected graph G is transversal if and only if M(G) contains no minor isomorphic to $M(K_4)$ or $M(C_n^2)$, $n>2$, where K_4 is the graph shown below and C_n^2 is the graph obtained by doubling up the edges of an n-gon:



K_4



C_5^2

(7) An algorithm for determining whether or not a matroid is transversal is given by Brualdi and Dinolt [4]. The paper also establishes necessary and sufficient conditions for a matroid to be transversal.

(8) Matroids play a very important role in transversal theory, cf. the treatise by Mirsky [26], where they are called "independence structures". In fact, Rado's matroid generalisation of Hall's "marriage" theorem can be considered the central result of transversal theory.
On the other hand, transversal theory has enriched general matroid theory: Welsh [34] has shown how very general and powerful results on the union and intersection of matroids due to Edmonds [10] can be deduced from Rado's theorem mentioned above, and that the application of these results to particular matroids yields many deep and apparently unrelated combinatorial results, some of which are very difficult to prove directly.

(9) A matroid generalisation of a transversal matroid, called a gammoid, was introduced and investigated by Mason [23]. A gammoid is the reduction of a strict gammoid, and Ingleton and Piff [18] showed that the class of strict gammoids is identical with the class of duals of transversal matroids, and that the class of gammoids is identical with the class of contractions of transversal matroids. Moreover, the dual of a gammoid is again a gammoid.

(10) Duals of transversal matroids were also characterised by Brown [39] using F-products.

(11) Another type of matroid motivated by a theorem of Gallai that was first conjectured by Sylvester for the plane, was studied by Murty ([47], [49]). The theorem is:
Let n given points in $\mathbb{R}^m$ have the property that the line joining any two of them passes through a third point of the set. Then the n points are collinear.
An obviously equivalent formulation is: if a set S of non-collinear points in real projective m-space has the above property, then $|S| = \infty$. This leads directly to a convenient matrix formulation.
A matroid on a finite set E is called a <u>Sylvester matroid</u> if $\bigwedge$ $e,e' \in E$ with $e \neq e'$ $\exists$ a circuit C with $e,e' \in C$ and $|C| = 3$.
Gallai's theorem then asserts the non-existence of Sylvester matrix-matroids $M_{\mathbb{R}}(A)$ of rank $\geqslant 3$ (cf. Example 1 of §3.1).
Murty proved that for a Sylvester matroid of rank $m \geqslant 2$ the inequality $|E| \geqslant 2^m - 1$ holds, and that in the case of equality it is isomorphic to the matrix-matroid $M_{\mathbb{Z}_2}(A)$ (cf. Example 1 of §3.1), where A is the $m \times (2^m - 1)$ matrix whose columns are the $2^m - 1$ distinct non-null elements of $\mathbb{Z}_2^m$.

(12) Let M be a matroid on E and $S \subset E$. Then the circuits of the contraction matroid $M \cdot S$ of M (cf. Remark (1) of §3.4) can be characterised as follows:

<u>Theorem</u>. $\bigwedge$ $S' \subset S$ [(S' is a circuit in $M \cdot S$) $\Longleftrightarrow$ (S' is minimal in $A := \{S'' \subset S : S'' \neq \emptyset \wedge \exists\ C \in Z$ such that $S'' = C \cap S\}$)].

<u>Proof</u>.
(a) $S'' \in A \Longrightarrow$ ($\exists$ hyperplane H (= E-C) in M* with $S - S'' = H \cap S$) $\Longrightarrow$ ($r^*(E) + r^*(S-S'') = r^*(H \cup S) + r^*(H \cap S) \leqslant r^*(H) + r(S) = r^*(E) - 1 + r^*(S)$ or $r^*(S-S'') < r^*(S)$) $\Longrightarrow r_{ctr}(S'') < |S''|$ $\Longrightarrow$ (S'' is dependent in $M \cdot S$).

(b) (S' is a circuit in M·S) $\Longrightarrow$ by Theorem 1(d) ($\bigwedge e \in S'$ $r_{ctr}(S' - \{e\}) = |S'| - 1 = r_{ctr}(S')$) $\Longrightarrow$ ($\bigwedge e \in S'$ $r^*(S) = r^*((S-S') \cup \{e\}) = r^*(S-S') + 1$) $\Longrightarrow$ ($\overline{S-S'} \cap S = S-S'$, where the bar denotes the span mapping in M*, and $\exists$ hyperplane S" in M* with $\overline{S-S'} = \overline{S} \cap S''$ by the Corollary of Theorem 9(b)) $\Longrightarrow$ ($\exists$ $C \in Z$ with $S' = C \cap S$, i.e. $S' \in A$) because $S' = S - \overline{S-S'} = S - \overline{S} \cap S'' = (E-S'') \cap S$ and we take $C := E-S''$. The minimality follows from (a). This proves the direction $\Longrightarrow$.

(c) The direction $\Longleftarrow$ now follows immediately from (a) and (b).

(13) Let M be a matroid on E. A subset $S \subset E$ is called a <u>separator</u> of M if $\bigwedge C \in Z$ $C \subset S$ or $C \subset E-S$. If the only separators of M are $\emptyset$ and E, then M is said to be <u>connected</u>. We then have the following corollaries of the theorem of Remark (12):

<u>Corollaries</u>. (Tutte [30]).

(1) $\bigwedge S \subset E$ [(S is a separator of M) $\Longleftrightarrow$ $M \times S = M \cdot S$].

(2) The separators of M* are the separators of M.

<u>Proof</u>. (1) follows trivially from the above theorem and Remark (1) of §3.4.

(2) follows trivially from (1) and Remark (1) of §3.4.

For further results on separators and connectedness cf. Tutte [30].

(14) The following type of matroid was also studied by Murty ([48], [50]). A matroid is called <u>k-equicardinal</u> if all its circuits have the same number k of elements. Murty characterised connected binary k-equicardinal matroids, $k \in \mathbb{N}_+$, giving a complete list of the possible types.

(15) For further interesting combinatorial examples of matroids, in particular geometric and lattice-theoretic ones, and a treatment of the critical problem, we refer the reader to the book by Crapo and Rota [7] and to Rota [51].

Chapter IV. Matroids and the Greedy Algorithm.

§4.1. Matroids and the Greedy Algorithm.

Definitions. Let E be a finite set.

(1) Let $w: E \longrightarrow \mathbb{R}$ be a function with $w(e) \geq 0$ for all $e \in E$. We extend w to a function $w: \mathcal{P}(E) \longrightarrow \mathbb{R}$ by setting $w(S) := \sum_{e \in S} w(e)$, $S \subset E$. The function w is called a weighting of E.

(2) A family F(E) of subsets of E with the property $[S' \subset S \in F(E) \implies S' \in F(E)]$ is called an independence system on E.

(3) If P is a family of subsets of E, then the family $\{S \subset E : \exists\ S' \in P \text{ such that } S \subset S'\}$ of subsets of E is the independence system F(P) on E generated by P.

Let P be a family of subsets of a finite set E and w a weighting of E. Then one can consider the following problem:

determine a set in P of maximum weight.

In an attempt to solve this problem, one is naturally led to consider the following algorithm:

The Greedy Algorithm: Choose $e_1 \in E$ such that $S_1 := \{e_1\} \in F(P)$ and $w(e_1) = \max\{w(e) : \{e\} \in F(P)\}$. Choose $e_2 \in E - S_1$ such that $S_2 := S_1 \cup \{e_2\} = \{e_1, e_2\} \in F(P)$ and $w(e_2) = \max\{w(e) : e \in E - S_1 \wedge S_1 \cup \{e\} \in F(P)\}$.

Continue in this way until the process terminates.

Clearly the greedy algorithm yields a maximal set in F(P) (which is thus in P), but this set will not in general be of maximum weight in P as the following counterexample shows.

<u>Counterexample</u>. $E := \{a,b,c\}$, $w(a) := 3$, $w(b) = w(c) := 2$, $P := \{\{a\},\{b,c\}\}$. Then $F(P) = \{\{a\},\{b\},\{c\},\{b,c\}\}$ and the greedy algorithm yields $\{a\} \in P$ whereas $\{b,c\}$ is the set of maximum weight in P.

<u>Definition</u>. Let P be a family of subsets of a finite set E and w a weighting of E. Let the elements of each set in P be written in order of non-increasing weight, i.e.

$S \in P, \qquad S = \{e_1, e_2, \ldots, e_k\}, \qquad w(e_1) \geqslant w(e_2) \geqslant \ldots \geqslant w(e_k).$

Then we call $\tilde{S} \in P$ <u>optimal in P</u> if $\bigwedge S \in P \quad |S| \leqslant |\tilde{S}|$ and

$\bigwedge i \in \{1,2,\ldots,|S|\} \qquad w(e_i) \leqslant w(\tilde{e}_i).$

Clearly this condition implies that $\tilde{S}$ is maximal in P and also that $\tilde{S}$ is a set in P of maximum weight. Furthermore, if the weighting w of E has the property

$\bigwedge e,e' \in E \qquad w(e) = w(e') \Longrightarrow e = e', \qquad \ldots\ldots\ldots\ldots\ldots (*)$

then clearly if an optimal set in P exists, it is unique.

The greedy algorithm does not however always yield an optimal set in P, as the above counterexample (first condition violated) and the following counterexample (second condition violated) show.

<u>Counterexample</u>. $E := \{a,b,c,d\}$, $w(a) := 4$, $w(b) = w(c) := 3$, $w(d) := 1$, $P := \{\{a,d\},\{b,c\}\}$. Then the greedy algorithm yields $\{a,d\}$ which is neither optimal in P nor a set of maximum weight in P.

<u>Lemma</u>. (Berge [1], Edmonds [11]). Let M be a matroid on E and w a weighting of E. Then the following properties of a basis B of M are equivalent:

(a) B is optimal in the family F of independent sets of M,

(b) B is a basis of maximum weight,

(c) B is a lexicographic maximum of the family W of bases of M,

(d) $\bigwedge e \in B$ $\{e' \in B : w(e') > w(e)\}$ is a maximal independent subset of $\{e' \in E : w(e') > w(e)\}$.

<u>Proof</u>. We saw above that (a) $\Longrightarrow$ (b).

(c) $\Longrightarrow$ (a): Let B be lexicographically maximal in W and suppose that B is not optimal in F, i.e. $\exists$ $S \in F$ and $\exists$ $k \in \{1,\dots,r(E)\}$ with $w(e_k^S) > w(e_k^B)$, where the elements of B and of S are written in order of non-increasing weight. Let $S' := \{e_1^B, e_2^B, \dots, e_{k-1}^B, e_1^S, e_2^S, \dots, e_k^S\}$. Then $r(S') \geqslant k$, hence $\exists$ $j \in \{1,\dots,k\}$ such that $S'' := \{e_1^B, e_2^B, \dots, e_{k-1}^B, e_j^S\} \in F$ (note use of axiom (F3)), and furthermore $\exists$ $B' \in W$ with $S'' \subset B'$. But then B' is clearly lexicographically greater than B because $w(e_j^S) \geqslant w(e_k^S) > w(e_k^B)$, which contradicts the lexicographic maximality of B.

(b) $\Longrightarrow$ (c): Let B be lexicographically maximal in W, and B' a basis of maximum weight. As (c) $\Longrightarrow$ (a), B is optimal in F, hence $\bigwedge i \in \{1,\dots,r(E)\}$ $w(e_i^B) \geqslant w(e_i^{B'})$, where the elements of B and of B' are written in order of non-increasing weight. As B' is a basis of maximum weight, $\bigwedge i \in \{1,\dots,r(E)\}$ $w(e_i^B) = w(e_i^{B'})$.

Hence B' is also lexicographically maximal in W.

(d) follows readily from either (a) or (c).

(d) $\Longrightarrow$ (b): Let B' be a basis of maximum weight and B a basis satisfying (d). Suppose that $\exists\ k \in \{1,\ldots,r(E)\}$ such that $w(e_k^B) < w(e_k^{B'})$, where the elements of B and of B' are written in order of non-increasing weight. Then $A := \{e \in B : w(e) > w(e_k^B)\}$ is not a maximal independent subset of $S := \{e \in E : w(e) > w(e_k^B)\}$, for $|A| < k$ and $\{e_1^{B'}, e_2^{B'}, \ldots, e_k^{B'}\}$ is an independent subset of S containing k elements. Hence B does not satisfy (d), contradiction. Thus $\bigwedge\ i \in \{1,\ldots,r(E)\}$ $w(e_i^B) \geqslant w(e_i^{B'})$, i.e. $w(e_i^B) = w(e_i^{B'})$ as B' is a basis of maximum weight, hence B is also a basis of maximum weight.

<u>Remark</u>. Given a particular weighting w of E and a particular application of the greedy algorithm, we can always perturb w slightly so as to obtain a weighting having property (*) while preserving the linear order in E in such a way that the greedy solution found for w remains a greedy solution, and in fact becomes the unique greedy solution. We observe that for weightings of E having property (*) the greedy algorithm undertakes the stepwise construction of the lexicographic maximum of the family of maximal sets in P - these sets, however, do not in general have the same cardinality. That the greedy algorithm does not in general do this for a weighting without property (*) is shown by the following counterexample.

<u>Counterexample</u>. $E := \{a,b,c,d\}$, $w(a) = w(b) := 4$, $w(c) := 3$, $w(d) := 1$, $P := \{\{a,c\},\{b,d\}\}$. Then $\{b,d\}$ is a greedy solution but is neither the lexicographic maximum of P nor the set of

maximum weight in P. If however we take $w(b) = 5$, then $\{b,d\}$ is the greedy solution and the lexicographic maximum of P, but not the set of maximum weight in P.

<u>Theorem 23.</u> Let P be a family of subsets of a finite set E.

(a) (Gale [13]). P contains an optimal set for every weighting of E if and only if $F(P)$ is the family of independent sets of a matroid M on E.

(b) The greedy algorithm yields a set of maximum weight in P for every weighting of E if and only if $F(P)$ is the family of independent sets of a matroid M on E.

<u>Proof.</u>

(a) $\Longleftarrow$: Let w be a weighting of E and let B be the lexicographic maximum of the family W of bases of M. Then B is optimal in P by the Lemma.

$\Longrightarrow$: If $F(P)$ is not the family of independent sets of a matroid on E, then $\exists$ subsets $S, S' \in F(P)$ such that $|S| < |S'|$ and S is maximal in $S \cup S'$. Take a weighting w of $E := \{e_1, e_2, \ldots, e_n\}$ such that $w(e_1) > w(e_2) > \ldots > w(e_n)$, and $S \cap S' = \{e_1, e_2, \ldots, e_r\}$, $S - S' = \{e_{r+1}, e_{r+2}, \ldots, e_{r+s}\}$, and $S' - S = \{e_{r+s+1}, e_{r+s+2}, \ldots, e_{r+s+t}\}$. We note that $s < t$. If $\tilde{S}$ is optimal in P, then $\tilde{S}$ must clearly be of the form $\tilde{S} = S \cup T = \{e_1, e_2, \ldots, e_{r+s}\} \cup T$, where $T \subset E - (S \cup S')$. However, comparing $\tilde{S}$ with $S' = \{e_1, e_2, \ldots, e_r, e_{r+s+1}, e_{r+s+2}, \ldots, e_{r+s+t}\}$ shows that $\tilde{S}$ cannot be optimal as $\bigwedge e \in T \quad w(e_{r+s+t}) > w(e)$.

(b) $\Longleftarrow$: This follows by the Remark and Lemma.

$\Longrightarrow$: By (a) we need only show: if for every weighting of E greedy solutions are sets of maximum weight in P, then they are optimal in P. Suppose that for a particular weighting a greedy solution $\tilde{S}$ is not optimal. Now $\tilde{S}$ will remain a greedy solution under weight changes which preserve the linear order of the elements. This allows us to construct new weightings of E for which $\tilde{S}$ is not of maximum weight:

(i) Suppose S is maximal in P with $|S| > |\tilde{S}|$. Move all weights into the interval $[1-\varepsilon, 1+\varepsilon]$, preserving the linear order. Then S weighs more than $\tilde{S}$.

(ii) Suppose S is maximal in P and $\exists\ k \in \{1,2,\dots,|S|\}$ with $w(e_k) > w(\tilde{e}_k)$. Move all weights $\geqslant w(e_k)$ into a neighbourhood of $w(e_k)$ and all weights $< w(e_k)$ into a neighbourhood of $w(\tilde{e}_k)$, preserving the linear order. Then the first neighbourhood contains at least one element more of S than of $\tilde{S}$. Now widen the gap between $w(e_k)$ and $w(\tilde{e}_k)$ until S weighs more than $\tilde{S}$.

<u>Remarks</u>.

(1) Proofs of the "if" part of Theorem 23(b) were also given by Rado [27], and Welsh [32].

(2) The application of the greedy algorithm to a particular matroid presupposes a subroutine for determining whether or not a set is independent.

If the matroid in question is a matrix-matroid $M_{\mathbb{F}}(A)$, this can be achieved automatically by using the following method based on Gaussian elimination: renumber the columns of A so that they are in order of non-increasing weight, let $A =: (a_1\ a_2\ \dots\ a_n)$. Go to the first nonvanishing column a_{k_1} of A. Let a_{ik_1} be the first nonvanishing element of a_{k_1}. Let $a'_j := a_j - \frac{a_{ij}}{a_{ik_1}} a_{k_1}$, $k_1 < j \leqslant n$, and $A' := (a'_{k_1+1}\ a'_{k_1+2}\ \dots\ a'_n)$. Now repeat this step on A'. Continue this process until only vanishing columns are left, i.e. after r steps, where $r := \mathbb{F}$-rank (A). Then $\{a_{k_1}, a_{k_2}, \dots, a_{k_r}\}$ is a basis of M of maximum weight.

If the matroid in question is a graphic matroid, then the greedy algorithm is the well-known algorithm of Kruskal [19]. However, the proof of the containing of no cycles at each step becomes increasingly tedious, and it is more efficient to use other algorithms, e.g. the ones given by Dijkstra [8], Sollin ([1] and [2]), or Rosenstiehl [28].

(3) For applications of the greedy algorithm to non-matroidal problems see Edmonds [10], [11], Dunstan and Welsh [9], and Magazine, Nemhauser and Trotter,Jr. [46].

Chapter V. Exchange Properties for Bases of Matroids.

§5.1. Symmetric Point Exchange.

Definitions. Let M be a matroid on the finite set E.

(1) Let $B \in W$, $e \in B$, and $e' \in E$. Then we say that *$e \in B$ can be replaced by e'* if $(B-\{e\}) \cup \{e'\} \in W$.

Clearly, if $e \in B$ can be replaced by e', then $e' \in B \implies e' = e$, or equivalently, $e \neq e' \implies e' \in E-B$.

(2) Let $B, B' \in W$, $e \in B$, and $e' \in B'$. Then we say that *$e \in B$ and $e' \in B'$ can be exchanged symmetrically* if $(B-\{e\}) \cup \{e'\}$, $(B'-\{e'\}) \cup \{e\} \in W$, i.e. if $e \in B$ can be replaced by e', and $e' \in B'$ by e.

Again, there are only two possibilities: the non-trivial one $e \in B-B'$ and $e' \in B'-B$, and the trivial one $e = e' \in B \cap B'$. Furthermore, we note that ($e \in B$ can be replaced by e') $\implies$ ($e' \in (B-\{e\}) \cup \{e'\}$ can be replaced by e) $\implies$ ($e \in B$ and $e' \in (B-\{e\}) \cup \{e'\}$ can be exchanged symmetrically).

Lemma. (Gabow, Glover and Klingman [43]). Let M be a matroid on E and $B, B' \in W$.

(a) Let $e \in B$ and $e' \in E-B$. Then

$e \in B$ can be replaced by e'

$\iff$ $e \in C(e', B)$, the fundamental circuit corresponding to e' with respect to B,

$\iff$ $e' \notin \overline{B-\{e\}}$.

(b) Let $e \in B-B'$ and $e' \in B'-B$. Then

$e \in B$ and $e' \in B'$ can be exchanged symmetrically

$\iff$ $e \in C(e', B) - \overline{B'-\{e'\}}$

$\iff$ $e' \in C(e, B') - \overline{B-\{e\}}$.

Proof.

(a) The first equivalence is clear by Theorem 9(i(α)). Furthermore, the first and last statements are equivalent because both are equivalent to $r((B-\{e\})\cup\{e'\}) > r(B-\{e\})$.

(b) The first statement $\Longleftrightarrow$ ($e \in B$ can be replaced by e', and $e' \in B'$ by e) $\Longleftrightarrow$ ($e \in C(e',B)$ and $e \notin \overline{B'-\{e'\}}$) by (a).

Theorem 24. Let M be a matroid and $B,B' \in W$. Then $\bigwedge e \in B$ $\exists\ e' \in B'$ such that e and e' can be exchanged symmetrically.

Proof. (Gabow, Glover and Klingman [43]).

If $e \in B'$, then take $e' := e$. Suppose that $e \notin B'$. Then $B'-B \neq \emptyset$, for otherwise $B' \subset B$, i.e. $B' = B$. As B is a minimal spanning set by Theorem 7(j), $e \notin \overline{B-\{e\}}$. Hence $C(e,B') - \{e\} \not\subset \overline{B-\{e\}}$, as otherwise $e \in C(e,B') \subset \overline{B-\{e\}} \cup \{e\}$, hence $e \in \overline{B-\{e\}}$ by Theorem 7(g), contradiction. Thus $\emptyset \neq [C(e,B') - \overline{B-\{e\}}] - \{e\} \subset B'-B$ and the result follows by (b) of the Lemma.

Direct Proof. (Brualdi [40]).

If $e \in B'$, then take $e' := e$. Suppose that $e \notin B'$. Then as above, $B'-B \neq \emptyset$. Furthermore, $C(e,B') \cap (B'-B) \neq \emptyset$, for otherwise $C(e,B') \subset B$. Suppose $x \in C(e,B') \cap (B'-B)$. If $e \notin C(x,B)$, then by Theorem 1(j) $\exists$ circuit C' such that

$e \in C' \subset (C(x,B) \cup C(e,B')) - \{x\}$, and $C' \cap (B'-B) \subsetneqq C(e,B') \cap (B'-B)$, hence $|C' \cap (B'-B)| < |C(e,B') \cap (B'-B)|$.

If $\bigwedge x \in C(e,B') \cap (B'-B)$ $e \notin C(x,B)$, then by repeating this step (with C' instead of $C(e,B')$ and so on) a finite number of times, we obtain a circuit $\tilde{C}$ with $e \in \tilde{C} \subset B$, contradiction. Hence $\exists\ e' \in C(e,B') \cap (B'-B)$ with $e \in C(e',B)$, i.e. by (a) of the Lemma $e \in B$ can be replaced by e', and $e' \in B'$ by e.

§5.2. Bijective Point Replacement.

Theorem 25. Let M be a matroid on E and B, $B' \in W$.

(a) $\exists$ bijection $f: B \longrightarrow B'$ such that each $e \in B$ can be replaced by f(e), i.e. $\bigwedge e \in B \quad (B-\{e\}) \cup \{f(e)\} \in W$.

More generally:

(b) (Gabow, Glover and Klingman [43]). If $B' =: \{e_1', e_2', \ldots, e_m'\}$, where $m := r(E)$, then $\exists$ an ordering $B = \{e_1, e_2, \ldots, e_m\}$ of B such that $\bigwedge i \in \{1, \ldots, m\}$ $e_i \in B$ can be replaced by e_i' and $B_i := \{e_1, e_2, \ldots, e_i, e_{i+1}', e_{i+2}', \ldots, e_m'\} \in W$, (thus $\bigwedge i \in \{1, \ldots, m\}$ $e_i \in B$ and $e_i' \in B_{i-1}$ can be exchanged symmetrically, where $B_0 := B'$), and in particular $f: B \longrightarrow B'$ defined by $f(e_i) := e_i'$ provides a serial replacement from B to B', and from B' to B (namely $B_0, B_1, \ldots, B_m$). Note that f does not provide a serial symmetric exchange between B and B', as the sets $B_i' := \{e_1', e_2', \ldots, e_i', e_{i+1}, e_{i+2}, \ldots, e_m\}$, $i \in \{2, \ldots, m-1\}$, are in general not bases (cf. Counterexample 1 below). We also note that reversal of the order in B and B' gives B_i' in place of B_i in the theorem.

Similarly:

(c) If $B := \{e_1, e_2, \ldots, e_m\}$, then $\exists$ an ordering $B' = \{e_1', e_2', \ldots, e_m'\}$ of B' such that $\bigwedge i \in \{1, \ldots, m\}$ $e_i \in B$ can be replaced by e_i' and $B_i \in W$, in particular $f: B \longrightarrow B'$ defined by $f(e_i) := e_i'$ provides a serial replacement from B to B', and from B' to B. Again, f does not in general provide a serial symmetric exchange between B and B' (cf. Counterexample 1 below), and reversal of the order in B and B' gives B_i' in place of B_i in the theorem.

<u>Proof</u>.

(b) (Gabow, Glover and Klingman [43]). By induction over i. The point e_1 is given by Theorem 24, and $(B'-\{e_1'\}) \cup \{e_1\} = B_1 \in W$. Suppose the theorem holds for all $i < j$. Then by Theorem 24 $e_j' \in B_{j-1}$ can be exchanged symmetrically for some point $\tilde{e} \in B$, and clearly $\tilde{e} \notin \{e_1, e_2, \dots, e_{j-1}\} \subset B_{j-1}$. Hence taking $e_j := \tilde{e}$ we have that $(B-\{e_j\}) \cup \{e_j'\} \in W$ and $(B_{j-1}- \{e_j'\}) \cup \{e_j\} = B_j \in W$.

(c) By induction over i. The point e_1' is given by Theorem 24, and $(B'-\{e_1'\}) \cup \{e_1\} = B_1 \in W$. Suppose the theorem holds for all $i < j$. Then by Theorem 24 $e_j \in B$ can be exchanged symmetrically for some point $\tilde{e}' \in B_{j-1}$, and clearly $\tilde{e}' \notin \{e_1, \dots, e_{j-1}\} \subset B$. Hence taking $e_j' := \tilde{e}'$ we have that $(B-\{e_j\}) \cup \{e_j'\} \in W$ and $(B_{j-1}- \{e_j'\}) \cup \{e_j\} = B_j \in W$.

A second proof of (b) and (c) based on a proof of (a) given by Brylawski [42] follows the discussion of certain special minors of M in the next section.

<u>Remark</u>.

Let M be a matroid and $B, B' \in W$. It is natural to ask firstly whether a bijection $f: B \longrightarrow B'$ exists such that $\bigwedge_{e \in B}$ e and f(e) can be exchanged symmetrically, and secondly whether, given a fixed ordering of B' (or B), a bijection f exists giving a serial symmetric exchange between B and B'. These questions are answered in the negative by the following two counterexamples.

<u>Counterexample 1</u>. (Brualdi [40]).

Consider the matrix-matroid $M_{\mathbb{Z}_2}(A)$ (cf. Example 1 of §3.1) associated with $A := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = (a_1\ a_2\ \dots\ a_6)$.

It is easily checked that every triple of columns of A is a basis of $M_{\mathbb{Z}_2}(A)$ except $\{a_1,a_2,a_6\}$, $\{a_1,a_3,a_5\}$, $\{a_2,a_3,a_4\}$, and $\{a_4,a_5,a_6\}$.

Let $B := \{a_1,a_4,a_5\}$ and $B' := \{a_2,a_3,a_6\}$. Suppose $f: B \longrightarrow B'$ is a bijection such that $\bigwedge e \in B$ e and f(e) can be exchanged symmetrically. Now

$(B-\{a_1\}) \cup \{e'\} \in W$ for $e' \in \{a_2,a_3\}$ but not for $e' = a_6$,

$(B'-\{e'\}) \cup \{a_1\} \in W$ for $e' \in \{a_2,a_6\}$ but not for $e' = a_3$,

therefore $f(a_1)$ can only be a_2. Similarly $f(a_4)$ can only be a_2, i.e. f is not bijective, contradiction. This answers the first question in the negative.

The only bijections answering Theorem 25(a) are

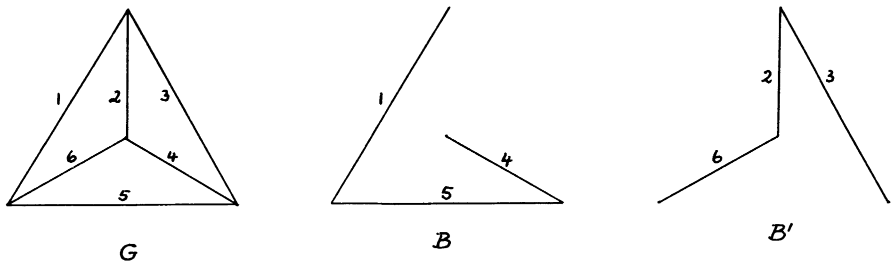
$$\begin{matrix} a_1 & a_4 & a_5 \\ \downarrow & \downarrow & \downarrow \\ a_2 & a_6 & a_3 \end{matrix}\ ,\quad \begin{matrix} a_1 & a_4 & a_5 \\ \downarrow & \downarrow & \downarrow \\ a_3 & a_2 & a_6 \end{matrix}\ ,\quad \begin{matrix} a_1 & a_4 & a_5 \\ \downarrow & \downarrow & \downarrow \\ a_3 & a_6 & a_2 \end{matrix}\ .$$

If we fix the order in B' as $\{a_3,a_2,a_6\}$, the only ordering of B answering Theorem 25(b) is $\{a_5,a_1,a_4\}$, and this bijection does not provide a serial symmetric exchange between B and B'.

If we fix the order in B as $\{a_4,a_5,a_1\}$, the only ordering of B' answering Theorem 25(c) is $\{a_2,a_6,a_3\}$, and this bijection does not provide a serial symmetric exchange between B and B'.

<u>Counterexample 2</u>. (Gabow, Glover and Klingman [43]).

Consider the graphic matroid M(G) (cf. Example 1 of §3.4), where G is the graph shown, and let $B := \{1,4,5\}$ and $B' := \{2,3,6\}$.



The rest of this counterexample is the same as Counterexample 1 above, in fact $A =: (I_3 \mid Q)$ is the fundamental cocircuit matrix of $M(G)$ with respect to the cobasis $\{4,5,6\}$ of $M(G)$ (cf. Definitions and Remarks after Theorem 21), and $M(G) = M_{\mathbb{Z}_2}(A)$. We summarise the relevant details:

The fundamental cocircuits of $M(G)$ with respect to $\{4,5,6\}$ are

$S_1 = \{1,5,6\}$, $S_2 = \{2,4,6\}$, $S_3 = \{3,4,5\}$.

The family of cocircuits of $M(G)$ is

$\{1,5,6\} = S_1$,	$\{1,2,4,5\} = S_1 \triangle S_2$,
$\{2,4,6\} = S_2$,	$\{2,3,5,6\} = S_2 \triangle S_3$,
$\{3,4,5\} = S_3$,	$\{1,3,4,6\} = S_3 \triangle S_1$.
$\{1,2,3\} = S_1 \triangle S_2 \triangle S_3$,	

The fundamental circuits of $M(G)$ with respect to the basis $\{1,2,3\}$ are $C_1 = \{2,3,4\}$, $C_2 = \{1,3,5\}$, $C_3 = \{1,2,6\}$.

The family of circuits of $M(G)$ is

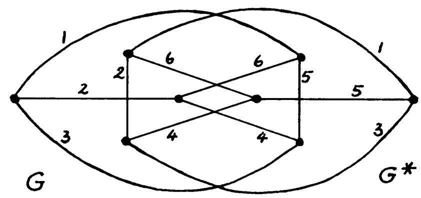
$\{2,3,4\} = C_1$,	$\{1,2,4,5\} = C_1 \triangle C_2$,
$\{1,3,5\} = C_2$,	$\{2,3,5,6\} = C_2 \triangle C_3$,
$\{1,2,6\} = C_3$,	$\{1,3,4,6\} = C_3 \triangle C_1$.
$\{4,5,6\} = C_1 \triangle C_2 \triangle C_3$,	

The fundamental circuit matrix C of $M(G)$ with respect to $\{1,2,3\}$ is

$$C = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} =: (P \mid I_3),$$

and clearly $P = Q^T = Q$.

We also note that G is a connected planar graph, hence the dual graph G* of G exists:



and $M(G) \overset{d}{\cong} M^*(G^*)$ and $M(G^*) \overset{d}{\cong} M^*(G)$ under the edge identification d given by the edge numberings (cf. Example 3 of §3.4). Furthermore, G and G* are the same and can be identified by the bijection g: G ——> G* given by

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 5 & 6 & 1 & 2 & 3 \end{matrix},$$

whence $M(G) \overset{g}{\cong} M(G^*) \overset{d}{\cong} M^*(G)$ or $M(G) \overset{h}{\cong} M^*(G)$ under the bijection h: G ——> G given by

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 5 & 6 & 1 & 2 & 3 \end{matrix}.$$

Under this isomorphism S_i corresponds to C_i, $i \in \{1,2,3\}$, and vice versa.

§5.3. More on Minors of a Matroid.

Let M be a matroid on E.

(1) Let $S \subset E$ and suppose that $S \in F^*$ (cf. Theorem 11). By Remark (1) of §3.4 the reduction matroid $M \times (E-S)$ is the matroid on E-S having basis set $\{B \in W : B \cap S = \emptyset\}$.

(2) Let $S \subset E$ and suppose that $S \in F$, and let M_1 be the matroid on E-S with basis set $\{B-S : S \subset B \in W\}$. Then the dual matroid M_1^* has basis set $\{E-B : S \subset B \in W\} = \{S' \in W^* : S' \cap S = \emptyset\}$, i.e. by (1) M_1^* is the reduction matroid $M^* \times (E-S)$, and hence by Remark (1) of §3.4 $M_1 = (M^* \times (E-S))^* = M \cdot (E-S)$.

Thus the contraction matroid $M\cdot(E-S)$ is the matroid on $E-S$ having basis set $\{B-S : S\subset B\in W\}$, and by Remark (1) of §3.4 the rank function r_{ctr} of $M\cdot(E-S)$ is given by

$r_{ctr}(S') = r(S'\cup S) - r(S) = r(S'\cup S) - |S|$, $\quad S'\subset E-S$.

In particular the rank of $M\cdot(E-S)$ is $r_{ctr}(E-S) = r(E) - |S|$.

(3) Let $S_1,S_2\subset E$ and suppose that $S_1\cap S_2 = \emptyset$, $S_1\in F$, $S_2\in F^*$. Then $(E-S_1) - (E - (S_1\cup S_2)) = S_2$, and $(M\cdot(E-S_1))\times(E-(S_1\cup S_2))$ is the matroid on $E-(S_1\cup S_2)$ having basis set

$\{B \text{ basis of } M\cdot(E-S_1) : B\cap S_2 = \emptyset\} = \{B-S_1 : S_1\subset B\in W \wedge B\cap S_2 = \emptyset\}$.

On the other hand, $(E-S_2) - (E-(S_1\cup S_2)) = S_1$, and $(M\times(E-S_2))\cdot(E-(S_1\cup S_2))$ is the matroid on $E-(S_1\cup S_2)$ having basis set $\{B-S_1 : S_1\subset B \text{ basis of } M\times(E-S_2)\} =$
$= \{B-S_1 : S_1\subset B\in W \wedge B\cap S_2 = \emptyset\}$, i.e.

$$(M\cdot(E-S_1))\times(E-(S_1\cup S_2)) = (M\times(E-S_2))\cdot(E-(S_1\cup S_2)),$$

with rank function $\tilde{r}(S') = r(S'\cup S_1) - |S_1|$, $\quad S'\subset E-(S_1\cup S_2)$,

and rank $\tilde{r}(E-(S_1\cup S_2)) = r(E-S_2) - |S_1| = r(E) - |S_1|$.

We shall denote this matroid by $M(S_1,S_2)$.

<u>Proof of Theorem 25(b)</u>. (based on Brylawski [42]).

By induction over the rank of M. Clearly the theorem is trivial if the rank of M is 1. Assume that the theorem holds for matroids of rank m-1, where m is the rank of M. Let $B,B'\in W$ and $B' =: \{e_1',e_2',\dots,e_m'\}$. Then by Theorem 24 e_1' can be exchanged symmetrically for some point $e_1\in B$. Thus $B-\{e_1\}$ and $B'-\{e_1'\}$ are both in the basis set $\tilde{W} := \{\tilde{B}-\{e_1\} : e_1\in \tilde{B}\in W\}$ of the matroid $M(\{e_1\},\emptyset)$ of rank m-1. Hence by the induction hypothesis $\exists$ an ordering $B-\{e_1\} = \{e_2, e_3, \ldots, e_m\}$ of $B-\{e_1\}$ such that

$\bigwedge\ i \in \{2,\ldots,m\}$ $(B-\{e_1,e_i\}) \cup \{e_i'\} \in \widetilde{W}$ and

$\{e_2,\ldots,e_i,e_{i+1}',\ldots,e_m'\} \in \widetilde{W}$, i.e. $\bigwedge\ i \in \{2,\ldots,m\}$

$(B-\{e_i\}) \cup \{e_i'\} \in W$ and $\{e_1,\ldots,e_i,e_{i+1}',\ldots,e_m'\} \in W$. Finally

$(B-\{e_1\}) \cup \{e_1'\} \in W$ and $\{e_1,e_2',\ldots,e_m'\} = (B'-\{e_1'\}) \cup \{e_1\} \in W$ by

definition of e_1.

The proof of Theorem 25(c) follows analogously.

Remark. Brylawski [42] also proved Theorem 24 and Theorem 26 below using the concepts introduced in this section.

§5.4. Symmetric Set Exchange.

Let A be an $(m \times n)$-matrix with coefficients in the field $\mathbb{F}$ and $\mathbb{F}$-rank m, and let $M_{\mathbb{F}}(A)$ be the associated matrix-matroid (cf. Example 1 of §3.1). If $S \subset E$, let $M(S)$ denote the corresponding submatrix of A. Now let $B, B' \in W$, i.e. $M(B)$ and $M(B')$ are non-singular $(m \times m)$-submatrices of A. By taking the columns of $M(B')$ as basis of $\mathbb{F}^m$ we can without loss of generality assume that $M(B') = I_m$. Let $S \subset B$. Then the classical Laplace expansion of det M(B) with respect to S gives

$$\det M(B) = \sum_{S' \subset B'} \pm \det M((B-S) \cup S') \cdot \det M((B'-S') \cup S) .$$

As $\det M(B) \neq 0$, some term on the right must be $\neq 0$, which proves the following generalisation of Theorem 24 for matrix-matroids:

<u>Theorem 26</u>. Let M be a matroid on E and $B, B' \in W$. Then $\bigwedge S \subset B \;\; \exists \; S' \subset B'$ such that

$$(B-S) \cup S' \in W \quad \text{and} \quad (B'-S') \cup S \in W.$$

<u>Remark</u>. If S and S' have the properties given in the theorem, then it follows readily that $S \cap B' = S' \cap B$ and $|S| = |S'|$.

<u>Proof (1)</u>. (Woodall [37]).
Let $m := r(E) = |B| = |B'| =$ rank of M, and $k := |S|$. We will prove the theorem for the case $B \cap B' = \emptyset$. Then the theorem follows by considering instead of M the contraction matroid $M \cdot (E-(B \cap B'))$ with basis set $\{\tilde{B}-(B \cap B') : B \cap B' \subset \tilde{B} \in W\}$ and rank function $r_{ctr}(S'') = r(S'' \cup (B \cap B')) - |B \cap B'|$, $S'' \subset E-(B \cap B')$, and rank $m - |B \cap B'|$, and taking $S-B'$ instead of S.
By the submodular inequality we have that $\bigwedge S'' \subset E$

$$r(S \cup S'') + r((B-S) \cup S'') \geqslant r(B \cup S'') + r((S \cap (B-S)) \cup S'')$$
$$= m + r(S''). \qquad \ldots\ldots\ldots\ldots \; (*)$$

Let $M_1 := (M \cdot (E-(B-S))) \times B'$, then $\bigwedge S'' \subset B'$
$r_1(S'') = r(S'' \cup (B-S)) - m + k$, and the rank of M_1 is k.
Let $M_2 := (M^* \times (E-S)) \cdot B'$, then $\bigwedge S'' \subset B'$

$$r_2(S'') = r^*(S'' \cup (E-(S \cup B'))) - r^*(E-(S \cup B'))$$
$$= |S''| + r(S \cup (B'-S'')) - m \quad \text{by Theorem 11(b)},$$

and the rank of M_2 is k.
Now Edmonds' <u>Matroid Intersection Theorem</u> (cf. Theorem 69 of Edmonds [10] and Theorem 4 of Welsh [34]) states:
Two matroids $M(E,r_1)$, $M(E,r_2)$ have a common independent set of k elements if and only if

$$\bigwedge S \subset E \qquad r_1(S) + r_2(E-S) \geqslant k.$$

For M_1 and M_2 we have: $\bigwedge S'' \subset B'$

$$r_1(S'') + r_2(B'-S'') = (r(S'' \cup (B-S)) - m + k) + (r(S \cup S'') - |S''|)$$
$$\geqslant k \quad \text{by } (*).$$

Hence $\exists \; S' \subset B'$ with $r_1(S') = r_2(S') = |S'| = k$, i.e.

$$r(S' \cup (B-S)) = r(S \cup (B'-S')) = m.$$

<u>Proof (2)</u>. (Greene and Magnanti [45]).

Let m and k be as in Proof (1), and again we can without loss of generality assume that $B \cap B' = \emptyset$. Furthermore, let M_1 be as in Proof (1).

Let $M_3 := (M\cdot(E-S)) \times B'$, then $\bigwedge S'' \subset B'$

$r_3(S'') = r(S'' \cup S) - k$, and the rank of M_3 is m-k. We note that $M_3^* = M_2$ of Proof (1).

Now the <u>Matroid Partition Theorem</u> of Edmonds and Fulkerson ([12]) states:

Let $n \in \mathbb{N}_+$ and $M(E, r_i)$, $i \in \{1,\dots,n\}$, be matroids on E. Then E can be partitioned into a family of subsets $S_1, S_2, \dots, S_n$, such that $\bigwedge i \in \{1,\dots,n\}$ $S_i \in F_i$, if and only if

$$\bigwedge S \subset E \qquad \sum_{i=1}^{n} r_i(S) \geqslant |S| .$$

For M_1 and M_3 we have: $\bigwedge S'' \subset B'$

$$r_1(S'') + r_3(S'') = (r(S'' \cup (B-S)) - m + k) + (r(S'' \cup S) - k)$$
$$\geqslant |S''| \quad \text{by (*) of Proof (1).}$$

Hence $\exists\, S' \subset B'$ with $r_1(S') = |S'|$ and

$r_3(B'-S') = |B'-S'| = m - |S'|$,

i.e. $r(S' \cup (B-S)) = |S'| + m - k$ and

$r(S \cup (B'-S')) = m + k - |S'|$.

As $r(S \cup (B'-S')) \leqslant m$, it follows that $|S'| \geqslant k$, and as $r(S' \cup (B-S)) \leqslant m$, it follows that $|S'| \leqslant k$, hence $|S'| = k$, and

$$r(S \cup (B'-S')) = r(S' \cup (B-S)) = m.$$

<u>Remark</u>.

A lengthy but direct proof of Theorem 26 was given by Greene [14]. See also the Remark at the end of the previous section.

§5.5. Bijective Set Replacement.

Theorem 26 gives rise naturally to the following generalisation of Theorem 25.

Theorem 27. Let M be a matroid and $B, B' \in W$.

(a) (Greene and Magnanti [45]). Suppose that B has been partitioned into a family of subsets $S_1, S_2, \ldots, S_n$. Then B' can be partitioned into a family of subsets $S_1', S_2', \ldots, S_n'$ such that

$$\bigwedge i \in \{1,\ldots,n\} \quad (B-S_i) \cup S_i' \in W \quad \text{and} \quad B_i := \left(\bigcup_{j=1}^{i} S_j\right) \cup \left(\bigcup_{j=i+1}^{n} S_j'\right) \in W.$$

(b) Suppose that B' has been partitioned into a family of subsets $S_1', S_2', \ldots, S_n'$. Then B can be partitioned into a family of subsets $S_1, S_2, \ldots, S_n$ such that $\bigwedge i \in \{1,\ldots,n\}$ $(B-S_i) \cup S_i' \in W$ and $B_i \in W$.

Proof. The earlier proofs by induction over i generalise readily to yield proofs of the above.

Remark.

Greene and Magnanti [45] gave a proof of all of (a) except $B_i \in W$, using the Matroid Partition Theorem of Edmonds and Fulkerson (cf. Proof (2) of Theorem 26) and a generalised submodular inequality.

§5.6. A Further Symmetric Set Exchange Property.

Theorem 28. (Greene [44]). Let M be a matroid on E and $B,B' \in W$. If $S \subset B-B'$ and $S' \subset B'-B$ with $|S| + |S'| > r(E)$, then $\exists$ non-empty subsets $S_o \subset S$ and $S'_o \subset S'$ such that $(B-S_o) \cup S'_o \in W$ and $(B'-S'_o) \cup S_o \in W$.

Remarks. The theorem is trivial if $S \cap S' \neq \emptyset$: take $S_o = S'_o = S \cap S'$. Furthermore, if $S \cap S' = \emptyset$ and S_o and S'_o have the properties given in the theorem, then $S_o \cap B' = \emptyset$ and $S'_o \cap B = \emptyset$ by the Remark after Theorem 26.

Proof.† Let $m := r(E)$. We can without loss of generality assume that $S = \{e_1,e_2,\ldots,e_k\}$, where $k \in \{1,\ldots,m\}$, and $|S'| = m-k+1$. Let C_i be the fundamental circuit corresponding to $e_i \in S$ with respect to B', and $S_i := C_i \cap S'$, $T_i := C_i \cap (B'-S')$, i.e. $C_i = S_i \cup T_i \cup \{e_i\}$, $i \in \{1,\ldots,k\}$.

(a) $K := \{\tilde{S} \subset S : \tilde{S} \neq \emptyset \wedge \bigwedge_{e_i \in \tilde{S}} S_i \not\subset \overline{B-\tilde{S}}\} \neq \emptyset$:-

Suppose $K = \emptyset$. Then by renumbering the $e_i \in S$, we have:

$S \notin K$ because $S_1 \subset \overline{B-S}$,

$S-\{e_1\} \notin K$ because $S_2 \subset \overline{(B-S) \cup \{e_1\}}$,

. . . .

$\{e_k\} \notin K$ because $S_k \subset \overline{B-\{e_k\}}$.

Let $V := \overline{(B-S) \cup (B'-S')}$. As $S_1 \subset \overline{B-S} \subset V$ and $T_1 \subset B'-S' \subset V$, we have $e_1 \in C_1 \subset V \cup \{e_1\}$ and thus $e_1 \in \overline{V} = V$ by Theorem 7(g) (cf. footnote on p.16).

---

† The above proof is an extended version of the proof given by Greene which applies only to combinatorial geometries (normal matroids all of whose elements are closed) and uses lattice-theoretic operators.

As $S_2 \subset \overline{(B-S)\cup\{e_1\}} \subset V$ and $T_2 \subset V$, we have $e_2 \in C_2 \subset V \cup \{e_2\}$ and thus $e_2 \in \overline{V} = V$ by Theorem 7(g).

Continuing in this way, we see that $S \subset V$ and thus $B \subset V$ which is a contradiction as $r(B) = m$ and

$r(V) \leqslant r(B-S) + r(B'-S')$ by the submodular inequality and Theorem 7(a),

$= (m-k) + (k-1) = m-1.$

(b) (S_o is minimal in K) $\Longrightarrow$ (S_o can be exchanged symmetrically):

(i) $|S_o| = 1$. Suppose $S_o = \{e_1\}$. As $S_o \in K$, we have $S_1 \not\subset \overline{B-\{e_1\}}$, hence $\exists\ e' \in S_1 - \overline{B-\{e_1\}} \subset C_1 - \overline{B-\{e_1\}}$. Then by (b) of the Lemma in §5.1 e_1 and e' can be exchanged symmetrically. Hence we take $S_o' := \{e'\}$.

(ii) $|S_o| > 1$. If $e_i \in S_o$, then $S_o - \{e_i\} \notin K$ by minimality of S_o, hence $\exists\ e_j \in S_o - \{e_i\}$ such that $S_j \subset \overline{(B-S_o)\cup\{e_i\}}$. Put $f(i) := j$, then $f\colon S_o \longrightarrow S_o$ is injective, hence bijective: suppose $i \neq i'$ and $f(i) = f(i') =: j$, and let $X := (B-S_o)\cup\{e_i\}$, $Y := (B-S_o)\cup\{e_{i'}\}$. Then $S_j \subset \overline{X} \cap \overline{Y} \supset \overline{B-S_o}$ by Theorem 7(d(1)), and

$m - |S_o| = r(B-S_o) \leqslant r(\overline{X} \cap \overline{Y})$

$\leqslant r(X) + r(Y) - r(X \cup Y)$ (cf. Theorem 7(d(3))

$= 2(m - |S_o| + 1) - (m - |S_o| + 2) = m - |S_o|.$

Hence by Theorem 7(e) and (d(2)) $\overline{B-S_o} = \overline{\overline{X} \cap \overline{Y}} = \overline{X} \cap \overline{Y}$. Thus $S_j \subset \overline{B-S_o}$ contradicting $S_o \in K$.

Suppose $e_i \in S_o$. Then by the above $S_{f(i)} \subset \overline{(B-S_o)\cup\{e_i\}}$, but $S_{f(i)} \not\subset \overline{B-S_o}$ as $S_o \in K$. Hence $\exists\ e_i' \in S_{f(i)} - \overline{B-S_o}$, and by Theorem 7(h) $e_i \in \overline{(B-S_o)\cup\{e_i'\}}$, i.e. $\overline{(B-S_o)\cup\{e_i\}} = \overline{(B-S_o)\cup\{e_i'\}}$.

Let $I := \{i \in \{1,\dots,k\} : e_i \in S_o\}$, then the sets $S_{f(i)} - \overline{B-S_o}$, $i \in I$, are pairwise disjoint: as f is bijective we need only show $(S_{f(i)} - \overline{B-S_o}) \cap (S_{f(i')} - \overline{B-S_o}) = \emptyset$ for $i \neq i'$. Now
$e' \in (S_{f(i)} - \overline{B-S_o}) \cap (S_{f(i')} - \overline{B-S_o}) \Longrightarrow e_i, e_{i'} \in \overline{(B-S_o) \cup \{e'\}} \Longrightarrow$
$\overline{(B-S_o) \cup \{e_i, e_{i'}\}} = \overline{(B-S_o) \cup \{e'\}}$, contradiction, as
$r((B-S_o) \cup \{e_i, e_{i'}\}) = m - |S_o| + 2$ and $r((B-S_o) \cup \{e'\}) \leqslant m - |S_o| + 1$.
Hence the e_i', $i \in I$, are distinct. Now $\bigwedge i \in I$
$e_i \in \overline{(B-S_o) \cup \{e_i' : i \in I\}}$, hence $(B-S_o) \cup \{e_i' : i \in I\} \in W$ by Theorem 7(j).

As each e_i', $i \in I$, lies in exactly one of the C_j, $j \in I$, namely $e_i' \in C_{f(i)}$, it follows, letting $I =: \{i_1, i_2, \dots, i_{|S_o|}\}$, that

$$\bigwedge j \in \{2,\dots,|S_o|\}$$

$$C_{f(i_j)} \subset (B' - \{e_{i_1}', \dots, e_{i_{j-1}}'\}) \cup \{e_{f(i_1)}, \dots, e_{f(i_j)}\} ,$$

hence it follows from (a) of the Lemma in §5.1 by induction that

$$\bigwedge j \in \{1,\dots,|S_o|\}$$

$$(B' - \{e_{i_1}', \dots, e_{i_j}'\}) \cup \{e_{f(i_1)}, \dots, e_{f(i_j)}\} \in W.$$

Thus we take $S_o' := \{e_i' : i \in I\}$.

Remarks.

It is natural to ask whether S_o and S'_o can be so chosen in Theorem 28, that the symmetric set exchange can be effected in a serial symmetric point exchange of $|S_o|$ steps. The matrix-matroid example considered in §5.2 yields the following counterexample.

Take $B := \{a_1, a_4, a_5\}$, $B' := \{a_2, a_3, a_6\}$, $S := \{a_1, a_4\}$, $S' := \{a_3, a_6\}$. Then one easily checks that there is just one possibility: $S_o := S$ and $S'_o := S'$, and no serial symmetric point exchange of two steps will effect this symmetric set exchange.

If however it is a question of finding some $S'_o \subset B'$ not necessarily with $S'_o \subset S'$, such that S'_o and a given $S_o \subset B$ can be exchanged symmetrically and a serial symmetric point exchange of $|S_o|$ steps exists, then the answer is yes if $|S_o| = 2$, as was proved by Greene and Magnanti [45]. In the above example $S'_o := \{a_2, a_3\}$ or $\{a_2, a_6\}$ would yield the required properties.

Bibliography

1. C.Berge: Graphes et Hypergraphes, (Dunod 1970).

2. C.Berge and A.Ghouila-Houri: Programmes, Jeux et Réseaux de Transport, (Dunod 1962).

* R.E.Bixby (see [38]).

3. J.A.Bondy:"Transversal matroids, base-orderable matroids, and graphs", Quart.J.Math.Oxford (2) 23 (1972) 81-89.

* T.J.Brown (see [39]).

* R.A.Brualdi (see [40]).

4. R.A.Brualdi and G.W.Dinolt: "Characterisations of transversal matroids and their presentations", J.Comb.Th. (B) 12 (1972) 268-286.

5. C.P.Bruter: Les Matroides, (Dunod 1970).

6. C.P.Bruter: Vue d'Ensemble sur la Théorie des Matroides, (Bull.Soc.Math.France, Mémoire 17, 1969).

* C.P.Bruter (see [41]).

* T.H.Brylawski (see [42]).

7. H.H.Crapo and G.-C.Rota: Combinatorial Geometries, (M.I.T. Press 1970).

8. E.W.Dijkstra: "A note on two problems in connexion with graphs", Num.Math.1 (1959) 269-271.

9. F.D.J.Dunstan and D.J.A.Welsh: "A greedy algorithm for solving a certain class of linear programmes", Math.Prog.5 (1973) 338-353.

10. J.Edmonds: "Submodular functions, matroids, and certain polyhedra", in: Combinatorial Structures and their Applications, Proc. Calgary Conf. 1969, edited by R.Guy et al., (Gordon & Breach 1970) 69-87.

11. J.Edmonds: "Matroids and the greedy algorithm", Math.Prog.1 (1971) 127-136.

12. J.Edmonds and D.R.Fulkerson: "Transversals and matroid partition", J.Res.Nat.Bur.Stand.(B) 69 (1965) 147-153.

* H.Gabow, F.Glover and D.Klingman (see [43]).

13. D.Gale: "Optimal assignments in an ordered set: an application of matroid theory", J.Comb.Th.4 (1968) 176-180.

14. C.Greene: "A multiple exchange property for bases", Proc. Amer.Math.Soc.39 (1973) 45-50.

* C.Greene (see [44]).

* C.Greene and T.L.Magnanti (see [45]).

15. F.Harary and D.J.A.Welsh: "Matroids versus graphs", in: The Many Facets of Graph Theory, Proc. Kalamazoo Conf. 1968, edited by G.Chartrand and S.F.Kapoor, Springer Lecture Notes in Mathematics No. 110, (Springer-Verlag 1969) 155-170.

16. C.A.Holzmann, P.G.Norton and M.D.Tobey: "A graphical representation of matroids", SIAM J.Appl.Math.25 (1973) 618-627.

17. A.W.Ingleton: "Representation of matroids", in: Combinatorial Mathematics and its Applications, Proc. Oxford Conf. 1969, edited by D.J.A.Welsh, (Academic Press 1971).

18. A.W.Ingleton and M.J.Piff: "Gammoids and transversal matroids", J.Comb.Th.(B) 15 (1973) 51-68.

19. J.B.Kruskal: "On the shortest spanning subtree of a graph and the travelling salesman problem", Proc.Amer.Math.Soc.7 (1956) 48-50.

20. K.Kuratowski: "Sur le problème des courbes gauches en topologie", Fund.Math.15 (1930) 271-283.

21. A.Lehman: "A solution of the Shannon switching game", J.Soc.Indust.Appl.Math.12 (1964) 687-725.

22. S.MacLane: "A combinatorial condition for planar graphs", Fund.Math.28 (1937) 22-32.

* M.J.Magazine, G.L.Nemhauser and L.E.Trotter,Jr. (see [46]).

23. J.H.Mason: "On a class of matroids arising from paths in graphs", Proc.Lond.Math.Soc.(3) 25 (1972) 55-74.

24. S.B.Maurer: "Matroid basis graphs I & II", J.Comb.Th.(B) 14 (1973) 216-240 and 15 (1973) 121-145.

25. G.J.Minty: "On the axiomatic foundations of the theories of directed linear graphs, electrical networks and network-programming", J.Math. and Mech.15 (1966) 485-520.

26. L.Mirsky: Transversal Theory, (Academic Press 1971).

* U.S.R.Murty (see [47]-[50]).

27. R.Rado: "Note on independence functions", Proc.Lond.Math. Soc.7 (1957) 300-320.

28. P.Rosenstiehl: "L'arbre minimum d'un graph", in: Théorie des Graphes, Proc. Rome Conf. 1966, edited by P.Rosenstiehl, (Dunod 1967) 357-368.

* G.-C.Rota (see [51]).

29. J.de Sousa and D.J.A.Welsh: "A characterisation of binary transversal structures", J.Math.Anal.Appl.40 (1972) 55-59.

30. W.T.Tutte: "Lectures on matroids", J.Res.Nat.Bur.Stand.(B) 69 (1965) 1-47.

31. W.T.Tutte: Introduction to the Theory of Matroids, (Elsevier 1971).

32. D.J.A.Welsh: "Kruskal's theorem for matroids", Proc.Camb. Phil.Soc.64 (1968) 3-4.

33. D.J.A.Welsh: "On the hyperplanes of a matroid", Proc.Camb. Phil.Soc.65 (1969) 11-18.

34. D.J.A.Welsh: "On matroid theorems of Edmonds and Rado", J.Lond.Math.Soc.(2) 2 (1970) 251-256.

35. H.Whitney: "On the abstract properties of linear dependence", Amer.J.Math.57 (1935) 509-533.

36. R.J.Wilson: "An introduction to matroid theory", Amer.Math. Monthly 80 (1973) 500-525.

37. D.R.Woodall: "An exchange theorem for bases of matroids", J.Comb.Th.(B) 16 (1974) 227-228.

38. R.E.Bixby: "ℓ-matrices and a characterization of binary matroids", Discrete Math.8 (1974) 139-145.

39. T.J.Brown: "Transversal theory and F-products", J.Comb. Th.(A) 17 (1974) 290-298.

40. R.A.Brualdi: "Comments on bases in dependence structures", Bull.Austral.Math.Soc.1 (1969) 161-167.

41. C.P.Bruter: Eléments de la Théorie des Matroides, Springer Lecture Notes in Mathematics No. 387, (Springer-Verlag 1974).

42. T.H.Brylawski: "Some properties of basic families of subsets", Discrete Math.6 (1973) 333-341.

43. H.Gabow, F.Glover and D.Klingman: "A note on exchanges in matroid bases", Research Report C.S.184 (1974), Center for Cybernetic Studies, University of Texas, Austin, Texas, USA.

44. C.Greene: "Another exchange property for bases", Proc.Amer. Math.Soc.46 (1974) 155-156.

45. C.Greene and T.L.Magnanti: "Some abstract pivot algorithms", Working Paper OR 037-74 (1974), Operations Research Center, MIT, Cambridge, Mass., USA.

46. M.J.Magazine, G.L.Nemhauser and L.E.Trotter,Jr.: "When the greedy solution solves a class of knapsack problems", MRC Technical Summary Report No. 1421 (1974), Mathematics Research Center, University of Wisconsin, Madison, Wisconsin, USA.

47. U.S.R.Murty: "Sylvester matroids", in: Recent Progress in Combinatorics, Proc. Third Waterloo Conf. on Combinatorics, edited by W.T.Tutte, (Academic Press 1969) 283-286.

48. U.S.R.Murty: "Equicardinal matroids and finite geometries", in: Combinatorial Structures and their Applications, Proc. Calgary Conf. 1969, edited by R.Guy et al., (Gordon & Breach 1970) 289-291.

49. U.S.R.Murty: "Matroids with Sylvester property", Aequationes Math.4 (1970) 44-50.

50. U.S.R.Murty: "Equicardinal matroids", J.Comb.Th.11 (1971) 120-126.

51. G.-C.Rota: "Combinatorial theory, old and new", Actes, Congrès Intern. Math., Nice (1970), Tome 3, (Gauthier-Villars, Paris 1971) 229-233.

Index

Vol. 59: J. A. Hanson, Growth in Open Economies. V, 128 pages. 1971. DM 18,-

Vol. 60: H. Hauptmann, Schätz- und Kontrolltheorie in stetigen dynamischen Wirtschaftsmodellen. V, 104 Seiten. 1971. DM 18,-

Vol. 61: K. H. F. Meyer, Wartesysteme mit variabler Bearbeitungsrate. VII, 314 Seiten. 1971. DM 27,-

Vol. 62: W. Krelle u. G. Gabisch unter Mitarbeit von J. Burgermeister, Wachstumstheorie. VII, 223 Seiten. 1972. DM 22,-

Vol. 63: J. Kohlas, Monte Carlo Simulation im Operations Research. VI, 162 Seiten. 1972. DM 18,-

Vol. 64: P. Gessner u. K. Spremann, Optimierung in Funktionenräumen. IV, 120 Seiten. 1972. DM 18,-

Vol. 65: W. Everling, Exercises in Computer Systems Analysis. VIII, 184 pages. 1972. DM 20,-

Vol. 66: F. Bauer, P. Garabedian and D. Korn, Supercritical Wing Sections. V, 211 pages. 1972. DM 22,-

Vol. 67: I. V. Girsanov, Lectures on Mathematical Theory of Extremum Problems. V, 136 pages. 1972. DM 18,-

Vol. 68: J. Loeckx, Computability and Decidability. An Introduction for Students of Computer Science. VI, 76 pages. 1972. DM 18,-

Vol. 69: S. Ashour, Sequencing Theory. V, 133 pages. 1972. DM 18,-

Vol. 70: J. P. Brown, The Economic Effects of Floods. Investigations of a Stochastic Model of Rational Investment. Behavior in the Face of Floods. V, 87 pages. 1972. DM 18,-

Vol. 71: R. Henn und O. Opitz, Konsum- und Produktionstheorie II. V, 134 Seiten. 1972. DM 18,-

Vol. 72: T. P. Bagchi and J. G. C. Templeton, Numerical Methods in Markov Chains and Bulk Queues. XI, 89 pages. 1972. DM 18,-

Vol. 73: H. Kiendl, Suboptimale Regler mit abschnittweise linearer Struktur. VI, 146 Seiten. 1972. DM 18,-

Vol. 74: F. Pokropp, Aggregation von Produktionsfunktionen. VI, 107 Seiten. 1972. DM 18,-

Vol. 75: GI-Gesellschaft für Informatik e.V. Bericht Nr. 3. 1. Fachtagung über Programmiersprachen · München, 9.-11. März 1971. Herausgegeben im Auftrag der Gesellschaft für Informatik von H. Langmaack und M. Paul. VII, 280 Seiten. 1972. DM 27,-

Vol. 76: G. Fandel, Optimale Entscheidung bei mehrfacher Zielsetzung. 121 Seiten. 1972. DM 18,-

Vol. 77: A. Auslender, Problèmes de Minimax via l'Analyse Convexe et les Inégalités Variationelles: Théorie et Algorithmes. VII, 132 pages. 1972. DM 18,-

Vol. 78: GI-Gesellschaft für Informatik e.V. 2. Jahrestagung, Karlsruhe, 2.-4. Oktober 1972. Herausgegeben im Auftrag der Gesellschaft für Informatik von P. Deussen. XI, 576 Seiten. 1973. DM 40,-

Vol. 79: A. Berman, Cones, Matrices and Mathematical Programming. V, 96 pages. 1973. DM 18,-

Vol. 80: International Seminar on Trends in Mathematical Modelling, Venice, 13-18 December 1971. Edited by N. Hawkes. VI, 288 pages. 1973. DM 27,-

Vol. 81: Advanced Course on Software Engineering. Edited by F. L. Bauer. XII, 545 pages. 1973. DM 35,-

Vol. 82: R. Saeks, Resolution Space, Operators and Systems. X, 267 pages. 1973. DM 24,-

Vol. 83: NTG/GI-Gesellschaft für Informatik, Nachrichtentechnische Gesellschaft. Fachtagung „Cognitive Verfahren und Systeme", Hamburg, 11.-13. April 1973. Herausgegeben im Auftrag der NTG/GI von Th. Einsele, W. Giloi und H.-H. Nagel. VIII, 373 Seiten. 1973. DM 32,-

Vol. 84: A. V. Balakrishnan, Stochastic Differential Systems I. Filtering and Control. A Function Space Approach. V, 252 pages. 1973. DM 24,-

Vol. 85: T. Page, Economics of Involuntary Transfers: A Unified Approach to Pollution and Congestion Externalities. XI, 159 pages. 1973. DM 20,-

Vol. 86: Symposium on the Theory of Scheduling and Its Applications. Edited by S. E. Elmaghraby. VIII, 437 pages. 1973. DM 35,-

Vol. 87: G. F. Newell, Approximate Stochastic Behavior of n-Server Service Systems with Large n. VIII, 118 pages. 1973. DM 18,-

Vol. 88: H. Steckhan, Güterströme in Netzen. VII, 134 Seiten. 1973. DM 18,-

Vol. 89: J. P. Wallace and A. Sherret, Estimation of Product. Attributes and Their Importances. V, 94 pages. 1973. DM 18,-

Vol. 90: J.-F. Richard, Posterior and Predictive Densities for Simultaneous Equation Models. VI, 226 pages. 1973. DM 22,-

Vol. 91: Th. Marschak and R. Selten, General Equilibrium with Price-Making Firms. XI, 246 pages. 1974. DM 24,-

Vol. 92: E. Dierker, Topological Methods in Walrasian Economics. IV, 130 pages. 1974. DM 18,-

Vol. 93: 4th IFAC/IFIP International Conference on Digital Computer Applications to Process Control, Zürich/Switzerland, March 19-22, 1974. Edited by M. Mansour and W. Schaufelberger. XVIII, 544 pages. 1974. DM 40,-

Vol. 94: 4th IFAC/IFIP International Conference on Digital Computer Applications to Process Control, Zürich/Switzerland, March 19-22, 1974. Edited by M. Mansour and W. Schaufelberger. XVIII, 546 pages. 1974. DM 40,-

Vol. 95: M. Zeleny, Linear Multiobjective Programming. XII, 220 pages. 1974. DM 22,-

Vol. 96: O. Moeschlin, Zur Theorie von Neumannscher Wachstumsmodelle. XI, 115 Seiten. 1974. DM 16,-

Vol. 97: G. Schmidt, Über die Stabilität des einfachen Bedienungskanals. VII, 147 Seiten. 1974. DM 16,-

Vol. 98: Mathematical Methods in Queueing Theory. Proceedings of a Conference at Western Michigan University, May 10-12, 1973. Edited by A. B. Clarke. VII, 374 pages. 1974. DM 28,-

Vol. 99: Production Theory. Edited by W. Eichhorn, R. Henn, O. Opitz, and R. W. Shephard. VIII, 386 pages. 1974. DM 32,-

Vol. 100: B. S. Duran and P. L. Odell, Cluster Analysis. A survey. VI, 137 pages. 1974. DM 18,-

Vol. 101: W. M. Wonham, Linear Multivariable Control. A Geometric Approach. X, 344 pages. 1974. DM 30,-

Vol. 102: Analyse Convexe et Ses Applications. Comptes Rendus, Janvier 1974. Edited by J.-P. Aubin. IV, 244 pages. 1974. DM 25,-

Vol. 103: D. E. Boyce, A. Farhi, R. Weischedel, Optimal Subset Selection. Multiple Regression, Interdependence and Optimal Network Algorithms. XIII, 187 pages. 1974. DM 20,-

Vol. 104: S. Fujino, A Neo-Keynesian Theory of Inflation and Economic Growth. V, 96 pages. 1974. DM 18,-

Vol. 105: Optimal Control Theory and its Applications. Part I. Proceedings of the Fourteenth Biennual Seminar of the Canadian Mathematical Congress. University of Western Ontario, August 12-25, 1973. Edited by B. J. Kirby. VI, 425 pages. 1974. DM 35,-

Vol. 106: Optimal Control Theory and its Applications. Part II. Proceedings of the Fourteenth Biennial Seminar of the Canadian Mathematical Congress. University of Western Ontario, August 12-25, 1973. Edited by B. J. Kirby. VI, 403 pages. 1974. DM 35,-

Vol. 107: Control Theory, Numerical Methods and Computer Systems Modelling. International Symposium, Rocquencourt, June 17-21, 1974. Edited by A. Bensoussan and J. L. Lions. VIII, 757 pages. 1975. DM 53,-

Vol. 108: F. Bauer et al., Supercritical Wing Sections II. A Handbook. V, 296 pages. 1975. DM 28,-

Vol. 109: R. von Randow, Introduction to the Theory of Matroids. IX, 102 pages. 1975. DM 18,-

Ökonometrie und Unternehmensforschung
Econometrics and Operations Research

Vol. I Nichtlineare Programmierung. Von H. P. Künzi und W. Krelle unter Mitwirkung von W. Oettli. - Mit 18 Abbildungen. XV, 221 Seiten. 1962. Geb. DM 38,-

Vol. II Lineare Programmierung und Erweiterungen. Von G. B. Dantzig. Ins Deutsche übertragen und bearbeitet von A. Jaeger. - Mit 103 Abbildungen. XVI, 712 Seiten. 1966. Geb. DM 68,-

Vol. III Stochastic Processes. By M. Girault. - With 35 figures. XII, 126 pages. 1966. Cloth DM 28,-

Vol. IV Methoden der Unternehmensforschung im Versicherungswesen. Von K.-H. Wolff. - Mit 14 Diagrammen. VIII, 266 Seiten. 1966. Geb. DM 49,-

Vol. V The Theory of Max-Min and its Application to Weapons Allocation Problems. By John M. Danskin. - With 6 figures. X, 126 pages. 1967. Cloth DM 32,-

Vol. VI Entscheidungskriterien bei Risiko. Von H. Schneeweiss. - Mit 35 Abbildungen. XII, 214 Seiten. 1967. Geb. DM 48,-

Vol. VII Boolean Methods in Operations Research and Related Areas. By P. L. Hammer (Ivănescu) and S. Rudeanu. With a preface by R. Bellman. - With 25 figures. XVI, 329 pages. 1968. Cloth DM 46,-

Vol. VIII Strategy for R & D: Studies in the Microeconomics of Development. By Th. Marschak, Th. K. Glennan JR., and R. Summers. - With 44 figures. XIV, 330 pages. 1967. Cloth DM 56,80

Vol. IX Dynamic Programming of Economic Decisions. By M. J. Beckmann. - With 9 figures XII, 143 pages. 1968. Cloth DM 28,-

Vol. X Input-Output-Analyse. Von J. Schumann. - Mit 12 Abbildungen. X, 311 Seiten. 1968. Geb. DM 58,-

Vol. XI Produktionstheorie. Von W. Wittmann. - Mit 54 Abbildungen. VIII, 177 Seiten. 1968. Geb. DM 42,-

Vol. XII Sensivitätsanalysen und parametrische Programmierung. Von W. Dinkelbach. - Mit 20 Abbildungen. XI, 190 Seiten. 1969. Geb. DM 48,-

Vol. XIII Graphentheoretische Methoden und ihre Anwendungen. Von W. Knödel. - Mit 24 Abbildungen. VIII, 111 Seiten. 1969. Geb. DM 38,-

Vol. XIV Praktische Studien zur Unternehmensforschung. Von E. Nievergelt, O. Müller, F. E. Schlaepfer und W. H. Landis. - Mit 82 Abbildungen. XII, 240 Seiten. Geb. DM 58,-

Vol. XV Optimale Reihenfolgen. Von H. Müller-Merbach. - Mit 43 Abbildungen. IX, 225 Seiten. 1970. Geb. DM 60,-

Vol. XVI Preispolitik der Mehrproduktenunternehmung in der statischen Theorie. Von R. Selten. - Mit 20 Abbildungen. VIII, 195 Seiten. 1970. Geb. DM 64,-

Vol. XVII Information Theory for Systems Engineers. By L. P. Hyvärinen. - With 42 figures. VIII, 197 pages. 1970. Cloth DM 44,-

Vol. XVIII Unternehmensforschung im Bergbau. Von F. L. Wilke. - Mit 29 Abbildungen. VIII, 150 Seiten. 1972. Geb. DM 54,-