CIME Summer Schools

83

A. Barlotti (Ed.)

Matroid Theory and its Applications

Varenna, Italy 1980

Springer

Fondazione CIME
Roberto Conti

A. Barlotti (Ed.)

Matroid Theory and Its Applications

Lectures given at a Summer School of the
Centro Internazionale Matematico Estivo (C.I.M.E.),
held in Varenna (Como), Italy,
August 24 - September 2, 1980

Springer

FONDAZIONE
CIME
ROBERTO CONTI

C.I.M.E. Foundation
c/o Dipartimento di Matematica “U. Dini”
Viale Morgagni n. 67/a
50134 Firenze
Italy
cime@math.unifi.it

ISBN 978-3-642-11109-9 e-ISBN: 978-3-642-11110-5
DOI:10.1007/978-3-642-11110-5
Springer Heidelberg Dordrecht London New York

Reprint of the 1st ed. C.I.M.E., Ed. Liguori, Napoli & Birkhäuser 1982
With kind permission of C.I.M.E.

Printed on acid-free paper

Springer.com

CONTENTS

CENTRO INTERNAZIONALE MATEMATICO ESTIVO

(C.I.M.E.)

UN'INTRODUZIONE ALLA TEORIA DELLE FUNZIONI DI MÖBIUS

M. BARNABEI - A.BRINI - G.C.ROTA

UN'INTRODUZIONE ALLA TEORIA DELLE FUNZIONI DI MÖBIUS

Marilena Barnabei
(Università di Ferrara)
Andrea Brini
(Università di Bologna)
Gian-Carlo Rota
(Massachusetts Institute of Technology)

1. Introduzione

Le idee principali che ci sono servite da guida e che vengono sviluppate in queste note sono le seguenti. In primo luogo si adotta pienamente la dualità tra il concetto di insieme parzialmente ordinato e quello di reticolo distributivo, idea che risale a Garrett Birkhoff e che è stata ulteriormente sviluppata da M.H. Stone, fino ad ottenere la versione definitiva nella tesi oxfordiana di Ann Priestley. Nel caso più semplice degli insiemi parzialmente ordinati finiti, questa dualità si riduce all'osservazione che ogni famiglia finita di sottoinsiemi di un insieme qualsiasi, chiusa per intersezione e unione - ma non sempre per complementazione - è funtorialmente isomorfa alla famiglia di tutti i sottoinsiemi decrescenti di un insieme parzialmente ordinato.

Questo fatto si esprime in modo naturale nell'equivalenza tra la categoria degli insiemi parzialmente ordinati finiti e la categoria dei reticoli distributivi finiti. In linea di massima, si può pensare che ogni proprietà combinatoria di insiemi parzialmente ordinati sia esprimibile in modo equivalente mediante i reticoli distributivi. In generale, l'espressione di tali proprietà in termini di reticoli distributivi è preferibile, non solo perché permette a volte generalizzazioni al caso infinito, ma soprattutto perché si inserisce più agevolmente nella problematica dell'algebra e della logica di oggi.

In secondo luogo, sviluppiamo il concetto di anello di valutazione di un reticolo distributivo, concetto che esprime in forma algebrica un processo di linearizzazione noto da tempo in analisi funzionale, cioè il passaggio da una misura su una famiglia di insiemi all'integrale sull'anello di funzioni semplici ad essa associate. Questo processo di linearizzazione ci permette di studiare le valutazioni su un reticolo distributivo come funzionali lineari sull'anello di valutazione, in analogia con lo studio della caratteristica di Eulero per le unioni finite di convessi - e più generalmente con i Quartermassintegrali di Minkowski - fatto da Hadwiger e dalla scuola di Blaschke per la geometria integrale.

Infatti, ancora sulle orme della geometria integrale, riusciamo a definire un analogo combinatorio della caratteristica di Eulero per i reticoli distributivi finiti (e quindi per gli insiemi parzialmente ordinati), come la valutazione, evidentemente unica, che prende il valore unità sugli elementi sup-irriducibili (o "coni") non zero. L'espressione di questa caratteristica di Eulero mediante la funzione di Möbius non è che un'estrema generalizzazione della nota formula di Eulero-Schläfli per i poliedri.

La teoria delle funzioni di Möbius degli insiemi parzialmente ordinati viene quindi sviluppata in base a questo legame fondamentale con la caratteristica di Eulero. Riusciamo così a ritrovare in forma semplice e, vorremmo credere, definitiva, le identità scoperte finora per le funzioni di Möbius, nonché varie disuguaglianze profonde dovute a C. Greene, e le eleganti applicazioni geometriche dovute a T. Zaslavsky.

Nei paragrafi 3 e 4 sviluppiamo dettagliatamente la struttura algebrica dell'anello aumentato di valutazione, introdotto da uno di noi e poi studiato da L. Geissinger in tre eleganti lavori. Troviamo così che con l'uso sistematico dell'aumentazione si semplificano varie dimostrazioni. Si può affermare che, con il concetto di anello di valutazione aumentato, la classica dualità insiemistico-booleana viene linearizzata.

Il presente materiale, con l'eccezione del paragrafo conclusivo riguardante le applicazioni della teoria delle funzioni di Möbius al problema classico dell'enumerazione delle regioni determinate da un sistema di iperpiani <u>non</u> in posizione generica nello spazio affine o proiettivo, è stato oggetto di alcune delle lezioni del Corso CIME tenuto a Varenna nell'agosto 1980.

La lettura di queste note non richiede particolari conoscenze preliminari, al di fuori di alcune elementari nozioni di algebra commutativa.

2. <u>Reticoli distributivi ed insiemi parzialmente ordinati</u>

Nel seguito, L indicherà un reticolo distributivo finito.

Un elemento $p \in L$ si dice <u>sup-irriducibile</u> se $p = a \vee b$ implica $p = a$ oppure $p = b$.

L'insieme $J(L)$ degli elementi sup-irriducibili di L, con l'ordine indotto, è un insieme parzialmente ordinato dotato di minimo. Indicheremo con $\hat{J}(L)$ l'insieme parzialmente ordinato ottenuto da $J(L)$ togliendo il minimo.

2.1. PROPOSIZIONE Ogni elemento del reticolo distributivo L può essere espresso in uno ed in un solo modo come sup di elementi sup-irriducibili a due a due non confrontabili.

DIMOSTRAZIONE Essendo L finito, si riconosce immediatamente che ogni elemento di L si può esprimere come sup di elementi sup-irriducibili; ci limiteremo perciò a dimostrare l'unicità della rappresentazione. A questo scopo, ricordiamo che, se p è un elemento sup-irriducibile in L e $p \leq a \vee b$, allora $p \leq a$ oppure $p \leq b$. Supponiamo ora che $\{p_1, p_2, \dots, p_n\}$ e $\{q_1, q_2, \dots, q_k\}$ siano insiemi di elementi sup-irriducibili a due a due non confrontabili, tali che

$$p_1 \vee p_2 \vee \dots \vee p_n = q_1 \vee q_2 \vee \dots \vee q_k \quad .$$

Grazie all'osservazione precedente, si ottiene, ad esempio, $q_1 \leq p_1$; d'altra parte

$$p_1 = (p_1 \wedge (q_2 \vee \dots \vee q_k)) \vee q_1$$

da cui si deduce $p_1 = q_1$. Iterando questo ragionamento, si prova la tesi.■

Sia P un insieme parzialmente ordinato finito. Un sottoinsieme I di P si dice ideale se $x \leq y \in I$ implica $x \in I$.

La famiglia $\mathcal{I}(P)$ degli ideali di P , con le operazioni di unione e intersezione, risulta essere un sottoreticolo dell'algebra di Boole su P , ed è quindi un reticolo distributivo.

Un sottoinsieme F di P si dice filtro se $x \geq y \in F$ implica $x \in F$.

Un ideale I di P si dice principale se esiste $p \in P$ tale che $I = \{x \in P;\ x \leq p\}$. Analogamente, un filtro F di P si dice principale se esiste $p \in P$ tale che $F = \{x \in P;\ x \geq p\}$.

2.2. PROPOSIZIONE Sia L un reticolo distributivo finito, sia $\hat{J}(L)$ l'insieme parzialmente ordinato dei sup-irriducibili di L privato del minimo, e sia $\mathcal{I}(\hat{J}(L))$ il reticolo degli ideali di $\hat{J}(L)$. Allora, L e $\mathcal{I}(\hat{J}(L))$ sono isomorfi.

DIMOSTRAZIONE L'applicazione

$$\begin{aligned} L &\longrightarrow \mathcal{I}(\hat{J}(L)) \\ x &\longrightarrow \{y \in \hat{J}(L);\ y \leq x\} \end{aligned}$$

è biiettiva e preserva l'ordine, quindi è un isomorfismo di reticoli.■

2.3. PROPOSIZIONE Sia P un insieme parzialmente ordinato finito, e sia $\mathcal{I}(P)$ il reticolo distributivo degli ideali di P. Allora P e $\hat{J}(\mathcal{I}(P))$ sono isomorfi.

DIMOSTRAZIONE E' sufficiente osservare che gli elementi di $\hat{J}(\mathcal{I}(P))$ sono tutti e soli i sottoinsiemi di P della forma

$$I_p = \{x \in P;\ x \leq p\} ,$$

con $p \in P$. Si verifica immediatamente che l'applicazione

$$\begin{aligned} P &\longrightarrow \hat{J}(\mathcal{I}(P)) \\ p &\longrightarrow I_p \end{aligned}$$

è biiettiva e preserva l'ordine.■

2.4. PROPOSIZIONE Sia P un insieme parzialmente ordinato finito, e P^* il suo duale d'ordine. Allora $\mathcal{I}(P^*)$ è il duale d'ordine di $\mathcal{I}(P)$.

DIMOSTRAZIONE Osserviamo che $\mathcal{I}(P^*)$ è il reticolo dei filtri di P. Poiché l'insieme complementare di un ideale è un filtro e viceversa, l'applicazione

$$\begin{aligned} \mathcal{I}(P) &\longrightarrow \mathcal{I}(P^*) \\ I &\longrightarrow P-I \end{aligned}$$

risulta un antiisomorfismo di reticoli.∎

Siano L_1, L_2 reticoli finiti. Un'applicazione

$$\alpha : L_1 \longrightarrow L_2$$

si dirà <u>u-z morfismo</u> di reticoli se è un morfismo reticolare e fa corrispondere il massimo di L_1 al massimo di L_2 e il minimo di L_1 al minimo di L_2.

2.5. TEOREMA La categoria dei reticoli distributivi finiti con gli u-z morfismi è funtorialmente equivalente alla categoria degli insiemi parzialmente ordinati finiti con i morfismi d'ordine.

DIMOSTRAZIONE Siano P_1, P_2 due insiemi parzialmente ordinati finiti, e sia

$$\alpha : P_1 \longrightarrow P_2$$

un morfismo d'ordine. Siano $\mathcal{I}(P_1)$ e $\mathcal{I}(P_2)$ i reticoli degli ideali di P_1 e P_2, rispettivamente. Definiamo un'applicazione

$$\alpha' : \mathcal{I}(P_2) \longrightarrow \mathcal{I}(P_1)$$

ponendo

$$\alpha'(I) = \{x \in P_1;\ \alpha(x) \in I\}$$

dove $I \in \mathcal{I}(P_2)$; α' risulta evidentemente un u-z morfismo di reticoli.

Viceversa, siano L_1, L_2 reticoli distributivi finiti, e sia

$$\beta : L_1 \longrightarrow L_2$$

un u-z morfismo; definiamo un'applicazione

$$\beta' : \hat{J}(L_2) \longrightarrow \hat{J}(L_1)$$

ponendo

$$\beta'(p) = \min \{x \in \hat{J}(L_1);\ \beta(x) = p\} \quad ,$$

dove $p \in \hat{J}(L_2)$.

La definizione di β' è ben posta, in quanto, se $x, y \in \hat{J}(L_1)$ sono tali che $\beta(x) = p = \beta(y)$ e sono minimali rispetto a tale condizione, allora $\beta(x \wedge y) = p$; sia $x \wedge y = p_1 \vee p_2 \vee \dots \vee p_n$, con p_i sup-irriducibile per ogni i. Poiché p è a sua volta sup-irriducibile, deve esistere un indice j tale che $\beta(p_j) = p$; dato che x,y sono minimali, si ha necessariamente $x = p_j = y$.

Si verifica poi immediatamente che β' è un morfismo d'ordine.

Utilizzando le costruzioni precedenti si completa la dimostrazione.■

3. Coni di valutazione

Sia A un anello, e sia ε una aumentazione per A, cioè un morfismo di anelli da A all'anello $\mathbb{Z}$ degli interi.

Definiamo ora una nuova operazione su A, che chiameremo moltiplicazione di Geissinger, e indicheremo con $*$, ponendo

$$a * b = \varepsilon(a)b + a\varepsilon(b) - ab$$

per ogni $a,b \in A$.

3.1. PROPOSIZIONE $(A,+,*)$ è un anello; inoltre, $(A,+,*)$ è commutativo se e solo se A è commutativo.

DIMOSTRAZIONE Per ogni $a,b,c \in A$ si ha:

i) $a*(b*c) = a*(\varepsilon(b)c + b\varepsilon(c) - bc) =$

$= \varepsilon(a)\varepsilon(b)c + \varepsilon(a)b\varepsilon(c) - \varepsilon(a)bc + a\varepsilon(b)\varepsilon(c) +$

$+ a\varepsilon(b)\varepsilon(c) - a\varepsilon(b)\varepsilon(c) - a\varepsilon(b)c - ab\varepsilon(c) + abc$.

L'espressione così ottenuta è una funzione simmetrica in a, b, c, quindi

$$a*(b*c) = (a*b)*c \quad .$$

ii) $a*(b+c) = \varepsilon(a)(b+c) + a(\varepsilon(b) + \varepsilon(c)) - a(b+c) =$

$= \varepsilon(a)b + \varepsilon(a)c + a\varepsilon(b) + a\varepsilon(c) - ab - ac$;

$(a*b) + (a*c) = \varepsilon(a)b + a\varepsilon(b) - ab + \varepsilon(a)c + a\varepsilon(c) - ac$.

Analogamente si dimostra l'altra legge distributiva.

L'ultima affermazione dell'enunciato segue direttamente dalla definizione dell'operazione $*$. ■

3.2. COROLLARIO L'aumentazione ε di A è un'aumentazione per l'anello $(A,+,*)$. Inoltre, la moltiplicazione di Geissinger di $(A,+,*)$ è la moltiplicazione di A. ■

Sia A un anello con aumentazione ε. Un elemento $z \in A$ si dirà <u>integrale</u> se risulta:

i) $\varepsilon(z) = 1$

ii) $\varepsilon(a)z = az$ per ogni $a \in A$.

3.3. PROPOSIZIONE Sia z un integrale di A; allora, z è l'elemento neutro dell'operazione $*$. Viceversa, se A possiede elemento neutro moltiplicativo ν, questo è un integrale per $(A,+,*)$. In particolare l'integrale, se esiste, è unico. ■

Un <u>semianello</u> $S(+,\cdot)$ sarà nel seguito una struttura dotata di due operazioni tali che

i) $S(+)$ ed $S(\cdot)$ siano semigruppi;

ii) in $S(+)$ valga la legge di cancellazione;

iii) $a(b+c) = ab+ac$

$(a+b)c = ac+bc$

per ogni $a,b,c \in S$.

Un'<u>aumentazione</u> di S sarà un'applicazione

$$\varepsilon: S \longrightarrow \mathbb{N}$$

che risulti un morfismo di semianelli.

Un cono di valutazione è un semianello commutativo unitario S con una aumentazione ε, dotato di integrale, e tale che sia definita in S un'operazione $*$ che soddisfi l'identità:

$$a * b + ab = a\varepsilon(b) + \varepsilon(a)b$$

per ogni $a, b \in S$.

Osserviamo che, nelle precedenti ipotesi, la struttura $(S,+,*)$ risulta anch'essa un cono di valutazione.

Siano S_1, S_2 coni di valutazione; un'applicazione

$$\varphi: S_1 \longrightarrow S_2$$

si dirà morfismo di coni di valutazione se φ è un morfismo di semianelli, ed inoltre:

i) $\varphi(a * b) = \varphi(a) * \varphi(b)$;

ii) $\varepsilon(\varphi(a)) = \varepsilon(a)$

per ogni $a, b \in S_1$.

3.4. PROPOSIZIONE (Principio di inclusione-esclusione)

Sia S un cono di valutazione, e siano $a_1, a_2, \ldots, a_n \in S$. Allora:

$$a_1 * a_2 * \ldots * a_n + \sum_{i<j} \varepsilon(a_i)\varepsilon(a_j)a_1 \ldots \hat{a}_i \ldots \hat{a}_j \ldots a_n +$$

$$+ \sum_{i<j<h<k} \varepsilon(a_i)\varepsilon(a_j)\varepsilon(a_h)\varepsilon(a_k)a_1 \ldots \hat{a}_i \ldots \hat{a}_j \ldots \hat{a}_h \ldots \hat{a}_k \ldots$$

$$\ldots a_n + \ldots = \sum_i \varepsilon(a_i)\, a_1 \ldots \hat{a}_i \ldots a_n +$$

$$+ \sum_{i<j<k} \varepsilon(a_i)\varepsilon(a_j)\varepsilon(a_k)\ a_1 \dots \hat{a}_i \dots \hat{a}_j \dots \hat{a}_k \dots a_n + \dots$$

DIMOSTRAZIONE Segue per induzione su n.∎

Sia L un reticolo distributivo finito.

Consideriamo il semigruppo abeliano libero su L e definiamo su questo semigruppo una struttura di semianello ponendo

$$x \cdot y = x \wedge y$$

se $x,y \in L$, ed estendendo il prodotto così definito per linearità. Tale semianello sarà indicato con $\mathbb{N}[L,\wedge]$.

Consideriamo ora le congruenze

$$(*) \qquad x \vee y + x \wedge y = x + y$$

per $x,y \in L$.

Osserviamo che le congruenze $(*)$ sono compatibili con la struttura di semianello, in quanto, per ogni $a \in L$ e per ogni $x,y \in L$:

$$a(x \vee y + x \wedge y) = (a \wedge x) \vee (a \wedge y) + (a \wedge x) \wedge (a \wedge y)$$

e

$$a(x+y) = (a \wedge x) + (a \wedge y) \ .$$

Quindi, è ben definito il semianello quoziente di $\mathbb{N}[L,\wedge]$ rispetto alle congruenze $(*)$. Tale semianello si indicherà con $V(L)$.

Diremo elementi puri di $V(L)$ quelli che sono immagine di elementi di L nell'immersione canonica $L \to V(L)$.

Definiamo ora un'applicazione:

$$\varepsilon : V(L) \to \mathbb{N}$$

nel modo seguente:

i) $\varepsilon(x) = 1$ se x è puro;

ii) $\varepsilon(\sum_i x_i) = \sum_i \varepsilon(x_i)$ con x_i puro per ogni i.

ε risulta perciò un'aumentazione per $V(L)$.

Si ha poi immediatamente che il massimo u del reticolo corrisponde all'unità del semianello, e che il minimo z del reticolo corrisponde all'integrale del semianello, cioè $\varepsilon(z) = 1$ e $z \cdot x = \varepsilon(x)z$ per ogni $x \in V(L)$.

Definiamo ora un'operazione su $V(L)$, che indicheremo con $*$, nel modo seguente:

$$x * y = x \vee y \qquad \text{se } x,y \text{ sono puri}$$

$$(\sum_i x_i) * (\sum_j y_j) = \sum_{i,j} (x_i \vee y_j) \quad ,$$

dove x_i, y_j sono puri per ogni i,j.

Questa definizione non dipende dalla rappresentazione mediante elementi puri che è stata scelta, poiché, se a,b,c sono puri, si ha

$$a \vee (b \vee c + b \wedge c) = a \vee (b + c) \quad .$$

3.5. PROPOSIZIONE Se $f,g \in V(L)$ si ha:

$$f * g + f g = f\, \varepsilon(g) + \varepsilon(f) g \quad .$$

DIMOSTRAZIONE Siano $f = \sum_i x_i$, $g = \sum_j y_j$, x_i, y_j puri. Allora

$$f \ast g + fg = \sum_{i,j} (x_i \vee y_j) + \sum_{i,j} (x_i \wedge y_j) = \sum_{i,j} (x_i + y_j) =$$

$$= \varepsilon(g) \sum_i x_i + \varepsilon(f) \sum_j y_j \quad . \blacksquare$$

Di conseguenza, $V(L)$ risulta un cono di valutazione.

Diremo cono ridotto del reticolo distributivo L il semianello $V_o(L)$ quoziente del cono di valutazione $V(L)$ rispetto al semiideale generato dall'integrale z :

$$V_o(L) = V(L)/\langle z \rangle \quad .$$

3.6. PROPOSIZIONE Sia P un insieme parzialmente ordinato finito, e $\mathscr{I}(P)$ il reticolo distributivo degli ideali d'ordine di P.
Una funzione

$$f : P \rightarrow \mathbb{N}$$

è decrescente se e solo se esistono $x_1, x_2, \dots, x_n \in \mathscr{I}(P)$ e $c_1, \dots, c_n \in \mathbb{N}$ tali che

$$f = \sum_{i=1}^{n} c_i I_{x_i}$$

dove I_{x_i} è la funzione caratteristica dell'ideale x_i .

DIMOSTRAZIONE Sia $f : P \rightarrow \mathbb{N}$ decrescente. Dato che P è finito, f assume un numero finito di valori non nulli; siano $v_1 < v_2 < \dots < v_n$ questi valori. Poniamo

$$A_o = \{ p \in P;\ f(p) > 0 \}$$

$$A_i = \{ p \in P;\ f(p) > v_i \} \qquad i = 1, \dots, n-1 \ .$$

Ciascuno degli insiemi $A_o, A_1, \dots, A_{n-1}$ è un ideale d'ordine di P. La funzione

$$f_1 = f - v_1 I_{A_o}$$

è anch'essa decrescente, ed inoltre

$$f_1(p) = \begin{cases} f(p) - v_1 & \text{se } p \in \bigcup_{i=1}^{n-1} A_i \\ 0 & \text{altrimenti} \end{cases}$$

Per induzione si ha allora

$$f = v_1 I_{A_o} + (v_2 - v_1) I_{A_1} + \dots + (v_{n-1} - v_{n-2}) I_{A_{n-1}} \ .$$

Dato che ciascun A_i è un elemento di $\mathscr{J}(P)$, l'affermazione è vera.

Viceversa, è ovvio che ogni I_A, con $A \in \mathscr{J}(P)$, è una funzione decrescente su P. ■

Da questo risultato si deduce il seguente teorema di struttura:

3.7. TEOREMA Per ogni reticolo distributivo finito L, il cono ridotto $V_o(L)$ è isomorfo al semianello delle funzioni decrescenti sull'ordine parziale $\hat{J}(L)$, a valori in $\mathbb{N}$. ■

4. Anello di valutazione di un reticolo distributivo

Sia L un reticolo distributivo finito ed M un semigruppo abeliano, nel quale valga la legge di cancellazione. Una valutazione su L è una funzione

$$f : L \rightarrow M$$

tale che

$$f(a \vee b) + f(a \wedge b) = f(a) + f(b)$$

per ogni a,b nel reticolo.

Se poi $f : L \rightarrow M$ è una valutazione che associa al minimo z di L l'elemento neutro del semigruppo M, f si dice misura.

Sia A un anello unitario; una valutazione $f : L \rightarrow A$ si dice moltiplicativa se, per ogni $x, y \in L$, risulta

$$f(x \wedge y) = f(x)\, f(y) \quad .$$

4.1. PROPOSIZIONE L'immersione canonica

$$i : L \rightarrow V(L)$$

del reticolo distributivo L nel suo cono di valutazione è la valutazione universale su L, cioè, per ogni semigruppo M e per ogni valutazione

$$f : L \rightarrow M \quad ,$$

esiste un morfismo di semigruppi

$$\varphi : V(L) \rightarrow M$$

tale che

$$f = \varphi \circ i \quad .$$

DIMOSTRAZIONE Definiamo $\varphi: V(L) \to M$ nel modo seguente:

1) $\varphi(x) = f(i^{-1}(x))$ se x è puro;

2) se $x = \sum_k a_k$, con a_k puro per ogni k ,

poniamo

$$\varphi(x) = \sum_k f(i^{-1}(a_k)) \quad .$$

Dato che f è una valutazione, questa definizione non dipende dalla rappresentazione di x mediante elementi puri.■

4.2. PROPOSIZIONE Un morfismo di reticoli distributivi finiti

$$\varphi: L_1 \to L_2$$

induce un (unico) morfismo di coni di valutazione

$$\varphi' : V(L_1) \to V(L_2)$$

tale che

$$\varphi' \circ i_1 = i_2 \circ \varphi \ ,$$

dove i_1, i_2 sono le immersioni di L_1 in $V(L_1)$ e di L_2 in $V(L_2)$, rispettivamente.

DIMOSTRAZIONE E` sufficiente osservare che, prolungando per linearità la φ a $\mathbb{N}[L,\wedge]$, si ottiene una funzione che rispetta le congruenze

$$a \vee b + a \wedge b = a + b$$

e che quindi è ben definita su $V(L)$. ■

4.3. PROPOSIZIONE Siano L_1, L_2 reticoli distributivi, e sia

$$\varphi' : V(L_1) \to V(L_2)$$

un morfismo di coni di valutazione. Allora esiste un unico morfismo di reticoli

$$\varphi: L_1 \longrightarrow L_2$$

tale che

$$\varphi' \circ i_1 = i_2 \circ \varphi ,$$

dove i_1, i_2 denotano le immersioni naturali di L_1 in $V(L_1)$ e di L_2 in $V(L_2)$, rispettivamente.

DIMOSTRAZIONE E' ovvio che gli elementi puri di $V(L_1)$ e $V(L_2)$ sono tutti e soli gli elementi di aumentazione 1 . E' quindi sufficiente provare che φ' muta elementi puri in elementi puri. Ma, se $x \in V(L_1)$, ed x è puro, si ha

$$x \cdot x = x$$

che implica

$$\varphi'(x)\ \varphi'(x) = \varphi'(x)$$

da cui:

$$\varepsilon(\varphi(x))^2 = \varepsilon(\varphi(x))$$

quindi

$$\varepsilon(\varphi(x)) = 1 \quad . \blacksquare$$

Sia L un reticolo distributivo finito; consideriamo il gruppo abeliano libero su L . Tale gruppo si può dotare di una struttura di $\mathbb{Z}$-algebra mediante l'operazione di prodotto indotta dall'inf $\wedge$ del reticolo. Questa algebra si dice algebra di semigruppo di L , e si indica con $\mathbb{Z}[L,\wedge]$. Sia I(L) l'ideale di $\mathbb{Z}[L,\wedge]$ generato dagli elementi del tipo

$$a \vee b + a \wedge b - a - b$$

con $a,b \in L$. L'anello quoziente

$$W(L) = \mathbb{Z}[L,\wedge] / I(L)$$

si dirà anello di valutazione di L . Gli elementi di W(L) immagine degli elementi di L si diranno elementi puri.

4.4. PROPOSIZIONE Sia L un reticolo distributivo finito, e sia M un gruppo abeliano. Per ogni valutazione

$$f : L \rightarrow M$$

esiste un morfismo di gruppi

$$\varphi : W(L) \rightarrow M$$

tale che

$$f = \varphi \circ i$$

dove i è l'immersione canonica di L in $W(L)$.

DIMOSTRAZIONE Analoga a quella della Proposizione 4.1.■

Analogamente a quanto fatto per il cono di valutazione $V(L)$, definiamo l'<u>aumentazione</u>

$$\varepsilon : W(L) \to \mathbb{Z}$$

nel modo seguente:

i) $\varepsilon(x) = 1$ se x è puro;

ii) $\varepsilon(\sum_i x_i) = \sum_i \varepsilon(x_i)$ se x_i è puro per ogni i.

Dal momento che $W(L)$ è un anello con aumentazione, si può definire in esso la moltiplicazione di Geissinger $*$:

$$a * b = a\,\varepsilon(b) + \varepsilon(a)b - ab$$

per ogni $a,b \in W(L)$. Ovviamente, se a,b sono puri, risulta

$$a * b = a \vee b$$

e, se $a = \sum_i x_i$, $b = \sum_j y_j$, dove x_i, y_j sono puri, si ha:

$$a * b = \sum_{i,j} (x_i \vee y_j) \quad .$$

4.5. PROPOSIZIONE L'immersione canonica

$$j : V(L) \to W(L)$$

è un morfismo di coni di valutazione.■

Osserviamo che la costruzione di $W(L)$ può essere ripetuta utilizzando l'operazione sup di L in luogo dell'operazione inf; si ottiene così un anello $W^*(L)$, che gode evidentemente delle stesse proprietà di $W(L)$. Più precisamente:

4.6. PROPOSIZIONE L'applicazasione

$$\tau : W(L) \longrightarrow W^*(L)$$

tale che

$$\tau(x) = u + z - x$$

è un isomorfismo involutorio di anelli.

DIMOSTRAZIONE E' sufficiente osservare che

$$\tau(x \wedge y) = z + u - (x \wedge y) = z + u + x \vee y - x - y =$$
$$= (z + u - x) \vee (z + u - y) = \tau(x) \vee \tau(y) \quad .$$

4.7. PROPOSIZIONE Gli elementi di $W(L)$ che corrispondono agli elementi sup-irriducibili di L costituiscono una base per $W(L)$.

DIMOSTRAZIONE

i) gli elementi sup-irriducibili di L sono ovviamente linearmente indipendenti in $W(L)$;

ii) sia $x \in L$, non sup-irriducibile, e sia

$$x = p_1 \vee p_2 \vee \dots \vee p_n$$

con $p_1, \dots, p_n$ sup-irriducibili e non confrontabili; grazie al principio di inclusione-esclusione, in $W(L)$, si ha:

$$x = p_1 + p_2 + \ldots + p_n - p_1 \wedge p_2 - p_1 \wedge p_3 - \ldots + p_1 \wedge p_2 \wedge p_3 + \ldots \quad ;$$

ciascuno degli addendi al secondo membro è strettamente minore di x ; ripetendo il procedimento per ogni addendo che non sia sup-irriducibile, dato che il reticolo L è finito, otteniamo

$$x = q_1 + q_2 + \ldots + q_k$$

con $q_1, \ldots, q_k$ sup-irriducibili;

iii) dato che gli elementi puri generano $W(L)$, l'affermazione è vera.■

4.8. PROPOSIZIONE Sia L un reticolo distributivo finito. Ogni valutazione su L è determinata dai suoi valori su $J(L)$, e questi valori possono essere assegnati arbitrariamente.

DIMOSTRAZIONE Segue dal fatto che $J(L)$ è una base per $W(L)$, e che ogni valutazione $f : L \to A$ si può esprimere nella forma $\varphi \circ i$, dove $\varphi : W(L) \to A$ è un morfismo di gruppi.

4.9. COROLLARIO Se $J(L)$ è un inf-semireticolo, allora $J(L)$ è un inf-sottosemireticolo di L, e $W(L)$ è l'algebra di semigruppo di $(J(L), \wedge)$.

DIMOSTRAZIONE Indichiamo con $\wedge$ l'operazione di inf in L, con $\underset{J}{\wedge}$ l'operazione di inf in $J(L)$. Siano $p, q \in J(L)$; supponiamo che

$$p \underset{J}{\wedge} q < p \wedge q = t \quad .$$

D'altra parte si avrà

$$t = a_1 \vee a_2 \vee \dots \vee a_n$$

con $a_1, a_2, \dots, a_n \in J(L)$; questo implica

$$p \underset{J}{\wedge} q < a_i$$

per qualche i , il che è assurdo. Di conseguenza

$$p \underset{J}{\wedge} q = p \wedge q \quad .$$

La seconda affermazione segue dal fatto che gli elementi di $J(L)$ costituiscono una base per $W(L)$.■

4.10. TEOREMA Sia L un reticolo distributivo finito; L si può immergere in un'algebra di Boole finita, $B(L)$, di rango $|\hat{J}(L)|$.

DIMOSTRAZIONE E' sufficiente osservare che, per il Teorema 2.5, L è isomorfo a un sottoreticolo dell'algebra di Boole generata dagli elementi di $\hat{J}(L)$.■

4.11. PROPOSIZIONE Sia L un reticolo distributivo finito, e $B(L)$ l'algebra di Boole generata da $\hat{J}(L)$; allora $W(L)$ e $W(B(L))$ sono isomorfi.

DIMOSTRAZIONE Segue dal fatto che

$$|J(L)| = |J(B(L))|$$

e quindi i due anelli di valutazione sono generati dallo stesso numero di elementi.■

5. La funzione di Möbius

Sia L un reticolo distributivo finito, e sia $J(L)$ l'insieme parzialmente ordinato degli elementi sup-irriducibili di L. Per ogni $p \in \hat{J}(L)$, l'insieme

$$\{x \in L;\ x < p\}$$

ha un massimo, che indicheremo con ∂p. Osserviamo inoltre che, se $p_1, p_2, \dots, p_n$ sono gli elementi sup-irriducibili di L tali che $p_i < p$ per ogni i, allora

$$\partial p = p_1 \vee p_2 \vee \dots \vee p_n \ .$$

Nell'anello di valutazione $W(L)$, definiamo

$$e_p = p - \partial p \ .$$

Poniamo inoltre

$$e_z = z \ .$$

5.1. PROPOSIZIONE L'insieme

$$\{e_p;\ p \in J(L)\}$$

è una base di idempotenti ortogonali per $W(L)$. Inoltre, per ogni $x \in L$, risulta

$$x = \sum_{p \leq x} e_p \ .$$

DIMOSTRAZIONE Innanzi tutto osserviamo che, per ogni $p \in J(L)$, si ha:

$$e_p \cdot e_p = (p - \partial p)^2 = p \wedge p + \partial p \wedge \partial p - 2\, p \wedge \partial p = p - \partial p = e_p \quad ,$$

e, per ogni $p, q \in J(L)$, $p \neq q$, risulta

$$p \wedge q = \partial p \wedge \partial q \quad ,$$

da cui

$$e_p \cdot e_q = (p - \partial p)(q - \partial q) = p \wedge q + \partial p \wedge \partial q - \partial p \wedge q - p \wedge \partial q = 0 \quad .$$

Inoltre, per ogni $x \in L$, risulta

$$x = \sum_{p \leq x} e_p \quad ;$$

infatti, supponiamo vera l'affermazione per ogni $y \in L$, $y < x$; se x non è sup-irriducibile, avremo $x = a \vee b$; se

$$a = \sum_{p \leq a} e_p \quad , \qquad b = \sum_{q \leq b} e_q \quad ;$$

allora

$$a \wedge b = (\sum_{p \leq a} e_p)(\sum_{q \leq b} e_q) = \sum_{p \leq a \wedge b} e_p$$

poiché gli e_p sono idempotenti ortogonali; quindi

$$x = a + b - a \wedge b = \sum_{p \leq x} e_p \quad .$$

Se invece x è sup-irriducibile, si ha:

$$x = e_x + \partial x \quad ,$$

dal momento che $\partial x < x$, la tesi è vera.$\blacksquare$

Dato che gli elementi di $J(L)$ sono una base per $W(L)$, sarà in particolare

$$e_p = \sum_{\substack{q \leq p \\ q \in J(L)}} \mu(q,p)\, q$$

per ogni $p \in J(L)$. I coefficienti $\mu(q,p)$ sono evidentemente numeri interi. Per convenzione, poniamo

$$\mu(q,p) = 0 \qquad\qquad \text{se} \quad q \not\leq p \ .$$

Abbiamo quindi:

5.2. PROPOSIZIONE Per ogni $x \in L$ si ha

$$x = \sum_{\substack{p,q \in J(L) \\ q \leq x}} \mu(p,q)\, p \quad .$$

DIMOSTRAZIONE Segue dalla Proposizione precedente e dalla definizione di $\mu(p,q)$.$\blacksquare$

5.3. PROPOSIZIONE Per ogni $a,b \in J(L)$ si ha:

$$\sum_{a \leq x \leq b} \mu(x,b) = \begin{cases} 0 & \text{se} \quad a \neq b \\ 1 & \text{se} \quad a = b \ . \end{cases}$$

DIMOSTRAZIONE Senza perdita di generalità, supponiamo che a sia il minimo del reticolo L. Abbiamo quindi:

$$e_b \cdot a = \sum_{a \leq b} \mu(x,b)(x \wedge a) = a \cdot \sum_{x \leq b} \mu(x,b) \quad .$$

Ma $e_b \cdot a = \varepsilon(e_b) \cdot a = 0$ se $b \neq a$, mentre $e_a \cdot a = a$; da qui segue l'affermazione.■

5.4. PROPOSIZIONE Per ogni $a, b \in J(L)$ si ha:

$$\sum_{a \leq x \leq b} \mu(a,x) = \begin{cases} 0 & \text{se } a \neq b \\ 1 & \text{se } a = b \end{cases} \quad .$$

DIMOSTRAZIONE Per ogni $p \in J(L)$ si ha

$$e_p = \sum_{x \leq p} \mu(x,p) x \quad ;$$

sia $q \in J(L)$. Allora

$$q = \sum_{p \leq q} e_p = \sum_{p \leq q} \sum_{x \leq p} \mu(x,p) x =$$

$$= \sum_{x \leq q} \left[\sum_{x \leq p \leq q} \mu(x,p) \right] x \quad ;$$

la tesi segue dal fatto che x e q sono linearmente indipendenti per ogni $x \in J(L)$, $x \neq q$.■

Sia P un insieme parzialmente ordinato finito; in base alle considerazioni precedenti resta definita una funzione

$$\mu : P \times P \longrightarrow \mathbb{Z}$$

che diremo <u>funzione di Möbius</u> di P. Osserviamo che la funzione di Möbius è l'unica funzione soddisfacente le seguenti condizioni:

M 1) $\mu(x,y) = 0$ se $x \not\leq y$;

M 2) $\mu(x,x) = 1$ per ogni $x \in P$;

M 3) $\sum_{x \leq z \leq y} \mu(x,z) = 0$ per ogni $x,y \in P$, $x \neq y$.

Se P è un insieme parzialmente ordinato finito e P^* è il suo duale d'ordine, indichiamo con μ^* la funzione di Möbius di .P^* .

5.5. PROPOSIZIONE Per ogni $x;y \in P$, si ha:

$$\mu^*(x,y) = \mu(y,x) \quad .$$

DIMOSTRAZIONE Definiamo una funzione

$$\nu : P^* \times P^* \rightarrow \mathbb{Z}$$

ponendo

$$\nu(x,y) = \mu(y,x) \quad .$$

Abbiamo allora che ν verifica le condizioni M1), M2), M3), e quindi è la funzione di Möbius di P^* .■

Ricordiamo che, in un reticolo distributivo finito L, si definisce rango la funzione che ad ogni $x \in L$ associa la lunghezza di una catena massimale tra il minimo di L ed x. Osserviamo che, dato che ogni reticolo distributivo è modulare, la funzione rango è una valutazione su L.

5.6. PROPOSIZIONE Sia L un reticolo distributivo finito, ed r la sua funzione rango. Allora, per ogni $x \in L$, si ha:

$$r(x) = \left| \left\{ p \in \hat{J}(L);\ p \leq x \right\} \right| \quad .$$

DIMOSTRAZIONE Consideriamo l'applicazione

$$f : L \longrightarrow \mathbf{Z}$$

$$f(x) = \left| \left\{ p \in \hat{J}(L);\ p \leq x \right\} \right|$$

e proviamo che è una valutazione. Infatti, se $a, b \in L$ e $p \in \hat{J}(L)$ è tale che $p \leq a \vee b$, allora $p \leq a$ oppure $p \leq b$, da cui

$$f(a \vee b) + f(a \wedge b) = f(a) + f(b) \quad .$$

A questo punto è sufficiente dimostrare che f ed r assumono gli stessi valori su $J(L)$. L'affermazione è vera per gli elementi di rango zero ed uno; per ipotesi di induzione, supponiamo l'affermazione vera per gli elementi di $J(L)$ di rango $\leq h$. Sia $a \in J(L)$, $r(a) = h+1$, e sia $b < a$, tale che $r(b) = h$. Allora

$$\left\{ x \in \hat{J}(L);\ x \leq a \right\} = \left\{ a \right\} \cup \left\{ x \in \hat{J}(L);\ x \leq b \right\}$$

quindi la tesi segue per induzione.∎

La valutazione χ definita sul reticolo distributivo finito L come segue:

$$\chi(p) = 1 \qquad \text{se } p \in \hat{J}(L)$$
$$\chi(z) = 0$$

dove z è il minimo di L, si dice valutazione caratteristica di L.

Osserviamo esplicitamente che, se $\hat{J}(L)$ è un complesso simpliciale, in base alle considerazioni precedenti si ha che $\chi(u)$ (dove u è il massimo di L) è la caratteristica di Eulero del complesso simpliciale $\hat{J}(L)$.

5.7. PROPOSIZIONE Per ogni $y \in L$, si ha:

$$\chi(y) = - \sum_{\substack{q \in \hat{J}(L) \\ q \leq y}} \mu(z,q) \quad .$$

Inoltre, se $p \in \hat{J}(L)$, risulta

$$\chi(\partial p) = 1 + \mu(z,p) \quad .$$

DIMOSTRAZIONE Applicando χ ad ambo i membri dell'uguaglianza

$$y = \sum_{\substack{p,q \in J(L) \\ q \leq y}} \mu(p,q)\, p$$

si ha

$$\chi(y) = \sum_{\substack{p,q \in \hat{J}(L) \\ q \leq y}} \mu(p,q) = - \sum_{q \in \hat{J}(L)} \mu(z,q) \quad .$$

Se poi $y = \partial p$:

$$\chi(\partial p) = - \sum_{\substack{q \in \hat{J}(L) \\ q < p}} \mu(z,q) = \mu(z,z) + \mu(z,p) \quad . \blacksquare$$

5.8. TEOREMA (Identità di Klee) Sia S un inf-semireticolo, e siano $x, a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m$ elementi di S tali che $x \geq a_i, b_j$ per ogni i,j . Allora, nell'algebra di semigruppo $\mathbb{Z}[S,\wedge]$, si ha:

$$\prod_i (x-a_i) + \prod_j (x-b_j) - (x - \bigvee_{i,j} (a_i \wedge b_j)) =$$

$$= \prod_i (x-a_i) \prod_j (x-b_j) \quad .$$

DIMOSTRAZIONE Senza perdita di generalità, possiamo supporre S finito. Per il Corollario 4.9 abbiamo che, identificando un elemento di S con l'ideale (principale) da esso generato, si ottiene un isomorfismo tra $\mathbb{Z}[S,\wedge]$ e $W(\hat{\mathscr{I}}(S))$. In quest'ultima algebra, l'affermazione del teorema si scrive come

$$(x - \bigvee_i a_i) + (x - \bigvee_j b_j) - (x - \bigvee_{i,j} (a_i \wedge b_j)) =$$

$$= x - (\bigvee_i a_i) \vee (\bigvee_j b_j)$$

dove $\vee$ indica l'operazione di sup in $\hat{\mathscr{I}}(S)$. Quest'ultima identità è vera, in quanto, in $\hat{\mathscr{I}}(S)$:

$$\bigvee_{i,j} (a_i \wedge b_j) = (\bigvee_i a_i) \wedge (\bigvee_j b_j) \quad . \blacksquare$$

5.9. PROPOSIZIONE Sia L un reticolo distributivo finito tale che $J(L)$ risulti a sua volta un reticolo; per ogni $p_1, p_2, \ldots, p_r \in \hat{J}(L)$, sia y il sup in L di $p_1, p_2, \ldots, p_r$. Allora

$$\chi(y) = 1 + c_2 - c_3 + c_4 - \ldots$$

dove c_k è il numero di sottoinsiemi con k elementi di $\{p_1, p_2, \ldots, p_r\}$ aventi per inf il minimo z di L.

DIMOSTRAZIONE Si ha:

$$(\chi - 1)(y) = (\chi - 1)(\bigvee_i p_i) =$$

$$= \sum_i (\chi-1)p_i - \sum_{i,j} (\chi-1)(p_i \wedge p_j) + \ldots$$

Dato che $(\chi - 1)(p) = 0$ se $p \in \hat{J}(L)$ e $(\chi - 1)(z) = -1$, si ha la tesi.■

5.10. COROLLARIO Sia P un reticolo finito e siano $q, p_1, p_2, \ldots, p_r \in \hat{P}$ tali che $p_i \leq q$ per ogni i e, per ogni $x \leq q$, x massimale rispetto a questa proprietà, esiste i tale che $x = p_i$; allora

$$\mu(\hat{0}, q) = c_2 - c_3 + \ldots$$

dove $\hat{0}$ è il minimo di P, e c_k è il numero di sottoinsiemi con k elementi di $\{p_1, p_2, \ldots, p_r\}$ aventi inf in $\hat{0}$.

DIMOSTRAZIONE Nel reticolo distributivo $\hat{\mathcal{J}}(P)$ si ha $\partial q = \bigvee_i p_i$;

allora, per la Proposizione 5.7, si ha:

$$\chi(\partial q) - 1 = \mu(\hat{0},q) \quad .$$

Sfruttando il risultato precedente si ha la tesi.■

Sia L un reticolo finito; indichiamo con $\hat{0}$ ed $\hat{1}$ rispettivamente il minimo e il massimo di L. Un insieme $T = \{a_1, a_2, \ldots, a_n\}$ di elementi di L si dice taglio (cross-cut) se sono soddisfatte le seguenti condizioni:

i) $\hat{0}$ ed $\hat{1}$ non appartengono a T;

ii) T è un'anticatena;

iii) ogni catena massimale tra $\hat{0}$ ed $\hat{1}$ ha intersezione non vuota con T.

Il Corollario 5.10 può essere generalizzato come segue:

5.11. TEOREMA (del Cross-cut) Sia L un reticolo finito, e sia T un taglio di L. Per ogni intero $k \geq 2$ sia q_k il numero dei sottoinsiemi S di T aventi k elementi e tali che

$$\bigwedge_{s \in S} s = \hat{0} \ , \qquad \bigvee_{s \in S} s = \hat{1} \quad .$$

Allora

$$\mu(\hat{0}, \hat{1}) = q_2 - q_3 + q_4 - \ldots$$

DIMOSTRAZIONE Definiamo la distanza d(x) di $x \in L$ dall'elemento $\hat{1}$ come la massima cardinalità di una catena di L avente per estremi x ed $\hat{1}$. Se T è un taglio di L, definiamo la sua distanza da $\hat{1}$ ponendo:

$$d(T) = \max_{x \in T} d(x) \quad .$$

Procederemo per induzione su $d(T)$. Per il Corollario precedente, la tesi è vera per $d(T) = 2$.

Sia ora B un sottoinsieme di L; per ogni $x \in L$, scriveremo $x \leq B$ $(x > B)$ se esiste $y \in B$ tale che $y \geq x$ $(y < x)$. Notiamo che, se B è un taglio, per ogni $x \in L$ risulta $x \leq B$ oppure $x > B$.

Sia L' il reticolo i cui elementi sono tutti e soli gli elementi $x \in L$ tali che $x \leq T$ (con T un taglio tale che $d(T) > 2$), uniti all'elemento $\hat{1}$, con l'ordine indotto da L. In L', il taglio T ha distanza 2, per cui, denotando con μ' la funzione di Möbius di L', il Corollario precedente implica

$$\mu'(\hat{0}, \hat{1}) = P_2 - P_3 + P_4 - \dots$$

dove P_k indica il numero di sottoinsiemi A di T con k elementi e tali che, in L',

$$\bigwedge_{a \in A} a = \hat{0} \quad .$$

D'altra parte, avremo:

$$\sum_{x \leq T} \mu(\hat{0},x) + \sum_{x > T} \mu(\hat{0},x) = 0 =$$

$$= \sum_{x \leq T} \mu'(\hat{0},x) + \mu'(\hat{0},\hat{1}) \quad .$$

Poiché $\mu(\hat{0},x) = \mu'(\hat{0},x)$ per ogni $x \leq T$, si ha:

$$\sum_{x\leq T} \mu(\hat{0},x) = -\mu'(\hat{0},\hat{1}) = -p_2+p_3-p_4+\dots$$

Ora, dato che gli insiemi $\{x\in L;\ x\leq T\}$ e $\{x\in L;\ x>T\}$ sono disgiunti, si può scrivere:

$$(*)\qquad \mu(\hat{0},\hat{1}) = -\sum_{x<\hat{1}} \mu(\hat{0},x) =$$

$$= -(\sum_{x\leq T} \mu(\hat{0},x) + \sum_{T<x<\hat{1}} \mu(\hat{0},x)) =$$

$$= p_2-p_3+p_4-\dots-\sum_{T<x<\hat{1}} \mu(\hat{0},x) \quad .$$

Sia ora $q_k(x)$ il numero dei sottoinsiemi A di T aventi k elementi e tali che

$$\bigvee_{a\in A} a = x\ ,\qquad \bigwedge_{a\in A} a = \hat{0}\ .$$

In particolare, $q_k(\hat{1}) = q_k$. Ne segue che

$$p_k = \sum_{x>T} q_k(x) \qquad\qquad (k\geq 2)\ ;$$

perciò, l'identità $(*)$ è equivalente all'identità:

$$(**)\qquad \mu(\hat{0},\hat{1}) = q_2-q_3+\dots-$$

$$-\sum_{T<x<\hat{1}} (-q_2(x)+q_3(x)-\dots+\mu(\hat{0},x))\ .$$

Sia ora x tale che $T < x < \hat{1}$; consideriamo l'intervallo $[\hat{0},x]$ in L. Sia $T(x) = T \cap [\hat{0},x]$; dal momento che $T(x)$ è un taglio dell'intervallo $[\hat{0},x]$, e che la sua distanza in questo intervallo è strettamente minore di $d(T)$, per l'ipotesi di induzione si ha:

$$\mu(\hat{0},x) = q_2(x) - q_3(x) + q_4(x) - \dots$$

Sostituendo nella (**), si ha l'identità voluta.■

5.12. COROLLARIO Se L è un reticolo finito tale che il suo massimo $\hat{1}$ risulti sup-irriducibile, allora

$$\mu(\hat{0},\hat{1}) = 0 \quad .■$$

5.13. COROLLARIO Sia L un reticolo finito; allora:

(a) se L ha un taglio di cardinalità uno, allora $\mu(\hat{0},\hat{1}) = 0$;

(b) se L ha un taglio di cardinalità due, allora $\mu(\hat{0},\hat{1}) = 0$ oppure $\mu(\hat{0},\hat{1}) = 1$;

(c) se L ha un taglio di cardinalità tre, allora $\mu(\hat{0},\hat{1})$ può assumere solo i valori $-1, 0, 1, 2$.■

5.14. PROPOSIZIONE Sia P un insieme parzialmente ordinato finito. Per ogni $a, b \in P$, con $a < b$, si ha

$$\mu(a,b) = -c_2(a,b) + c_3(a,b) - \dots$$

dove $c_k(a,b)$ indica il numero di catene con k elementi tra a e b .

DIMOSTRAZIONE Procediamo per induzione sul numero di elementi dell'intervallo $[a,b]$. Se l'intervallo è costituito solo dai punti a e b, risulta $\mu(a,b) = -1$, e quindi l'affermazione è vera. In generale, si ha:

$$\mu(a,b) = -\mu(b,b) - \sum_{a<x<b} \mu(x,b)$$

e quindi, per l'ipotesi di induzione:

$$\mu(a,b) = -1 - \sum_{a<x<b} (-c_2(x,b) + c_3(x,b) - \dots) =$$

$$= -1 + c_3(a,b) - c_4(a,b) + \dots$$

in quanto, per ogni $k \geq 3$:

$$c_k(a,b) = \sum_{a<x<b} c_{k-1}(x,b) \qquad . \blacksquare$$

5.15. TEOREMA Siano P,Q insiemi parzialmente ordinati, e sia

$$f : P \longrightarrow Q$$

un morfismo d'ordine. Siano $a,b \in P$ tali che $a < b$ e $f(a) < f(b)$. Allora, indicando con μ la funzione di Möbius di P, si ha:

$$\mu(a,b) = \sum_{\substack{x \in P \\ f(x)=f(b)}} \mu_f(a,x)\,\mu(x,b)$$

dove, per ogni $p,q \in P$, si pone

$$\mu_f(p,q) = - \sum_{\substack{x \leq q \\ f(x) < f(q)}} \mu(p,x) \quad .$$

DIMOSTRAZIONE Per la Proposizione 5.14

$$\mu(a,b) = -c_2(a,b) + c_3(a,b) - \dots$$

dove $c_k(a,b)$ indica il numero di catene con k elementi tra a e b. Sia λ una variabile formale; poniamo

$$C(a,b;\lambda) = \sum_{k \geq 2} c_k(a,b)\lambda^{k-1} \quad ;$$

analogamente, definiamo $c_k^f(a,b)$ come il numero delle catene

$$a = t_1 < t_2 < \dots < t_k = b$$

tali che

$$f(t_i) < f(b)$$

per $i = 1, 2, \dots, k-1$. Poniamo

$$C^f(a,b;\lambda) = \sum_{k \geq 2} c_k^f(a,b)\lambda^{k-1} \quad .$$

Osserviamo che, per ogni catena tra a e b:

$$a = t_1 < t_2 < \dots < t_k = b$$

esiste $j \leq k$ tale che

$$f(t_j) = f(b)\ , \qquad f(t_{j-1}) < f(b) \qquad ;$$

ne segue che, se $a < b$ e $f(a) < f(b)$:

$$C(a,b;\lambda) = \sum_{\substack{x \in P \\ f(x)=f(b)}} C^f(a,x;\lambda)\ C(x,b;\lambda) \quad .$$

Ponendo $\lambda = -1$ si ha la tesi. ■

Ricordiamo che, se P è un insieme parzialmente ordinato finito, si dice <u>funzione zeta</u> di P la funzione

$$\zeta : P \times P \longrightarrow \mathbb{Z}$$

definita nel modo seguente:

$$\zeta(x,y) = \begin{cases} 1 & \text{se } x \leq y \\ 0 & \text{altrimenti} \end{cases} \quad .$$

5.16. COROLLARIO Siano P,Q due insiemi parzialmente ordinati finiti, e sia

$$f : P \rightarrow Q$$

un morfismo d'ordine. Siano μ e ζ la funzione di Möbius e la funzione zeta di P , rispettivamente. Per ogni $a,b \in P$ con $a < b$ e $f(a) < f(b)$, risulta:

$$\mu(a,b) = \sum_{\substack{x,y \in P \\ f(y)=f(x)=f(b)}} \mu(a,y)\ \zeta(y,x)\ \mu(x,b) \quad .$$

DIMOSTRAZIONE Segue dal teorema precedente, osservando che:

$$0 = \sum_{x \leq b} \mu(a,x) = \sum_{\substack{x \leq b \\ f(x)<f(b)}} \mu(a,x) + \sum_{\substack{x \leq b \\ f(x)=f(b)}} \mu(a,x) =$$

$$= - \mu_f(a,b) + \sum_{\substack{x \leq b \\ f(x)=f(b)}} \mu(a,x) \quad . \blacksquare$$

5.17. TEOREMA (di complementazione) Sia P un reticolo finito, con minimo $\hat{0}$ e massimo $\hat{1}$. Se $s \in P$, indichiamo con $s^{\perp}$ l'insieme dei complementi di s in P. Allora

$$\mu(\hat{0},\hat{1}) = \sum_{x,y \in s^{\perp}} \mu(\hat{0},x)\, \zeta(x,y)\, \mu(y,\hat{1}) \quad .$$

DIMOSTRAZIONE Sia

$$f : P \longrightarrow [s,\hat{1}]$$

$$f(x) = x \vee s \quad ;$$

f è un morfismo d'ordine; per il Teorema 5.15 si ha:

$$\mu(\hat{0},\hat{1}) = \sum_{\substack{x \in P \\ x \vee s=\hat{1}}} \mu_f(\hat{0},x)\, \mu(x,\hat{1}) \quad .$$

Sia $y \in P$ tale che $y \vee s = \hat{1}$. Consideriamo l'insieme

$$S = \{x \in P;\ x \vee s < \hat{1},\ x \leq y\} \cup \{y\} \quad .$$

L'insieme S, con l'ordine indotto da P, risulta ovviamente un reticolo. Per ogni $t \in S$ si ha $t \vee (s \wedge y) \in S$; di conseguenza, l'elemento $s \wedge y$ è un estremo inferiore per gli elementi massimali di $S \setminus \{y\}$. Questo implica che $\{s \wedge y\}$ è un taglio di S purché $s \wedge y \neq \hat{0}$. In questo caso, per il Teorema del Cross-cut, $\mu_f(\hat{0},y) = 0$. Da qui, sfruttando il Corollario precedente, si ottiene la tesi.■

5.18. COROLLARIO Se P è un reticolo finito non complementato, allora:

$$\mu(\hat{0},\hat{1}) = 0 \quad .■$$

6. L'algebra di Möbius

Sia P un insieme parzialmente ordinato finito. Si definisce algebra di Möbius $M(P)$ di P lo $\mathbb{Z}$-modulo libero su P dotato dell'operazione di prodotto definita nel modo seguente:

$$qr = \sum_{\substack{s,t \in P \\ s \leq t \leq q,r}} \mu(s,t)\, s \quad ,$$

per ogni $q,r \in P$.

Osserviamo esplicitamente che, se P è un inf-semireticolo:

$$M(P) \cong \mathbb{Z}[P, \wedge] \quad ,$$

cioè, l'algebra di Möbius di P coincide con l'algebra di semigruppo su P rispetto all'operazione di inf.

Come abbiamo visto, P è isomorfo all'insieme parzialmente ordinato $\hat{J}(\mathcal{J}(P))$. Se P è dotato di minimo $\hat{0}$, allora anche $\hat{\mathcal{J}}(P) = \mathcal{J}(P)\setminus\{\phi\}$ è un reticolo distributivo, il cui minimo è l'ideale costituito dal solo elemento $\hat{0}$. In questo caso

$$\hat{J}(\mathcal{J}(P)) = J(\hat{\mathcal{J}}(P))$$

e quindi P è isomorfo a $J(\hat{\mathcal{J}}(P))$. Ne segue che, dato che gli elementi di $J(\hat{\mathcal{J}}(P))$ sono una base per l'anello di valutazione di $\hat{\mathcal{J}}(P)$, sussiste l'isomorfismo di moduli

$$(*) \qquad M(P) \cong W(\hat{\mathcal{J}}(P)) \quad .$$

Se invece P non ha minimo, osserviamo che il minimo z di $\mathcal{J}(P)$, cioè l'insieme vuoto, è sup-irriducibile in $\mathcal{J}(P)$, e quindi appartiene ad una base di $W(\mathcal{J}(P))$; z genera perciò un sottomodulo $<z>$ di $W(\mathcal{J}(P))$ avente rango 1, e sussiste l'isomorfismo di moduli:

$$(**) \qquad M(P) \cong W(\mathcal{J}(P))/<z> \quad .$$

Gli isomorfismi (*) e (**) risultano inoltre isomorfismi di algebre. Infatti, in $W(\mathcal{J}(P))$, si ha:

$$p\cdot q = (\sum_{s\leq p} e_s)(\sum_{t\leq q} e_t) =$$

$$= \sum_{r\leq p,q} e_r = \sum_{x\leq r\leq p,q} \mu(x,r)x \quad ;$$

perciò, l'operazione di prodotto in $W(\mathscr{I}(P))$ coincide con il prodotto in $M(P)$.

Si ha di conseguenza:

6.1. PROPOSIZIONE Sia P un insieme parzialmente ordinato finito, e sia $M(P)$ la sua algebra di Möbius. Per ogni $p \in P$, poniamo

$$e_p = \sum_{r \leq p} \mu(r,p)\, r \quad .$$

Allora, l'insieme $\{e_p ; p \in P\}$ è una base di idempotenti ortogonali per $M(P)$. ■

6.2. PROPOSIZIONE Siano P,Q insiemi parzialmente ordinati finiti. Ogni morfismo d'ordine

$$\alpha : P \longrightarrow Q$$

induce i morfismi di algebre

$$\alpha' : W(\mathscr{I}(Q)) \longrightarrow W(\mathscr{I}(P))$$

e

$$\alpha'' : M(Q) \longrightarrow M(P)$$

definiti nel modo seguente:

$$\alpha'(e_q) = \sum_{\substack{p \in P \\ \alpha(p)=q}} e_p \,, \qquad q \in \hat{J}(\mathscr{I}(Q)), \qquad \alpha'(e_\phi) = e_\phi \quad ,$$

e:

$$\alpha''(e_q) = \sum_{\substack{p\in P\\ \alpha(p)=q}} e_p \ , \qquad q\in Q \ .$$

DIMOSTRAZIONE Ovvia.■

6.3. PROPOSIZIONE (Lemma di Weisner) Sia P un reticolo finito, e siano $a,b,c\in P$. Allora

$$\sum_{\substack{x\in P\\ x\wedge a=c}} \mu(x,b) = \begin{cases} 0 & \text{se } a \ngeq b \\ \mu(c,b) & \text{se } a \geq b \end{cases} \ .$$

DIMOSTRAZIONE Nell'algebra di Möbius $M(P)$ abbiamo

$$a = \sum_{y\leq a} e_y \ .$$

Quindi

$$a\, e_b = \sum_{y\leq a} (e_y \wedge e_b) = \begin{cases} 0 & \text{se } a \ngeq b \\ e_b & \text{se } a \geq b \end{cases} \ .$$

Ricordando poi che

$$e_b = \sum_{t\leq b} \mu(t,b)t$$

abbiamo

$$a\, e_b = \sum_{t\leq b} \mu(t,b)\, t\wedge a \quad =$$

$$= \sum_{\substack{t\leq b\\ t\wedge a=c}} \mu(t,b)\, c + \sum_{\substack{t\leq b\\ t\wedge a\neq c}} \mu(t,b)\, t\wedge a \qquad ;$$

da qui si ha la tesi.■

6.4. TEOREMA Sia P un insieme parzialmente ordinato finito dotato di minimo $\hat{0}$ e di massimo $\hat{1}$, e sia $t \in P$ tale che per ogni $p \in P$ esista $p \vee t$ in P. Allora, nell'algebra di Möbius di P, sussiste l'identità:

$$\sum_{r \in P} \mu(r,\hat{1})r = \Big(\sum_{r \geq t} \mu(r,\hat{1})r\Big)\Big(\sum_{r \vee t = \hat{1}} \mu(r,\hat{1})r\Big) \quad .$$

DIMOSTRAZIONE Per $t = \hat{1}$ l'affermazione è vera. Sia allora $t \neq \hat{1}$. Indichiamo con K l'insieme degli elementi di P che sono coperti da $\hat{1}$, e sia

$$C = \{k \in K;\ k \geq t\} \quad .$$

Sia $L = \hat{\mathcal{J}}(P)$; l'algebra di Möbius $M(P)$ si può identificare con $W(L)$, in quanto P è dotato di minimo. In $W(L)$ avremo perciò

$$e_{\hat{1}} = \hat{1} - \partial\hat{1} = \hat{1} - \bigvee_{k \in K} k = \prod_{k \in K} (\hat{1} - k)$$

e, d'altra parte

$$e_{\hat{1}} = \sum_{r \in P} \mu(r,\hat{1})\, r \quad .$$

Inoltre si ha:

$$\prod_{c \in C} (\hat{1} - c)e_{\hat{1}} = \prod_{c \in C} (\hat{1} - c) \prod_{k \in K} (\hat{1} - k) \quad =$$

$$= \prod_{k\in K} (\hat{1} - k) = e_{\hat{1}} \quad .$$

Per ogni $c \in C$ e per ogni $r \in P$, $r \leq c$, si ha:

$$(\hat{1} - c)\, r = \hat{1} \wedge r - c \wedge r = 0 \quad .$$

Allora

$$(\hat{1} - c) e_{\hat{1}} = (\hat{1} - c) \sum_{r \nleq c} \mu(r,\hat{1}) r$$

e perciò, posto $d = \bigvee_{c\in C} c$ (in $\hat{\mathscr{I}}(P)$):

$$e_{\hat{1}} = \prod_{c\in C} (\hat{1} - c) e_{\hat{1}} =$$

$$= \prod_{c\in C} (\hat{1} - c) (\sum_{r \nleq d} \mu(r,\hat{1}) r) \quad .$$

Ora, se $r \nleq d$ in $\hat{\mathscr{I}}(P)$, allora $r \vee t = \hat{1}$ in P, e viceversa.

Osserviamo che, nell'algebra di Möbius dell'intervallo $[t,\hat{1}]$ dell'insieme parzialmente ordinato P, sussiste l'identità:

$$\prod_{c\in C} (\hat{1} - c) = e_{\hat{1}} = \sum_{r \geq t} \mu(r,\hat{1})\, r \quad ,$$

poiché la funzione di Möbius di un qualunque intervallo di P è la restrizione di μ. Di conseguenza, otteniamo l'identità

$$\sum_{r\in P} \mu(r,\hat{1}) r = e_{\hat{1}} = \prod_{c\in C} (\hat{1} - c) (\sum_{r \vee t = \hat{1}} \mu(r,\hat{1}) r) =$$

$$= (\sum_{r \geq t} \mu(r,\hat{1}) r) (\sum_{r \vee t = \hat{1}} \mu(r,\hat{1}) r) \quad . \blacksquare$$

6.5. TEOREMA Sia P un reticolo finito, e sia P_o l'insieme dei coatomi di P. Siano $A,B \subseteq P_o$ tali che $A \cap B = \phi$ e $A \cup B = P_o$. Allora

$$\sum_{x \in L} \mu(x,\hat{1})x = \Big(\sum_{y \in H(A)} \mu_A(y,\hat{1})y\Big)\Big(\sum_{z \in H(B)} \mu_B(z,\hat{1})\, z\Big) \quad ,$$

dove $H(A)$, $H(B)$ sono gli inf-sottoreticoli di P generati da A e B, con funzioni di Möbius μ_A, μ_B rispettivamente.

DIMOSTRAZIONE Abbiamo, in $M(P)$:

$$e_{\hat{1}} = \prod_{p \in P_o} (\hat{1} - p) = \prod_{p \in A} (\hat{1} - p) \prod_{q \in B} (\hat{1} - q) \quad .$$

Da qui, grazie al Teorema precedente, segue l'uguaglianza.∎

Sia P un insieme parzialmente ordinato finito. Un <u>operatore di chiusura</u> è un'applicazione

$$\varrho : P \longrightarrow P$$

tale che:

i) ϱ è un morfismo d'ordine;

ii) per ogni $x \in P$, $\varrho(\varrho(x)) = \varrho(x)$;

iii) per ogni $x \in P$, $x \leq \varrho(x)$.

Gli elementi $x \in P$ tali che $\varrho(x) = x$ si dicono <u>chiusi</u>.

Se P,Q sono insiemi parzialmente ordinati finiti, una <u>connessione di Galois</u> tra P e Q è una coppia di funzioni

$$\varphi : P \longrightarrow Q \quad ,$$
$$\sigma : Q \longrightarrow P$$

tali che:

i) φ e σ invertono l'ordine, cioè se $x,y \in P$, $x \leq y$, allora $\varphi(x) \geq \varphi(y)$ e analogamente per σ;

ii) $\sigma\circ\varphi$ e $\varphi\circ\sigma$ sono operatori di chiusura su P e Q, rispettivamente.

6.6. TEOREMA Siano P e Q insiemi parzialmente ordinati finiti; un'applicazione

$$\varphi : P \longrightarrow Q$$

induce un morfismo

$$\phi : M(P) \longrightarrow M(Q)$$

se e solo se:

i) φ è un morfismo d'ordine;

ii) la controimmagine attraverso φ di un filtro principale in Q è un filtro principale di P, oppure l'insieme vuoto.

DIMOSTRAZIONE Supponiamo che $\varphi : P \to Q$ induca un morfismo $\phi : M(P) \to M(Q)$. Poiché $x \leq y$ in P se e solo se $xy = x$ in M(P), si ha che $x \leq y$ implica $\phi(xy) = \phi(x)$; d'altra parte, $\phi(xy) = \phi(x)\phi(y)$, quindi $\varphi(x) \leq \varphi(y)$. Di conseguenza, la i) è verificata.

Sia ora $q \in Q$, e sia

$$\{p \in P;\ \varphi(p) \geq q\} \neq \phi \qquad ;$$

allora, esiste $p \in P$ tale che $\varphi(p) \geq q$. Poiché in $M(Q)$:

$$\sum_{y \leq \varphi(p)} e_y = \varphi(p) = \phi(\sum_{x \leq p} e_x) = \sum_{x \leq p} \phi(e_x) \quad ,$$

si ha che e_q è uno dei termini che compaiono nella somma

$$\sum_{x \leq p} \phi(e_x) \quad ,$$

e quindi esiste $x \leq p$ tale che e_q compaia come addendo nell' espressione di $\phi(e_x)$; perciò questo x è tale che $\varphi(x) \geq q$. Inoltre, tale x è unico, poiché sia gli e_t , $t \in Q$, sia i $\phi(e_y)$, $y \in P$, sono idempotenti ortogonali di $M(Q)$ ed $M(P)$ rispettivamente. Di conseguenza, $x \leq p$ per ogni $p \in P$ tale che $\varphi(p) \geq q$. Allora

$$x = \min \{p \in P;\ \varphi(p) \geq q\}$$

e quindi la ii) è verificata.

Viceversa, supponiamo che

$$\varphi : P \rightarrow Q$$

soddisfi le condizioni i) e ii).

Poniamo

$$Q_o = \{q \in Q;\ q \leq \varphi(p) \text{ per qualche } p \in P\} \quad .$$

Per $q \in Q_o$, sia

$$\psi(q) = \min \{p \in P;\ \varphi(p) \geq q\} \quad .$$

Si ha allora che φ e ψ costituiscono una connessione di Galois, e che le funzioni

$$p \rightarrow \bar{p} = \psi(\varphi(p))$$

e

$$q \rightarrow \bar{q} = \varphi(\psi(q))$$

sono operatori di chiusura. Definiamo ora un omomorfismo

$$\phi : M(P) \longrightarrow M(Q)$$

ponendo

$$\phi(e_p) = \begin{cases} 0 & \text{se } \bar{p} > p \\ \sum\limits_{\substack{p\epsilon Q \\ \bar{q}=\varphi(p)}} e_q & \text{se } \bar{p} = p \end{cases}$$

ed estendendo per linearità.
E' immediato verificare che ϕ coincide con φ su P, e quindi è il morfismo voluto.■

6.7. COROLLARIO Sia P un insieme parzialmente ordinato finito, e sia P_o un sottoinsieme di P. L'algebra $M(P_o)$ è isomorfa alla sottoalgebra di $M(P)$ generata da P_o se e solo se la restrizione a P_o di ogni filtro principale di P è ancora un filtro principale, o, equivalentemente, se e solo se esiste un operatore di chiusura ϱ su P tale che P_o coincida con l'insieme parzialmente ordinato dei chiusi di P rispetto a ϱ .■

6.8. PROPOSIZIONE Sia P un insieme parzialmente ordinato finito, e sia

$$\varphi : P \longrightarrow P$$
$$\varphi : x \longrightarrow \bar{x}$$

un operatore di chiusura su P. Posto

$$\bar{P} = \{x \in P;\ x = \bar{x}\}$$

si ha, indicando con μ e $\bar{\mu}$ le funzioni di Möbius di P e $\bar{P}$ rispettivamente:

$$\sum_{\substack{t \in P \\ \bar{t}=\bar{y}}} \mu(t,x) = \begin{cases} 0 & \text{se } x < \bar{x} \\ \bar{\mu}(\bar{y},\bar{x}) & \text{se } x = \bar{x} \end{cases},$$

per ogni $x,y \in P$.

DIMOSTRAZIONE Per il Teorema 6.6, dato che la restrizione a $\bar{P}$ di ogni filtro principale di P è un filtro principale di $\bar{P}$, φ si può estendere ad un morfismo di algebre

$$\phi : M(P) \longrightarrow M(\bar{P}) \quad .$$

Per ogni $x \in P$ si ha:

$$\phi(e_x) = \begin{cases} 0 & \text{se } x < \bar{x} \\ \bar{e}_x & \text{se } x = \bar{x} \end{cases}$$

dove $\bar{e}_x$ è l'idempotente corrispondente ad x in $M(\bar{P})$. Ma, in $M(P)$, risulta:

$$e_x = \sum_{t \leq x} \mu(t,x)t$$

e, in $M(\bar{P})$, se $x = \bar{x}$:

$$\bar{e}_x = \sum_{\bar{y} \leq \bar{x}} \bar{\mu}(\bar{y},\bar{x})\bar{y} \quad ;$$

confrontando i coefficienti di $\bar{y}$ in $\bar{e}_x$ ed in $\phi(e_x)$ si ha l'uguaglianza voluta.

Se poi $x < \bar{x}$, $\phi(e_x) = 0$ fornisce la seconda uguaglianza. ∎

6.9. COROLLARIO Siano P,Q insiemi parzialmente ordinati finiti; supponiamo che siano date due funzioni

$$\varphi : P \longrightarrow Q$$
$$\psi : Q \longrightarrow P$$

che formino una connessione di Galois fra P e Q . Allora, per ogni $p \in P$ ed ogni $q \in Q$, risulta

$$\sum_{\substack{t \in P \\ \varphi(t)=q}} \mu_P(p,t) = \begin{cases} 0 & \text{se } \psi(\varphi(p)) > p \\ \displaystyle\sum_{\substack{s \in Q \\ \varphi(\psi(s))=\varphi(p)}} \mu_Q(s,q) & \text{se } \psi(\varphi(p)) = p \, , \end{cases}$$

dove μ_P e μ_Q sono le funzioni di Möbius di P e Q , rispettivamente. ∎

7. La funzione di Möbius nei reticoli semimodulari

Sia P un insieme parzialmente ordinato finito dotato di minimo $\hat{0}$ e tale che, per ogni $x,y \in P$, $x \leq y$, tutte le catene massimali tra x e y abbiano lo stesso numero di elementi; si definisce rango di un elemento $x \in P$ l'intero

$$r(x) = l(x) - 1 \quad ,$$

dove $l(x)$ è la cardinalità di una catena massimale tra $\hat{0}$ ed x. Inoltre, se P è dotato di massimo $\hat{1}$, si dice rango di P l'intero

$$r(P) = r(\hat{1}) \quad .$$

Per ogni $a,b \in P$, $a \leq b$, si dice polinomio caratteristico dell'intervallo $[a,b]$ il polinomio nella variabile formale λ :

$$P([a,b]; \lambda) = \sum_{x \leq b} \mu(a,x)\lambda^{r(b)-r(x)} \quad .$$

Osserviamo che

$$P([a,b]; 0) = \mu(a,b) \quad .$$

7.1. TEOREMA Sia P un inf-semireticolo dotato di rango; per ogni $a,b,c \in P$, con $c \leq a \wedge b$, si ha:

$$\lambda^{r(b)-r(a\wedge b)} P([c,a\wedge b]; \lambda) =$$

$$= \sum_{x\wedge a=c} P([x,b]; \lambda) \quad .$$

DIMOSTRAZIONE Si ha:

$$\sum_{x\wedge a=c} P([x,b];\lambda) = \sum_{x\wedge a=c}\ \sum_{y\leq b} \mu(x,y)\lambda^{r(b)-r(y)} =$$

$$= \lambda^{r(b)} \sum_{x\in P}\ \sum_{t\leq a} \mu(c,t)\,\zeta(t,x) \sum_{y\leq b} \mu(x,y)\lambda^{-r(y)} =$$

$$= \lambda^{r(b)} \sum_{y\leq b} \lambda^{-r(y)} \sum_{x\in P}\ \sum_{t\leq a} \mu(c,t)\,\zeta(t,x)\mu(x,y) =$$

$$= \lambda^{r(b)} \sum_{y\leq b} \lambda^{-r(y)}\ \mu(c,y)\,\zeta(y,a) =$$

$$= \lambda^{r(b)-r(a\wedge b)} \sum_{y\leq a\wedge b} \mu(c,y)\lambda^{r(a\wedge b)-r(y)} =$$

$$= \lambda^{r(b)-r(a\wedge b)}\ P([c,a\wedge b];\lambda) \quad . \blacksquare$$

7.2. COROLLARIO Sia P un inf-semireticolo dotato di rango, e siano $a,b,d\in P$ tali che $a\wedge b = a\wedge d$. Allora, per ogni $c\in P$, si ha:

$$\lambda^{r(d)} \sum_{t\wedge a=c} P([t,b];\lambda) = \lambda^{r(b)} \sum_{s\wedge a=c} P([s,d];\lambda) \quad .$$

DIMOSTRAZIONE Per il Teorema precedente, si ha:

$$\sum_{t\wedge a=c} P([t,b];\lambda) = \lambda^{r(b)-r(a\wedge b)} P([c,a\wedge b];\lambda) \quad ;$$

$$\sum_{s\wedge a=c} P([s,d];\lambda) = \lambda^{r(d)-r(a\wedge d)} P([c,a\wedge d];\lambda) \quad ;$$

dato che $a\wedge b = a\wedge d$, si ha la tesi.■

7.3. COROLLARIO Sia P un inf-semireticolo dotato di rango, e siano $a,b \in P$, $a \leq b$. Allora

$$\lambda^{r(b)-r(a)} = \sum_{t\geq a} P([t,b];\lambda) \quad .■$$

Un reticolo finito L si dice semimodulare se gode della seguente proprietà: per ogni $a,b \in L$ tali che a copra $a\wedge b$, $a\vee b$ copre b.

Ricordiamo che un reticolo semimodulare è dotato di rango r; inoltre, per ogni $a,b \in L$, risulta:

$$r(a\vee b) + r(a\wedge b) \leq r(a) + r(b) \quad .$$

Se L è un reticolo semimodulare, $a,b \in L$ formano una coppia modulare se

$$r(a\vee b) + r(a\wedge b) = r(a) + r(b) \quad ,$$

o, equivalentemente, se, per ogni $x \in L$ tale che $x < b$, si ha

$$x\vee(a\wedge b) = (x\vee a)\wedge b \quad .$$

Un elemento a di L si dice <u>elemento modulare</u> se, per ogni $x \in L$, la coppia (a,x) è una coppia modulare.

Sia L un reticolo semimodulare. Si dice <u>k-mo numero di Whitney di prima specie</u> di L il numero

$$w_k = \sum_{\substack{x \in L \\ r(\hat{1})-r(x)=k}} \mu(\hat{0},x)$$

dove $\hat{0}$, $\hat{1}$ sono rispettivamente il minimo ed il massimo di L, e μ è la funzione di Möbius di L. w_k risulta quindi il coefficiente di λ^k nel polinomio caratteristico $P(L;\lambda)$.

Si dice poi <u>k-mo numero di Whitney di seconda specie</u> di L il numero

$$W_k = \left|\left\{ x \in L;\ r(\hat{1}) - r(x) = k \right\}\right| .$$

Si dice inoltre <u>invariante di Crapo</u> di L il numero

$$\beta(L) = \left| \left(\frac{d}{d\lambda} P(L;\lambda)\right)_{\lambda=1} \right| .$$

Un reticolo semimodulare si dice <u>supersolubile</u> se esiste una catena massimale tra $\hat{0}$ ed $\hat{1}$ i cui elementi siano tutti modulari.

Un reticolo semimodulare L si dice <u>geometrico</u> se i soli elementi sup-irriducibili di L sono gli atomi e il minimo $\hat{0}$.

7.4. TEOREMA Sia L un reticolo semimodulare. Per ogni $x,y \in L$ si ha:

a) se $r(x) = r(y)$ e $\mu(\hat{0},x)$, $\mu(\hat{0},y)$ sono entrambe non nulle, allora $\mu(\hat{0},x)$ e $\mu(\hat{0},y)$ hanno lo stesso segno;

b) se $r(x) = r(y)+1$ e $\mu(\hat{0},x)$, $\mu(\hat{0},y)$ sono entrambe non nulle, allora $\mu(\hat{0},x)$ e $\mu(\hat{0},y)$ hanno segni opposti;

c) se $\mu(\hat{0},x) \neq 0$, allora $\mu(\hat{0},x)$ è positivo o negativo, a seconda che $r(x)$ sia pari o dispari, rispettivamente;

d) se L è geometrico, $\mu(\hat{0},x) \neq 0$.

DIMOSTRAZIONE Sia $x \in L$, tale che $r(x) = k > z$. Per il Lemma di Weisner, si ha, per ogni atomo $a \in [\hat{0},x]$:

$$(*) \qquad \mu(\hat{0},x) = - \sum_{\substack{y \vee a = x \\ y \neq x}} \mu(\hat{0},y)$$

e, grazie alla semimodularità di L:

$$A = \{y \in L;\ y \vee a = x, y \neq x\} =$$
$$= \{y \in L;\ y \leq x,\ r(y) = k-1,\ y \not\geq a\} .$$

Dimostriamo la prima affermazione procedendo per induzione su $r(x)$. Se $r(x) = 2$, la tesi è vera. Se $r(x) = k > 2$, e l'insieme A è non vuoto, per l'ipotesi di induzione tutti i $\mu(\hat{0},y)$ con $y \in A$ hanno lo stesso segno, e, grazie alla $(*)$, segue la prima affermazione. La seconda affermazione si deduce dalla prima applicando nuovamente l'identità $(*)$. La terza affermazione si dimostra ancora per induzione, a partire dalla $(*)$. Se poi il reticolo L è geometrico, ricordiamo che:

$$\mu(\hat{0},x) > 0 \qquad \text{per ogni} \quad x \in L \qquad \text{tale che} \quad r(x) = 2 \ ;$$

procedendo per induzione su $r(x)$ e utilizzando ancora $(*)$, si ha l'ultima affermazione.■

7.5. COROLLARIO Sia L un reticolo geometrico. Allora, i coefficienti del polinomio caratteristico $P(L;\lambda)$ hanno segni alterni.■

E' ben noto che ogni reticolo geometrico L è isomorfo al reticolo dei chiusi dell'algebra di Boole B generata dagli atomi di L, rispetto ad un operatore di chiusura

$$\varphi : B \longrightarrow B$$

tale che:

i) φ muta atomi di B in atomi di B;

ii) per ogni $a,b,x \in B$, con a,b atomi,

$$a \leq \varphi(x \vee b) \ , \qquad a \not\leq \varphi(x)$$

implica

$$b \leq \varphi(x \vee a) \quad .$$

7.6. PROPOSIZIONE Sia L un reticolo geometrico, e sia A l'insieme degli atomi di L. Allora, per ogni $x \in L$, si ha

$$\mu(\hat{0},x) = \sum_{\substack{F \subseteq A \\ \bigvee_{a \in F} a = x}} (-1)^{|F|} \quad .$$

DIMOSTRAZIONE Segue dalla Proposizione 6.8.■

7.7. COROLLARIO Sia L un reticolo geometrico, e sia A l'insieme degli atomi di L. Allora:

$$P(L;\lambda) = \sum_{F \subseteq A} (-1)^{|F|} \lambda^{r(\hat{1})-r(f)}$$

dove

$$f = \bigvee_{x \in F} x$$

DIMOSTRAZIONE Si ha, per la proposizione precedente:

$$\sum_{F \subseteq A} (-1)^{|F|} \lambda^{r(\hat{1})-r(f)} =$$

$$= \sum_{x \in L} \sum_{\substack{F \subseteq A \\ f=x}} (-1)^{|F|} \lambda^{r(\hat{1})-r(x)} =$$

$$= \sum_{x \in L} \mu(\hat{0},x) \lambda^{r(\hat{1})-r(x)} = P(L;\lambda) \quad .■$$

7.8. TEOREMA Sia L un reticolo semimodulare, e sia a un elemento modulare di L. Allora:

$$P(L;\lambda) = P([\hat{0},a];\lambda) \sum_{y \wedge a = \hat{0}} \mu(\hat{0},y)\lambda^{r(\hat{1})-r(a)-r(y)} \quad .$$

DIMOSTRAZIONE Dal Teorema 6.4 applicato al reticolo duale di L si ha:

$$\sum_{x\in L} \mu(\hat{0},x)x = \sum_{t\leq a} \mu(\hat{0},t) \sum_{y\wedge a=\hat{0}} \mu(\hat{0},y)\, t\vee y \quad ;$$

effettuando le sostituzioni:

$$x \longleftarrow \lambda^{r(\hat{1})-r(x)}$$

$$t\vee y \longleftarrow \lambda^{r(\hat{1})-r(t\vee y)}$$

si ha:

$$(*) \qquad \sum_{x\in L} \mu(\hat{0},x)\, \lambda^{r(\hat{1})-r(x)} =$$

$$= \sum_{t\leq a} \mu(\hat{0},t) \sum_{y\wedge a=\hat{0}} \mu(\hat{0},y)\, \lambda^{r(\hat{1})-r(t\vee y)} \quad ;$$

ora, poiché a è un elemento modulare, per ogni $y,t\in L$ risulta:

$$(1) \qquad r(y\vee a)+r(y\wedge a) = r(a) + r(y)$$

e

$$(2) \qquad r(t\vee y\vee a)+r(t\vee y)\wedge a) = r(t\vee y) + r(a) \quad ;$$

se $t \leq a$, essendo a un elemento modulare, risulta:

$$(t\vee y)\wedge a = t\vee(y\wedge a)$$

e, se $y\wedge a = \hat{0}$, si ha

$$(t\vee y)\wedge a = t$$

da cui, utilizzando (1) e (2):

$$r(t \vee y) = r(t) + r(y) \quad ;$$

sostituendo quest'ultima identità nella (*) si ha la tesi. ■

7.9. COROLLARIO Sia L un reticolo semi-modulare, e sia p un atomo di L. Allora

$$\beta(L) = (-1)^{r(\hat{1})-1} \sum_{y \ngeq p} \mu(\hat{0},y) \quad .$$

DIMOSTRAZIONE Segue dalla Proposizione precedente, ponendo $a = p$. ■

7.10. TEOREMA Sia L un reticolo supersolubile, e sia

$$0 = a_o < a_1 < \ldots < a_{k-1} < a_k = \hat{1}$$

una catena massimale di elementi modulari in L. Allora

$$P(L;\lambda) = (\lambda - n_1)(\lambda - n_2)\ldots(\lambda - n_k) \quad ,$$

dove

$$n_i = \left| \left\{ x \in L;\ x \text{ atomo},\ x \leq a_i,\ x \nleq a_{i-1} \right\} \right|$$

per $i = 1, 2, \ldots, k$.

DIMOSTRAZIONE Procediamo per induzione su k. Se $k = 1$, l'affermazione è vera. Sia $k > 1$. Dalla Proposizione 7.8, si ha:

$$P(L;\lambda) = P([\hat{0},a_{k-1}];\lambda) \sum_{y\wedge a_{k-1}=\hat{0}} \mu(\hat{0},y)\, \lambda^{1-r(y)} \quad ;$$

d'altra parte:

$$\{y\in L;\ y\wedge a_{k-1} = \hat{0}\} =$$

$$= \{\hat{0}\} \cup \{y\in L;\ r(y) = 1,\ y \not\leq a_{k-1}\} \quad ,$$

da cui

$$\sum_{y\wedge a_{k-1}=\hat{0}} \mu(\hat{0},y)\, \lambda^{1-r(y)} = \lambda - n_k \quad . \blacksquare$$

7.11. COROLLARIO Se L è un reticolo supersolubile, allora

$$\mu(\hat{0},\hat{1}) = (-1)^k\, n_1 n_2 \dots n_k \quad . \blacksquare$$

Sia L un reticolo geometrico. Il polinomio di Möbius di L è il polinomio definito nel modo seguente:

$$M(L;s,t) = \sum_{x,y\in L} \mu(x,y)\, s^{r(x)}\, t^{r(\hat{1})-r(y)} =$$

$$= \sum_{x\in L} s^{r(x)}\, P([x,\hat{1}];\ t) \quad .$$

Sia L un reticolo geometrico, e sia A l'insieme degli atomi di L. Un sottoinsieme I di A si dice indipendente se, posto $y = \bigvee_{x \in I} x$, risulta

$$r(y) = |I| \quad .$$

Un <u>circuito</u> di L è un sottoinsieme di A non indipendente minimale.

7.12. TEOREMA Sia L un reticolo geometrico di rango r ; indichiamo con c la cardinalità minima di un circuito in L , e con n il numero degli atomi di L . Allora sussistono le seguenti disuguaglianze:

1) $$|w_{r-k}| \geq \sum_{i=0}^{c-2} \binom{n-r+i-1}{i}\binom{r-i}{k-i}$$

per ogni $k \leq r$; l'uguaglianza sussiste se e solo se L è isomorfo al prodotto diretto dell'algebra di Boole di rango r-c+1 con il (c-1)-troncamento dell'algebra di Boole di rango n-r+c-1 . In particolare

$$|\mu(\hat{0},\hat{1})| \geq \binom{n-r+c-2}{c-2} \quad .$$

2) $$|w_{r-k}| \geq \sum_{i=0}^{c-1} \binom{n-r+i-1}{i}\binom{r-i}{k-i} - q\binom{r-c+1}{r-k} \quad ,$$

dove q è il numero dei circuiti di L aventi cardinalità esattamente c . In particolare

$$|\mu(\hat{0},\hat{1})| \geq \binom{n-r+c-1}{c-1} - q \quad .$$

3) Se L è connesso e $c \leq r$,

$$|w_{r-k}| \geq \sum_{i=0}^{c-2} \binom{n-r+i-1}{i}\binom{r-i}{k-i} + (n-r)\binom{r-c+2}{k-c+1}$$

per $k \leq r-2$; inoltre:

$$|w_1| \geq \sum_{i=0}^{c-2} (r-i)\binom{n-r+i-1}{i} + (n-r)\left(\binom{r-c+2}{2}-1\right) + \beta(L)$$

e, infine:

$$|\mu(\hat{0},\hat{1})| \geq \binom{n-r+c-2}{c-2} + (n-r)(r-c) + \beta(L)$$

ove $\beta(L)$ è l'invariante di Crapo del reticolo geometrico L.■

8. L'anello di Tutte-Grothendieck

Sia L un reticolo geometrico. Una base di L è un insieme

$$A = \{a_1, a_2, \dots, a_n\}$$

di atomi di L tale che:

i) $a_1 \vee a_2 \vee \dots \vee a_n = \hat{1}$;

ii) A è minimale rispetto alla proprietà i).

Un istmo di L è un atomo che appartiene ad ogni base di L.

Ricordiamo che, se p è un istmo di L, si ha l'isomorfismo:

$$(*) \qquad L \cong [\hat{0},p] \oplus [p,\hat{1}]$$

dove $\oplus$ indica l'usuale somma diretta di reticoli. Viceversa, se per un atomo p sussiste l'isomorfismo $(*)$, allora p è un istmo di L. Inoltre, se p è un istmo di L, si ha l'isomorfismo

$$[p,\hat{1}] \cong L-p \quad ,$$

dove $L-p$ indica il reticolo geometrico generato dagli atomi di L diversi da p.

E' poi facile verificare che, se p,q sono atomi di L, si ha:

$$[q,\hat{1}] - (p \vee q) \cong [q,\hat{1}]_{L-p} \quad ,$$

dove $[q,\hat{1}]_{L-p}$ indica l'intervallo $[q,\hat{1}]$ nel reticolo $L-p$.

Osserviamo infine che, fissato $p \in L$, l'applicazione

$$q \longrightarrow p \vee q$$

muta atomi di L in atomi di $[p,\hat{1}]$.

Indicheremo in seguito con $\mathscr{L}$ l'insieme delle classi di isomorfismo di reticoli geometrici. In particolare, indicheremo con x la classe di equivalenza dei reticoli geometrici con due elementi.

Dato un anello commutativo unitario A, un <u>invariante di Tutte-Grothendieck</u> a valori in A è un'applicazione

$$\varphi : \mathscr{L} \longrightarrow A$$

tale che:

i) $\varphi(L_1 \oplus L_2) = \varphi(L_1)\,\varphi(L_2)$;

ii) $\varphi(L) = \varphi([p,\hat{1}]) + \varphi(L-p)$,

se p è un atomo di L e non è istmo di L .

Indichiamo ora con $\mathbb{Z}(\mathscr{L})$ la $\mathbb{Z}$-algebra commutativa unitaria libera generata da $\mathscr{L}$.

Sia $\mathscr{I}$ l'ideale di $\mathbb{Z}(\mathscr{L})$ generato dagli elementi della forma:

T1) $L_1 \oplus L_2 - L_1 L_2$;

T2) $L-(L-p)-[p,\hat{1}]$, se p è un atomo di L e non è un istmo di L .

Si dice <u>anello di Tutte-Grothendieck</u> l'anello quoziente

$$\mathscr{T} = \mathbb{Z}(\mathscr{L})/\mathscr{I} \quad .$$

8.1. TEOREMA (di struttura) L'anello di Tutte-Grothendieck è isomorfo all'anello dei polinomi in una variabile a coefficienti interi senza termine noto.

DIMOSTRAZIONE E' sufficiente provare che, per ogni $L \in \mathscr{L}$, nella classe di equivalenza di L in $\mathscr{T}$ esiste un unico polinomio a coefficienti interi (positivi), senza termine noto, nella variabile x , che rappresenta la classe di equivalenza dei reticoli geometrici con due elementi. Con un semplice argomento di induzione è facile provare che ogni reticolo L è equivalente ad un tale polinomio. Per provare che questo polinomio è unico, è sufficiente dimostrare che applicare ad L le identità subordinate da T1 e T2) ordinatamente rispetto agli atomi p,q è equivalente ad applicare le stesse identità ordinatamente rispetto agli atomi q,p.

Supponiamo dapprima che p,q non siano istmi per L. Dimostriamo prima di tutto che, in questo caso, p è istmo per $L-q$ se e solo se q è istmo per $L-p$. Infatti, se p non è istmo per $L-q$, esiste una base B di $L-q$ che non contiene p. Dato che q non è istmo per L, B è anche una base di L e, non contenendo p, è una base per $L-p$. Di conseguenza, q non è istmo per $L-p$. Allora, nell'ipotesi che p non sia un istmo per $L-q$, si ottengono le seguenti identità:

$$\begin{aligned} L &= (L-p) + [p,\hat{1}] = \\ &= (L-\{p,q\}) + [q,\hat{1}]_{L-p} + ([p,\hat{1}]-q) + [p\vee q,\hat{1}] = \\ &= (L-\{p,q\}) + ([q,\hat{1}]-p) + ([p,\hat{1}]-q) + [p\vee q,\hat{1}] = \\ &= (L-q) + [q,\hat{1}] = L \ . \end{aligned}$$

Se invece p è istmo per $L-q$:

$$\begin{aligned} L &= (L-p) + [p,\hat{1}] = \\ &= (L-\{p,q\})x + ([p,\hat{1}]-q) + [p\vee q,\hat{1}] = \\ &= (L-\{p,q\})x + [p,\hat{1}]_{L-q} + [p\vee q,\hat{1}] = \\ &= (L-q) + [q,\hat{1}] = L \ . \end{aligned}$$

Supponiamo ora che p sia istmo per L, e q non lo sia. Allora:

$$\begin{aligned} L &= (L-p)x = ((L-\{p,q\}) + [q,\hat{1}]_{L-p})x = \\ &= (L-q) + [q,\hat{1}] = L \ . \end{aligned}$$

Infine, se p e q sono entrambi istmi per L , allora:

$$L = (L - p)x = (L - \{p,q\})x^2 =$$

$$= (L - q)x = L \quad . \blacksquare \; .$$

8.2. PROPOSIZIONE L'immersione naturale

$$\tau : \mathscr{L} \longrightarrow \mathscr{T}$$

è l'invariante di Tutte-Grothendieck universale, cioè, per ogni invariante di Tutte-Grothendieck

$$\varphi : \mathscr{L} \longrightarrow A$$

esiste un unico morfismo di anelli

$$h : \mathscr{T} \longrightarrow A$$

tale che

$$\varphi = h \circ \tau \quad .$$

Inoltre, per ogni $L \in \mathscr{L}$, $\varphi(L)$ si ottiene da $\tau(L)$ effettuando la sostituzione

$$x \longleftarrow \varphi(x) \quad . \blacksquare$$

8.3. PROPOSIZIONE Il "valore assoluto" del polinomio caratteristico:

$$(-1)^{r(\hat{1})} \; P(L;\lambda)$$

è un invariante di Tutte-Grothendieck, ed il suo valore si ottiene da $\tau(L)$ effettuando la sostituzione

$$x \leftarrow 1-\lambda \quad .$$

DIMOSTRAZIONE Ricordiamo che, se $a \in L_1$ e $b \in L_2$, allora

$$\mu_{L_1}(\hat{0},a)\ \mu_{L_2}(\hat{0},b) = \mu_{L_1 \oplus L_2}(\hat{0}, a \vee b)$$

ed inoltre, in $L_1 \oplus L_2$, risulta

$$r(a) + r(b) = r(a \vee b) \quad .$$

Da ciò si deduce

$$P(L_1 \oplus L_2;\lambda) = P(L_1;\lambda)\ P(L_2;\lambda) \quad .$$

Proviamo ora che, per ogni $L \in \mathscr{L}$ e per ogni p atomo di L, p non istmo, risulta:

$$P(L;\lambda) = -\ P([p,\hat{1}];\lambda) + P(L-p;\lambda) \quad .$$

Infatti, se A è l'insieme degli atomi di L, si ha:

$$P(L;\lambda) = \sum_{B \subseteq A} (-1)^{|B|}\ \lambda^{r(\hat{1})-r(\vee B)} =$$

$$= \sum_{\substack{B \subseteq A \\ p \notin B}} (-1)^{|B|}\ \lambda^{r(\hat{1})-r(\vee B)} +$$

$$+ \sum_{\substack{C\subseteq A\\ p\notin C}} (-1)^{|C|+1} \lambda^{r(\hat{1})-r(\vee C\vee p)} =$$

$$= P(L-p;\lambda) - \sum_{\substack{C\subseteq A\\ p\notin C}} (-1)^{|C|} \lambda^{r_p(\hat{1})-r_p(\vee C\vee p)} =$$

$$= P(L-p;\lambda) - P([p,\hat{1}];\lambda)$$

dove r_p indica il rango in $[p,\hat{1}]$ e

$$\vee B = \bigvee_{b\in B} b \quad , \qquad \vee C = \bigvee_{c\in C} c \quad .$$

Infine, ricordiamo che, se p non è istmo per L ,

$$r([p,\hat{1}]) = r(L)-1 = r(L-p)-1 \quad .$$

Da qui segue la tesi.■

8.4. COROLLARIO Il valore assoluto $|\mu(\hat{0},\hat{1})|$ della funzione di Möbius tra gli estremi $\hat{0}$ ed $\hat{1}$ è un invariante di Tutte-Grothendieck.

DIMOSTRAZIONE Segue dalla Proposizione precedente, osservando che

$$|\mu(\hat{0},\hat{1})| = (-1)^{r(\hat{1})} P(L;0) \quad .$$■

8.5. COROLLARIO Per ogni $L\in\mathscr{L}$ e per ogni p atomo di L , si ha:

a) $|\mu(p,\hat{1})| \leq |\mu(\hat{0},\hat{1})|$;

l'uguaglianza sussiste se e solo se p è un istmo;

b) $|\mu_{L-p}(\hat{0},\hat{1})| \leq |\mu(\hat{0},\hat{1})|$,

dove μ_{L-p} indica la funzione di Möbius di $L-p$;

c) se $x,y \in L$ sono tali che $x \in y^{\perp}$ e inoltre (x,y) è una coppia modulare, allora

$|\mu(\hat{0},x)| \leq |\mu(y,\hat{1})|$;

l'uguaglianza sussiste se e solo se si ha l'isomorfismo

$$[\hat{0},x] \cong [y,\hat{1}] \quad . \blacksquare$$

8.6. COROLLARIO L'invariante di Crapo soddisfa le seguenti identità:

i) se $p \in L$ e p non è istmo, allora

$\beta(L) = \beta(L-p) + \beta([p,\hat{1}])$;

ii) $\beta(L_1 \oplus L_2) = 0$.■

8.7. TEOREMA Sia L un reticolo geometrico, e sia $a \in L$. Allora

$$|\mu(\hat{0},a)| \sum_{y \perp a} |\mu(\hat{0},y)| \leq |\mu(\hat{0},\hat{1})|$$

dove $y \perp a$ indica che y è un complemento di a e che (y,a) è una coppia modulare.

L'uguaglianza vale se e solo se a è un elemento modulare di L.

DIMOSTRAZIONE Procediamo per induzione sul numero n di atomi di L che non sono minori o uguali ad a. Se $n = 1$ l'affermazione è banale. Sia $n > 1$. Per l'ipotesi di induzione, per ogni atomo $p \in L$, $p \not\leq a$, risulta

$$(*) \qquad |\mu_{L-p}(\hat{0},\hat{1})| \geq |\mu(\hat{0},a)| \sum_{\substack{y \in L-p \\ y \perp a}} |\mu_{L-p}(\hat{0},y)| ,$$

poiché $a \in L-p$ e $\mu_{L-p}(\hat{0},a) = \mu(\hat{0},a)$. Se p è un istmo di L, il teorema segue immediatamente, in quanto

$$|\mu_{L-p}(\hat{0},y)| = |\mu(\hat{0},y \vee p)|$$

e $y \perp a$ in $L-p$ se e solo se $(y \vee p) \perp a$ in L.

Se invece p non è istmo, sommando $|\mu(p,\hat{1})|$ ad ambo i membri della $(*)$, otteniamo:

$$|\mu(\hat{0},\hat{1})| \geq |\mu(\hat{0},a)| \sum_{\substack{y \in L-p \\ y \perp a}} |\mu_{L-p}(\hat{0},y)| + |\mu(p,\hat{1})| ;$$

ma, per l'ipotesi di induzione, abbiamo:

$$|\mu(p,\hat{1})| \geq |\mu(p,a \vee p)| \sum_{\substack{y \geq p \\ y \perp a}} |\mu(p,y)| \geq$$

$$\geq |\mu(\hat{0},a)| \sum_{\substack{y \geq p \\ y \perp a}} |\mu(p,y)| ,$$

grazie al Corollario 8.5, in quanto $(a \vee p) \perp y$ in $[p,\hat{1}]$ se e solo se $y \geq p$ e $a \perp y$. Osserviamo ora che, se $y \not\geq p$,

$$|\mu_{L-p}(\hat{0},y)| = |\mu(\hat{0},y)| \quad ,$$

e, se $y \geq p$,

$$|\mu_{L-p}(\hat{0},y)| + |\mu(p,y)| \geq |\mu(\hat{0},y)| \quad ,$$

dove l'uguaglianza sussiste se e solo se p non è istmo per $[\hat{0},y]$. Di conseguenza:

$$|\mu(\hat{0},\hat{1})| \geq |\mu(\hat{0},a)| \sum_{\substack{y \in L-p \\ y \perp a}} |\mu_{L-p}(\hat{0},y)| +$$

$$+ \sum_{\substack{y \geq p \\ y \perp a}} |\mu(p,y)|) \geq |\mu(\hat{0},a)| \sum_{y \perp a} |\mu(\hat{0},y)| \quad .$$

In modo analogo si dimostra la seconda affermazione del Teorema.■

8.8. COROLLARIO Sia L un reticolo geometrico, e sia x un coatomo di L . Posto

$$A(x) = |\{a \in L;\ a \text{ atomo},\ a \not\leq x\}| \quad ,$$

risulta:

$$|\mu(\hat{0},\hat{1})| \geq A(x)\ |\mu(\hat{0},x)| \quad .$$

L'uguaglianza sussiste se e solo se x è un elemento modulare.

DIMOSTRAZIONE Dal momento che x è un coatomo di L, un elemento $a \in L$ tale che (x,a) sia una coppia modulare e a sia un complemento di x è necessariamente un atomo non minore di x; la disuguaglianza segue allora dal Teorema precedente. ■

8.9. COROLLARIO Sia L un reticolo geometrico di rango n; allora

$$W_{n-1} \leq W_1 \quad ,$$

dove W_i indica l'i-mo numero di Whitney di seconda specie di L. L'uguaglianza sussiste se e solo se L è modulare.

DIMOSTRAZIONE Con le notazioni del corollario precedente, si ha:

$$W_1 |\mu(\hat{0},\hat{1})| \geq \sum_{\substack{x \in L \\ r(x)=n-1}} |\mu(\hat{0},x)|\, A(x) =$$

$$= \sum_{\substack{p \in L \\ r(p)=1}} \sum_{\substack{x \not\geq p \\ r(x)=n-1}} |\mu(\hat{0},x)| \quad ;$$

per il Lemma di Weisner, quest'ultimo intero è uguale a

$$W_{n-1} |\mu(\hat{0},\hat{1})| \quad . ■$$

8.10. COROLLARIO Sia L un reticolo geometrico. Per ogni $i = 1, 2, \ldots, n-1$ risulta:

$$W_{n-1} \leq W_i \quad .$$

8.11. COROLLARIO Sia L un reticolo geometrico, e sia

$$\hat{0} = x_o < x_1 < \dots < x_{n-1} < x_n = \hat{1}$$

una catena massimale in L . Posto

$$\lambda_k = |\{a \in L;\ a \text{ atomo},\ a \leq x_k,\ a \nleq x_{k-1}\}| \ ,$$

risulta:

$$|\mu(\hat{0},\hat{1})| \geq \lambda_1\lambda_2 \dots \lambda_n \quad .$$

L'uguaglianza sussiste se e solo se ciascun x_i è modulare.

DIMOSTRAZIONE Si applica il Teorema 8.7 successivamente agli elementi $x_{n-1}, x_{n-2}, \dots, x_1$. ■

9. Un'applicazione geometrica

Nello spazio affine $\mathbb{R}^d$ consideriamo un insieme finito H di iperpiani. Questi individuano in $\mathbb{R}^d$ un numero finito di poliedri d-dimensionali (aperti e non necessariamente limitati), chiamati regioni. Gli iperpiahi di H saranno detti tagli; diremo partizione dello spazio mediante H l'insieme di tutte le facce (aperte) k-dimensionali, per $k = 0,1,\dots,d$, dei poliedri d-dimensionali individuati da H .

La partizione relativa alla famiglia di iperpiani H si dirà centrale se

$$\bigcap_{h\in H} h \neq \phi \quad .$$

Per estensione, anche la famiglia H si dirà centrale.

Data una famiglia finita H di iperpiani in $\mathbb{R}^d$, consideriamo l'insieme parzialmente ordinato S costituito da tutte le intersezioni non vuote degli elementi di H, ordinate per inclusione. Per convenzione, poniamo $\mathbb{R}^d \in S$. Indichiamo con L_H il duale d'ordine di S. L_H risulta un inf-semireticolo, e si dirà semireticolo associato ad H. Osserviamo che, per costruzione, il semireticolo L_H è atomico ed è dotato di rango r; in particolare, per ogni $x \in L_H$, si ha:

$$r(x) = d - \dim x \quad .$$

Per definizione, poniamo

$$r(L_H) = \max \{ r(x) ; \ x \in L_H \} \quad .$$

Notiamo che, se H è centrale, posto

$$a = \bigcap_{h\in H} h$$

L_H è isomorfo alla restrizione ad H del duale d'ordine dell'intervallo $[a, \hat{1}]$ del reticolo dei sottospazi di $\mathbb{R}^d$. Di conseguenza, L_H risulta un reticolo geometrico.

Sia H un insieme finito di iperpiani di $\mathbb{R}^d$. Poniamo:

$c(H)$ = numero delle regioni individuate da H,

$f_k(H)$ = numero delle facce k-dimensionali individuate da H,

per $k = 0, 1, \dots, d$.

La funzione generatrice degli interi $f_k(H)$:

$$f_H(t) = \sum_{k=0}^{d} f_k(H)\, t^{d-k}$$

si dirà <u>f-polinomio</u> di H .

9.1. TEOREMA Sia H un insieme finito di iperpiani di $\mathbb{R}^d$. Allora

$$c(H) = \sum_{y \in L_H} |\mu(\hat{0},y)| \quad .$$

DIMOSTRAZIONE Proviamo innanzi tutto che c(H) soddisfa la seguente recursione: per ogni h iperpiano di $\mathbb{R}^d$, $h \notin H$, poniamo

$$F_h = \{h \cap k;\ k \in H,\ \dim(h \cap k) = d-2\} \quad ;$$

risulta allora

$$(*) \qquad c(H \cup h) = c(H) + c(F_h) \quad .$$

Infatti, sia P una regione individuata da H . Se P non è intersecata da h , allora è anche una regione relativamente ad $H \cup h$. Se invece P è intersecata da h , P si può suddividere in tre parti disgiunte: due sottoinsiemi aperti di $\mathbb{R}^d$, che sono regioni relative ad $H \cup h$, e $P \cap h$, che è una regione relativa ad F_h .

Viceversa, se Q è una regione relativa ad F_h , allora esiste una regione P relativa ad H tale che $Q = P \cap h$; infatti, se ciò non fosse vero, avremmo necessariamente $Q \subseteq h'$ per qualche $h' \in H$, e questo implicherebbe $h = h' \in H$, il che è assurdo.

Quindi, ogni regione di H corrisponde ad una regione di $H \cup h$, oppure a due regioni di $H \cup h$ e ad una di F_h, e questa corrispondenza esaurisce le regioni di $H \cup h$ e di F_h. Questo prova la ricursione (*).

Poniamo ora, per ogni insieme finito H di iperpiani di $\mathbb{R}^d$:

$$V(H) = \sum_{y \in L_H} |\mu(\hat{0},y)|$$

e proviamo che è soddisfatta la recursione:

$$V(H \cup h) = V(H) + V(F_h) \quad .$$

Sia $y \in L_{H \cup h}$; l'intervallo $[\hat{0},y]$ in $L_{H \cup h}$ è un reticolo geometrico, per ovvie considerazioni. Di conseguenza si ha:

$$(**) \qquad |\mu_{H \cup h}(\hat{0},y)| = |\mu_H(\hat{0},y)| + |\mu_{H \cup h}(h,y)|$$

dove $\mu_{H \cup h}$ e μ_H indicano la funzione di Möbius di $L_{H \cup h}$ e di L_H, rispettivamente. Infatti, se $h \not\leq y$, allora

$$\mu_{H \cup h}(\hat{0},y) = \mu_H(\hat{0},y)$$

e

$$\mu_{H \cup y}(h,y) = 0 \quad ;$$

se invece $h \leq y$, l'identità segue dal fatto che $[\hat{0},y]$ è un reticolo geometrico e $|\mu_{H \cup h}(\hat{0},y)|$ è un invariante di Tutte-Grothendieck. Sommando le identità (**) per ogni $y \in L_{H \cup h}$ si ottiene la ricursione voluta.

Osserviamo ancora che, se l'insieme H è costituito da un solo elemento, cioè L_H è la catena di due elementi, si ha

$$V(H) = 2 = c(H) \quad .$$

Ora, poiché le funzioni V(H) e c(H) soddisfano la medesima ricursione sulla classe ereditaria dei semireticoli associati ad insiemi di iperpiani, ed assumono lo stesso valore sulle catene con due elementi, si ha

$$c(H) = V(H)$$

per ogni insieme di iperpiani H . ■

9.2. COROLLARIO Sia H una famiglia centrale; allora

$$c(H) = (-1)^{r(L_H)} P(L_H; -1) \quad . ■$$

Osserviamo che, se H è una famiglia finita di iperpiani di $\mathbb{R}^d$ tale che

$$\bigcap_{h \in H} h = \phi \quad ,$$

ma

$$h \cap k \neq \phi \quad \text{per ogni} \quad h, k \in H \quad ,$$

allora si può completare il semireticolo L_H aggiungendo un elemento massimo, ed il reticolo L'_H così ottenuto è un reticolo geometrico.

9.3. COROLLARIO Sia H una famiglia di iperpiani tale che

$$\bigcap_{h\in H} h = \phi$$

e

$$h \cap k \neq \phi \qquad \text{per ogni} \quad h, k \in H \ ;$$

allora

$$c(H) = (-1)^{r(L'_H)} P(L'_H;-1) - |\mu(\hat{0},\hat{1})|$$

dove μ si intende relativa ad L'_H . ■

9.4. TEOREMA Sia H una famiglia finita di iperpiani di $\mathbb{R}^d$. Allora

$$f_H(t) = \sum_{x,y\in L_H} \mu(x,y)(-1)^{r(x)-r(y)}\, t^{r(x)} \quad .$$

DIMOSTRAZIONE Si ottiene applicando il risultato precedente a tutti i filtri principali di L_H , e sommando su tutti i punti aventi lo stesso rango. ■

9.5. COROLLARIO Se H è una famiglia centrale, risulta

$$f_H(t) = (-1)^{r(L_H)} M(L_H;-t,-1) \quad . ■$$

Sia H una famiglia finita di iperpiani di $\mathbb{R}^d$; l'<u>invariante di Eulero</u> di $\mathbb{R}^d$ è definito come l'intero:

$$k(\mathbb{R}^d) = f_o - f_1 + f_2 - \dots \quad .$$

9.6. TEOREMA L'invariante di Eulero non dipende dalla famiglia di iperpiani H. Inoltre, $k(\mathbb{R}^d) = (-1)^d$.

DIMOSTRAZIONE Per ogni famiglia H risulta:

$$k(\mathbb{R}^d) = (-1)^d f_H(-1) =$$

$$= (-1)^d \sum_{y \in L_H} \sum_{x \in L_H} \mu(x,y)(-1)^{r(y)} =$$

$$= \mu(\hat{0},\hat{0})(-1)^d = (-1)^d \quad . \blacksquare$$

Sia H una famiglia finita di iperpiani di $\mathbb{R}^d$, e sia K un compatto di $\mathbb{R}^d$ con interno non vuoto; indichiamo con H' il sottoinsieme di H costituito dagli iperpiani che intersecano l'interno di K . H' induce allora una partizione di K ; indichiamo con f'_j il numero delle facce di dimensione j di tale partizione. La caratteristica di Eulero di K si definisce come l'intero

$$\chi(K) = f'_o - f'_1 + f'_2 - \dots \quad .$$

9.7. TEOREMA Per ogni compatto K di $\mathbb{R}^d$ con interno non vuoto e per ogni famiglia H di iperpiani risulta

$$\chi(K) = (-1)^d \quad .$$

DIMOSTRAZIONE Sia H' il sottoinsieme di H costituito dagli iperpiani che intersecano l'intero di K; indichiamo con S_H il semireticolo ottenuto da $L_{H'}$ eliminando gli elementi relativi a sottospazi di $\mathbb{R}^d$ che non intersecano l'interno di K. Relativamente al semireticolo S_H si possono ripetere tutti i ragionamenti fatti in precedenza per L_H; procedendo come nella dimostrazione del teorema precedente, si ha la tesi. ∎

Sia H una famiglia finita di iperpiani in $\mathbb{R}^d$, e sia L_H il semireticolo ad essa associato; in generale, L_H risulta isomorfo ai semireticoli associati ad altre famiglie di iperpiani in spazi di dimensione diversa. Fra queste famiglie, diremo rappresentazione minimale di L_H una famiglia di iperpiani di $\mathbb{R}^n$, con $n = r(L_H)$, il cui semireticolo associato sia isomorfo ad L_H.

Vogliamo ora esaminare il caso in cui alcune delle regioni relative alla famiglia H di iperpiani siano limitate; osserviamo che, in questo caso, la famiglia H non è centrale, ed è una rappresentazione minimale del semireticolo ad essa associato.

9.8. TEOREMA Sia H una famiglia di iperpiani di $\mathbb{R}^d$ che sia una rappresentazione minimale del semireticolo L_H ad essa associato; allora, il numero di regioni limitate individuate da H è dato da

$$l(H) = \left| \sum_{x \in L_H} \mu(\hat{0},x) \right| .$$

DIMOSTRAZIONE Sia h un iperpiano di $\mathbb{R}^d$, $h \notin H$; poniamo

$$F_h = \left\{ h \cap k;\ k \in H,\ \dim(h \cap k) = d-2 \right\} .$$

Con argomenti analoghi a quelli utilizzati nella dimostrazione del Teorema 9.1, si ottiene che l soddisfa la seguente ricursione:

$$l(H\cup h) = l(H) + l(F_h) \quad .$$

Dato che, se $|H| = 1$, risulta:

$$l(H) = 0 = \Big| \sum_{x\in L_H} \mu(\hat{0},x) \Big| \quad ,$$

è sufficiente provare la ricursione:

$$(*) \qquad \Big| \sum_{x\in L_{H\cup h}} \mu_{H\cup h}(\hat{0},x) \Big| = \Big| \sum_{x\in L_H} \mu_H(\hat{0},x) \Big| + \Big| \sum_{x\in L_{H\cup h}} \mu_{H\cup h}(h,x) \Big| \; .$$

Sia $x\in L_{H\cup h}$; analogamente a quanto fatto nella dimostrazione del Teorema 9.1, si dimostra che

$$\mu_{H\cup h}(\hat{0},x) = \mu_H(\hat{0},x) - \mu_{H\cup h}(h,x) \quad ;$$

di conseguenza:

$$(**) \qquad \sum_{x\in L_{H\cup h}} \mu_{H\cup h}(\hat{0},x) = \sum_{x\in L_H} \mu_H(\hat{0},x) - \sum_{x\in L_{H\cup h}} \mu_{H\cup h}(h,x) \; .$$

Indichiamo con $\hat{L}_H$ ed $\hat{L}_{H\cup h}$ i reticoli ottenuti da L_H ed $L_{H\cup h}$, rispettivamente, aggiungendo un massimo $\hat{1}$; in questi reticoli l'identità (**) diventa:

$$\mu_{H\cup h}(\hat{0},\hat{1}) = \mu_H(\hat{0},\hat{1}) - \mu_{H\cup h}(h,\hat{1}) \quad .$$

Osserviamo ora che i reticoli $\hat{L}_H^*$ ed $\hat{L}_{H\cup h}^*$, duali di $\hat{L}_H$ ed $\hat{L}_{H\cup h}$ rispettivamente, sono semimodulari; di conseguenza, grazie all'affermazione d) del Teorema 7.4, abbiamo

$$|\mu_{H\cup h}(\hat{0},\hat{1})| = |\mu_H(\hat{0},\hat{1})| + |\mu_{H\cup h}(h,\hat{1})|$$

che è equivalente alla ricursione (*). ∎

Consideriamo ora lo spazio proiettivo reale $\mathbb{P}^d$, di dimensione d. Se H è una famiglia finita di iperpiani di $\mathbb{P}^d$, possiamo considerare la partizione di $\mathbb{P}^d - H$ in parti connesse massimali, che chiameremo <u>regioni</u>, e definire i numeri $c(H)$ e $f_j(H)$ in modo analogo a quanto fatto nel caso affine. Costruendo analogamente al caso affine il semireticolo L_H, questo risulta un reticolo geometrico.

9.9. TEOREMA Sia H una famiglia finita di iperpiani di $\mathbb{P}^d$; allora

$$c(H) = \frac{1}{2}\,(-1)^{r(H)}\,P(L_H; -1)$$

e

$$f_H(t) = \frac{1}{2}\,(t^{r(H)} + (-1)^{r(H)}\,M(L_H; -t, -1)) \quad .$$

DIMOSTRAZIONE Ricordando la corrispondenza tra sottospazi proiettivi di $\mathbb{P}^d$ e sottospazi vettoriali di $\mathbb{R}^{d+1}$, abbiamo che la famiglia H corrisponde ad una famiglia H_1 di iperpiani per l'origine in $\mathbb{R}^{d+1}$, e risulta ovviamente

$$L_H \cong L_{H_1} \quad .$$

Ogni regione di $\mathbb{P}^d - H$ corrisponde a due regioni relative ad H_1 in $\mathbb{R}^{d+1}$, simmetriche rispetto all'origine; così si ottiene la prima identità.

La seconda affermazione si dimostra procedendo in modo analogo, ricordando però che la faccia $\bigcap_{h\in H} h$ in $\mathbb{P}^d$ corrisponde solo alla faccia $\bigcap_{h\in H_1}$ in $\mathbb{R}^{d+1}$. ■

Sia H una famiglia finita di iperpiani dello spazio affine $\mathbb{R}^d$. Consideriamo il completamento proiettivo $\mathbb{P}^d$ di $\mathbb{R}^d$ ottenuto aggiungendo l'iperpiano all'infinito, h_∞; sia L_H^∞ la restrizione del reticolo duale di quello dei sottospazi di $\mathbb{P}^d$ all'insieme di atomi $H \cup h_\infty$. L_H^∞ è un reticolo geometrico e contiene come sottosemireticolo L_H.

La famiglia $H_\infty = H \cup h_\infty$ di iperpiani di $\mathbb{P}^d$ si dirà <u>completamento proiettivo</u> di H.

Le regioni relative ad H_∞ in $\mathbb{P}^d$ sono nello stesso numero di quelle relative ad H in $\mathbb{R}^d$. Risulta inoltre

$$r(H) = r(H_\infty) - 1 \quad .$$

9.10. TEOREMA Sia H una famiglia finita di iperpiani in $\mathbb{R}^d$, che sia una rappresentazione minimale del semireticolo associato L_H; detto L_H^∞ il reticolo del completamento proiettivo di H, risulta

$$l(H) = \beta(L_H^\infty)$$

dove β è l'invariante di Crapo.

DIMOSTRAZIONE Indicando con μ_∞ la funzione di Möbius del reticolo L_H^∞, per il Corollario 7.9, si ha:

$$\beta(L_H^\infty) = (-1)^{r(H)} \sum_{\substack{x\in L_H^\infty \\ x \not\geq h_\infty}} \mu_\infty(\hat{0},x) \quad .$$

Grazie al Teorema 9.8, è dunque sufficiente provare che

$$\sum_{x\in L_H} \mu(\hat{0},x) = \sum_{\substack{x\in L_H^\infty \\ x \not\geq h_\infty}} \mu_\infty(\hat{0},x) \quad ;$$

questo segue immediatamente dal fatto che, nell'intervallo $[\hat{0},x]$ del reticolo L_H^∞, con $x \not\geq h_\infty$, non ci sono elementi maggiori di h_∞, quindi gli intervalli $[\hat{0},x]$ in L_H^∞ e $[\hat{0},x]$ in L_H sono isomorfi.∎

9.11. PROPOSIZIONE Sia H una famiglia centrale di $\mathbb{R}^d$, e sia $h\notin H$ un iperpiano parallelo ad uno degli iperpiani in H. Allora

$$l(H\cup h) = \beta(L_H) \quad .$$

DIMOSTRAZIONE E' sufficiente osservare che le regioni limitate relative alla famiglia $H\cup h$ corrispondono biunivocamente alle regioni limitate indotte su h dagli iperpiani

$$\{h\cap k;\ k\in H,\ \dim(h\cap k) = d-2\}$$

di $\mathbb{R}^{d-1}$. Quindi,

$$l(H\cup h) = l([h,\hat{1}]_{\infty}) \qquad ,$$

dove $[h,\hat{1}]_{\infty}$ è l'intervallo superiore con minimo h nel reticolo $L^{\infty}_{H\cup h}$. Ora, si verifica facilmente che la funzione

$$\varphi : L_H \longrightarrow [h,\hat{1}]_{\infty}$$

$$\varphi : x \longrightarrow x \vee h$$

(dove il sup è inteso in $L^{\infty}_{H\cup h}$) è un isomorfismo di reticoli; da qui si ha la tesi. ∎

Vogliamo ora mostrare come i problemi affrontati a proposito delle partizioni di uno spazio affine (o proiettivo) mediante famiglie di iperpiani permettano di provare in modo assai semplice alcuni significativi risultati relativi alle orientazioni acicliche di un grafo.

Sia G un grafo non orientato privo di lati paralleli e di loops; un'*orientazione aciclica* di G è un'orientazione dei lati di G tale che il grafo orientato così ottenuto non contenga circuiti orientati.

Dato un grafo non orientato G con vertici $p_1, p_2, \dots, p_d$, associamo ad esso la famiglia H(G) di iperpiani dello spazio affine $\mathbb{R}^d$ così definita: indicato con h_{ij} l'iperpiano di $\mathbb{R}^d$ di equazione $x_i = x_j$, $h_{ij} \in H(G)$ se e solo se p_i, p_j sono vertici adiacenti in G . Essendo H(G) una famiglia centrale, $L_{H(G)}$ risulta un reticolo. Inoltre, è facile verificare che i circuiti del grafo G corrispondono biunivocamente ai circuiti del reticolo $L_{H(G)}$. Di conseguenza, indicato con $\chi_G(\lambda)$ il polinomio cromatico del grafo G e con c il numero delle componenti connesse di G , applicando la ricursione di Tutte-Grothendieck si dimostra facilmente l'identità:

$$\chi_G(\lambda) = \lambda^c \, P(L_{H(G)}; \lambda) \quad .$$

Osserviamo ora che sussiste una corrispondenza biunivoca tra le regioni relative alla famiglia $H(G)$ e le orientazioni acicliche del grafo G. Infatti, fissata una regione di $H(G)$, per ogni lato $\{p_i, p_j\}$ di G, tutti i punti della regione soddisfano una (ed una sola) delle disuguaglianze:

$$x_i < x_j \quad , \qquad x_i > x_j \quad ;$$

orientiamo allora il lato $\{p_i, p_j\}$ scegliendo come sorgente p_i se è soddisfatta la disuguaglianza $x_i < x_j$. E' facile verificare che l'orientazione così ottenuta è aciclica.

Da queste considerazioni segue:

9.12. TEOREMA Il numero delle orientazioni acicliche del grafo G è dato da

$$|\chi_G(-1)| = \sum_{x \in L} |\mu(\hat{0},x)| \quad ,$$

dove L è il reticolo geometrico associato al grafo G.∎

9.13. TEOREMA Fissato un lato $\{p_i, p_j\}$ del grafo G, il numero delle orientazioni acicliche di G aventi come unica sorgente p_i e unico pozzo p_j è dato da

$$|\beta(G)| = |\sum_{x \in L} \mu(\hat{0},x)\, c(x)| \quad ,$$

dove L è il reticolo geometrico associato al grafo G, e $c(x)$ è il numero delle componenti connesse del grafo associato al punto x di L.

DIMOSTRAZIONE Sia d il numero dei vertici del grafo G, e sia h l'iperpiano avente equazione $x_j = x_i + 1$. Ogni regione di $H(G)$ che interseca h dà luogo ad un'orientazione di G in cui il lato $\{p_i, p_j\}$ è orientato da p_i a p_j. Inoltre, con considerazioni elementari si dimostra che, tra queste regioni, quelle che danno luogo ad orientazioni del tipo voluto sono tutte e sole quelle che corrispondono a regioni limitate in una rappresentazione minimale del reticolo $L_{H\cup h}$. Da qui segue la tesi. ■

Con metodi analoghi si dimostra infine il seguente risultato:

9.14. TEOREMA Sia p_i un vertice del grafo G. Il numero delle orientazioni acicliche di G per cui p_i risulta l'unica sorgente è dato da

$$\left| \frac{d}{d\lambda} \chi_G(0) \right| = \begin{cases} |\mu(\hat{0}, \hat{1})| & \text{se } G \text{ è connesso} \\ 0 & \text{altrimenti,} \end{cases}$$

dove μ è la funzione di Möbius del reticolo geometrico associato al grafo G. ■

Bibliografia

1. G. ANDREWS, Partition identities, Advances in Math. 9 (1972), 10-51.

2. K. BACLAWSKI, Automorphisms and derivations of incidence algebras, Proc. Amer. Math. Soc. 36 (1972), 351-356.

3. K. BACLAWSKI, Whitney numbers of geometric lattices, Advances in Math. 16 (1975), 125-138.

4. K. BACLAWSKI, "Homology and Combinatorics of Partially Ordered Sets", Ph.D. Thesis, Harvard Univ., 1976.

5. K. BACLAWSKI, Galois connections and the Leray spectral sequence, Advances in Math. 25 (1977), 191-215.

6. K. BACLAWSKI, The Möbius algebra as a Grothendieck ring, J. of Algebra 57 (1979), 167-179.

7. K. BACLAWSKI, Cohen-Macaulay ordered sets, J. of Algebra 63 (1980), 226-258.

8. K. BACLAWSKI e A. BJÖRNER, Fixed point in partially ordered sets, Advances in Math. 31 (1979), 263-287.

9. M. BARNABEI, A. BRINI e G.-C. ROTA, "Sistemi di coefficienti sezionali", Centro di Analisi Globale, CNR, Firenze, 1979.

10. M. BARNABEI, A. BRINI e G.-C. ROTA, Section coefficients and section sequences, Rendic. Accad. Naz. Lincei, serie VIII, vol. LXVIII (1980), 5-12.

11. M. BARNABEI e A. BRINI, Some properties of characteristic polynomials and applications to T-lattices, Discrete Math. 31 (1980), 261-270.

12. R. BELDING, Structures characterizing partially ordered sets and their automorphism groups, Discrete Math. 27 (1979), 117-131.

13. E. BENDER e J. GOLDMAN, On the application of Möbius inversion in combinatorial analysis, Amer. Math. Monthly 82 (1975), 789-803.

14. G.D. BIRKHOFF, A determinantal formula for the number of ways of colouring a map, Annals of Math. 14 (1912), 42-46.

15. G.D. BIRKHOFF e D.C. LEWIS, Chromatic polynomials, Trans. Amer. Math. Soc. 60 (1946), 355-451.

16. G. BIRKHOFF, "Lattice Theory", 3rd ed., Amer. Math. Soc. Colloq. Publ., vol. 25, Amer. Math. Soc., Providence, R.I., 1967.

17. A. BJÖRNER, Some matroid inequalities, Discrete Math. 31 (1980), 101-103.

18. A. BJÖRNER, Homotopy type of posets and lattice complementation, preprint.

19. A. BJÖRNER, Shellable and Cohen-Macaulay partially ordered sets, preprint.

20. A. BJÖRNER e A. GARSIA, On posets with alternating Möbius

function, preprint.

21. A. BRINI, A class of rank-invariants for perfect matroid designs, Europ. J. Comb. 1 (1980), 33-38.

22. T. BRYLAWSKI, A combinatorial model for series-parallel networks, Trans. Amer. Math. Soc. 154 (1971), 1-22.

23. T. BRYLAWSKI, A decomposition for combinatorial geometries, Trans. Amer. Math. Soc. 171 (1972), 235-282.

24. T. BRYLAWSKI, The Möbius function on geometric lattices as a decomposition invariant, Proc. Conference on Möbius Algebras, Univ. of Waterloo, 1971, pp. 143-148.

25. T. BRYLAWSKI, Modular constructions for combinatorial geometries,Trans. Amer. Math. Soc. 203 (1975), 1-44.

26. T. BRYLAWSKI, The broken-circuit complex, Trans. Amer. Math. Soc. (1977), 417-433.

27. T. BRYLAWSKI, Connected matroids with the smallest Whitney numbers, Discrete Math. 18 (1977), 243-252.

28. T. BRYLAWSKI, Intersection theory for embeddings of matroids into uniform geometries, Studies in Appl. Math. 61 (1979), 211-244.

29. T. BRYLAWSKI e J. OXLEY, Several identities for the characteristic polynomial of a combinatorial geometry, Discrete Math. 31 (1980), 161-170.

30. T. BRYLAWSKI e J. OXLEY, The broken-circuit complex: its structure and factorizations, preprint.

31. L. CARLITZ, Specialized Möbius inversion, *J. Comb. Th.* (A) 24 (1978), 261-277.

32. P. CARTIER e D. FOATA, "Problèmes combinatoires de commutation et rearrangement", Lectures Notes in Math. 85, Springer-Verlag, 1969.

33. M. CERASOLI, La funzione di Möbius-Rota come metodo di enumerazione, in "Rassegna di Matematica", Tilgher, Genova, 1981.

34. M. CONTENT, F. LEMAY e P. LEROUX, Catégories de Möbius et fonctorialités: un cadre général pour l'inversion de Möbius, *J. Comb. Th.* (A) 28 (1980), 169-190.

35. H. CRAPO, The Möbius function of a lattice, *J. Comb. Th.* 1 (1966), 126-131.

36. H. CRAPO, A higher invariant for matroids, *J. Comb. Th.* 2 (1967), 406-417.

37. H. CRAPO, Möbius inversion in lattices, *Archiv Math.* 19 (1968), 595-607.

38. H. CRAPO, The Tutte polynomial, *Aequationes Math.* 3 (1969), 211-229.

39. H. CRAPO e G.-C. ROTA, "On the Foundations of Combinatorial Theory II: Combinatorial Geometries", M.I.T. Press, Cam-

bridge, Mass., 1970.

40. H. CRAPO e G.-C. ROTA, Geometric lattices, in "Trends in Lattice Theory" (H. Abbot, ed.), 1971, 127-165.

41. P. CRAWLEY e R. DILWORTH, "Algebraic Theory of Lattices", Englewood Cliffs: Prentice Hall Inc., 1973.

42. R. DAVIS, Order algebras, Bull. Amer. Math. Soc. 76 (1970), 83-87.

43. R. DAVIS, Algebras defined by patterns of zeroes, J. Comb. Th. 9 (1970), 257-260.

44. R. DEHEUVELS, Homologie des ensembles ordonnés et des espaces topologiques, Bull. Soc. Math. France 90 (1962), 261-321.

45. S. DELSARTE, Fonctions de Möbius sur le groupes abéliens finis, Annals of Math. 49 (1948), 600-609.

46. R. DILWORTH, Arithmetic theory of Birkhoff lattices, Duke Math. J. 8 (1941), 286-299.

47. R. DILWORTH, Ideals in Birkhoff lattices, Trans. Amer. Math. Soc. 49 (1941), 325-353.

48. R. DILWORTH, Dependence relations in a semimodular lattice, Duke Math. J. 11 (1944), 575-587.

49. R. DILWORTH, The structure of relatively complemented lattices, Annals of Math. 51 (1950), 348-359.

50. R. DILWORTH, A decomposition theorem for partially ordered sets, Annals of Math. 51 (1950), 161-166.

51. R. DILWORTH, Proof of a conjecture on finite modular lattices, Annals of Math. 60 (1954), 359-364.

52. R. DILWORTH, Some combinatorial problems on partially ordered sets, in "Proc. Symposia Applied Maths. (Combinatorial Analysis)", Providence, 1960, 85-90.

53. P. DOUBILET, On the foundations of Combinatorial Theory VII: Symmetric Functions through the Theory of Distribution and Occupancy, Studies in Appl. Math. 51 (1972), 377-396.

54. P. DOUBILET, G.-C. ROTA e R. STANLEY, On the foundations of Combinatorial Theory VI: The idea of generating functions, in "Sixth Berkeley Symposium on Mathematical Statistics and Probability", vol. II, Berkeley Univ. Press, 1972, 267-318.

55. C. DOWKER, Homology groups of relations, Annals of Math. 56 (1952), 84-95.

56. T. DOWLING, Codes, packings and the critical problem, in "Atti Convegno di Geometria Combinatoria e sue Applicazioni", Perugia, 1971, 210-224.

57. T. DOWLING, A q-analog of the partition lattice, in "A Survey of Combinatorial Theory" (J. Shrivastava, ed.), North-Holland, 1973, 101-115.

58. T. DOWLING, A class of geometric lattices based on finite groups, J. Comb. Th. (B) 13 (1973), 61-86.

59. T. DOWLING e R. WILSON, The slimmest geometric lattices, Trans. Amer. Math. Soc. 196 (1974), 203-215.

60. T. DOWLING e R. WILSON, Whitney number inequalities for geometric lattices, Proc. Amer. Math. Soc. 47 (1975), 504-512.

61. J. ESSAM, Graph theory and Statistical Physics, Discrete Math. 1 (1971), 83-112.

62. F. FARMER, Cellular homology for posets, preprint.

63. J. FOLKMAN, The homology groups of a lattice, J. Math. Mech. 15 (1966), 631-636.

64. R. FRUCHT e G.-C. ROTA, La funcion de Möbius para particiones de un conjunto, Scientia 122 (1963), 111-115.

65. L. GEISSINGER, Valuations of distributive lattices I, II, III, Archiv Math. 24 (1973), 230-239, 337-345, 475-481.

66. L. GEISSINGER e W. GRAVES, The category of complete algebraic lattices, J. Comb. Th. (A) 13 (1972), 332-338.

67. J. GOLDMAN, J. JOICHI e D. WHITE, Rook Theory V: Rook Polynomials, Möbius Inversion and The Umbral Calculus, J. Comb. Th. (A) 21 (1976), 230-239.

68. J. GOLDMAN e G.-C. ROTA, On the foundations of Combinatorial Theory IV: Finite vector spaces and Eulerian generating functions, Studies in Appl. Math. 49 (1970), 239-258.

69. B. GORDON e L. HOUTON, Note on plane partitions I, II, J. Comb. Th. 4 (1968) 72-80, 81-99.

70. W. GRAVES, An algebra associated to a combinatorial geometry, Bull. Amer. Math. Soc. 77 (1971), 757-761.

71. W. GRAVES e S. MOLNAR, Incidence algebras as algebras of endomorphisms, Bull. Amer. Math. Soc. 79 (1973), 815-820.

72. M. GREENE e R. NETTLETON, Expression in terms of modular distribution functions for the entropy density in an infinite system, J. Chemical Physics 29 (1958), 1365-1370.

73. M. GREENE e R. NETTLETON, Möbius function of the lattice of dense graphs, J. Res. Nat. Bur. Standards 64 B (1962), 41-47.

74. C. GREENE, A rank inequality for finite geometric lattices, J. Comb. Th. 9 (1970), 357-364.

75. C. GREENE, On the Möbius algebra of a partially ordered set, Advances in Math. 10 (1973), 177-187.

76. C. GREENE, An inequality for the Möbius function of a geometric lattice, Studies in Appl. Math. 54 (1975), 71-74.

77. H. GRIFFITHS, The homology of some ordered systems, Acta Math. 129 (1972), 195-235.

78. H. HADWIGER, Gruppierung mit Nebenbedingungen, Mitt. Verein Schweizer Vers. Math. 43 (1943), 113-222.

79. H. HADWIGER, Über eine Klassifikation der Streckenkomplexe,

Viertelj. Schr. Naturforsch. Ges. Zürich 88 (1943), 133-142.

80. H. HADWIGER, Über additive Funktionale K-dimensionaler Eipolyeder, Publ. Math. Debrecen 3 (1953), 87-94.

81. H. HADWIGER, Eulers Charakteristik und combinatorische Geometrie, J. reine angew. Math. 194 (1955), 101-110.

82. H. HADWIGER, Zur eulerschen Charakteristik euklidischer Polyeder, Monatsch. für Math. 64 (1960), 349-354.

83. P. HALL, A contribution to the theory of groups of prime power order, Proc. London Math. Soc. 36 (1932), 101-110.

84. P. HALL, The Eulerian function of a group, Quart. J. Math. (Oxford) 7 (1936), 134-151.

85. G. HANSEL, Problèmes de dénombrément et d'évaluation de bornes concérnant les éléments du treillis distributif libre, Publ. Inst. Stat. Paris 16 (1967), 163-294.

86. L. HARPER e G.-C. ROTA, Matching Theory: an introduction, Advances in Probability 1 (1971), 169-213.

87. S. HOGGAR, Chromatic polynomials and logarithmic concavity, J. Comb. Th. (B) 16 (1974), 248-255.

88. A. HORN e A. TARSKI, Measures in Boolean algebras, Trans. Amer. Math. Soc. 64 (1948), 467-497.

89. V. KLEE, The Euler characteristic in combinatorial geometries, Amer. Math. Monthly 70 (1963), 119-127.

90. H. LAKSER, The homology of a lattice, Discrete Math. 1 (1971), 187-191.

91. P. LEROUX, Les catégories de Möbius, Cahiers de topologie et géométrie différentielle 16 (1975), 280-282.

92. B. LINDSTRÖM, On the realization of convex polytopes, Euler's formula and Möbius functions, Aequationes Math. 6 (1971), 235-240.

93. H. MACNEILLE, Partially ordered sets, Trans. Amer. Math. Soc. 42 (1937), 416-460.

94. J. MASON, Maximal families of pairwise disjoint proper chains in a geometric lattice, J. London Math. Soc. 6 (1973), 539-542.

95. A. MÖBIUS, Über eine besondere Art von Umkehrung der Reihen, J. reine angew. Math. 9 (1832), 105-123.

96. P. ORLIK e L. SOLOMON, Combinatorics and topology of complements of hyperplanes, Inventiones Math. 56 (1980), 167-189.

97. P. ORLIK e L. SOLOMON, Unitary reflection groups and cohomology, Inventiones Math. 59 (1980), 77-94.

98. J. OXLEY, Colouring, packing and the critical problem, Quart. J. Math. (Oxford) 29 (1978), 11-22.

99. B. PETTIS, Remarks on the extension of lattice functionals, Bull. Amer. Math. Soc. 54 (1948), 471-472.

100. B. PETTIS, On the extension of measures, Annals of Math. 54 (1951), 186-197.

101. R. RADO, A theorem on general measure functions, Proc. London Math. Soc. 44 (1938), 61-91.

102. R. RADO, Theorems on linear combinatorial topology and general measure, Annals of Math. 44 (1943), 228-276.

103. R. RADO, A combinatorial theorem on vector spaces, J. London Math. Soc. 37 (1962), 351-353.

104. R. RADO, Abstract linear dependence, Colloq. Math. 14 (1966), 258-264.

105. R. READ, An introduction to chromatic polynomials. J. Comb. Th. 4 (1968), 52-71.

106. G.-C. ROTA, On the foundations of Combinatorial Theory I: Theory of Möbius functions. Z. Warsch. 2 (1964), 340-368.

107. G.-C. ROTA, On the combinatorics of Euler characteristic, in "Studies in Pure Mathematics" (L. Mirsky, ed.), London, Acad. Press, 1971, pp. 221-233.

108. G.-C. ROTA e B. SAGAN, Congruences derived from group action, Europ. J. Comb. 1 (1980), 67-76.

109. G.-C. ROTA e D. SMITH, Enumeration under group action, Ann. Sc. Norm. Pisa, Classe di Scienze 4 (1977), 637-646.

110. H. SCHEID, Einige Ringe zahlentheoretischer Funktionen,

J. reine angew. Math. 237 (1969), 1-11.

111. H. SCHEID, Über ordnungtheoretische Funktionen, J. reine angew. Math. 238 (1969), 1-13.

112. H. SCHEID, Über die Möbiusfunktion einer local endlichen Halbordnung, J. Comb. Th. 13 (1972), 315-331.

113. M. SCHÜTZENBERGER, Contribution aux application statistiques de la théorie de l'information, Publ. Inst. Stat. Univ. Paris 3 (1954), 5-117.

114. D. SMITH, Incidence functions as generalized arithmetic functions I, II, III, Duke Math. J. 34 (1967), 617-634; 36 (1969), 15-30, 343-368.

115. D. SMITH, Multiplication operators on incidence algebras, Indiana Univ. Math. J. 20 (1970/71), 369-383.

116. L. SOLOMON, The Burnside algebra of a finite group, J. Comb. Th. 2 (1967), 607-615.

117. R. STANLEY, Structure of incidence algebras and their automorphism groups, Bull. Amer. Math. Soc. 76 (1970), 1236-1239.

118. R. STANLEY, Modular elements in geometric lattices, Algebra Universalis 1 (1971), 214-217.

119. R. STANLEY, Supersolvable lattices, Algebra Universalis 2 (1972), 197-217.

120. R. STANLEY, Ordered structures and partitions, Memoirs Amer. Math. Soc. 119 (1972).

121. R. STANLEY, Acyclic orientations of graphs, Discrete Math. 5 (1973), 171-178.

122. R. STANLEY, Finite lattices and Jordan-Hölder sets, Algebra Universalis 4 (1974), 361-371.

123. R. STANLEY, Combinatorial reciprocity theorems, Advances in Math. 14 (1974), 194-253.

124. R. STANLEY, The Fibónacci lattice, Fibonacci Quart. 13 (1975), 215-232.

125. R. STANLEY, Binomial posets, Möbius inversion and permutation enumeration, J. Comb. Th. (A) 20 (1976), 336-356.

126. R. STANLEY, Balanced Cohen-Macaulay complexes, Trans.Amer. Math. Soc. 249 (1979), 139-157.

127. M. STONE, Topological representations of distributive lattices and Brouwerian logics, Casopis Math. Fys. 67 (1937), 1-25.

128. W. TUTTE, A ring in graph theory, Proc. Cambridge Phil. Soc. 43 (1947), 26-40.

129. W. TUTTE, A contribution to the theory of chromatic polynomials, Can. J. Math. 6 (1954), 80-91.

130. W. TUTTE, A class of Abelian groups, Can. J. Math. 8 (1956),

13-28.

131. W. TUTTE, On dichromatic polynomials, J. Comb. Th. 2 (1967), 301-313.

132. M. WARD, Arithmetic functions on rings, Annals of Math. 38 (1937), 725-732.

133. M. WARD, The algebra of lattice functions, Duke Math. J. 5 (1939), 357-371.

134. L. WEISNER, Some properties of prime-power groups, Trans. Amer. Math. Soc. 38 (1935), 485-492.

135. L. WEISNER, Abstract theory of inversion of finite series, Trans. Amer. Math. Soc. 38 (1935), 474-484.

136. H. WILF, Hadamard determinants, Möbius functions and the chromatic number of a graph, Bull. Amer. Math. Soc. 74 (1968), 960-964.

137. H. WILF, A mechanical counting method and combinatorial applications, J. Comb. Th. 4 (1968), 246-258.

138. T. ZASLAVSKY, Counting faces of cut-up spaces, Bull. Amer. Math. Soc. 81 (1975), 916-918.

139. T. ZASLAVSKY, Facing up to arrangements: face count formulas for partitions of space by hyperplanes, Memoirs Amer. Math. Soc. 154 (1975).

140. T. ZASLAVSKY, Maximal dissections of a simplex, J. Comb.

Th. (A) 20 (1976), 244-257.

141. T. ZASLAVSKY, A combinatorial analysis of topological dissections, Advances in Math. 25 (1977), 267-289.

142. T. ZASLAVSKY, Arrangements of hyperplanes: matroids and graphs, in "Proc. Tenth Southeastern Conf. on Combinatorics, Graph Theory and Computing", Boca Raton, 1979.

143. T. ZASLAVSKY, Signed graph colorings, preprint.

CENTRO INTERNAZIONALE MATEMATICO ESTIVO

(C.I.M.E.)

SOME REMARKS ON THE CRITICAL PROBLEM

ANDREA BRINI

SOME REMARKS ON THE CRITICAL PROBLEM

Andrea Brini
(Università di Bologna)

Introduction

In 1970, Crapo and Rota proposed a reformulation of a classical extremal problem on finite vector spaces, namely, the problem of finding the largest dimension of a subspace having empty intersection with a given set of vectors S. Besides achieving an higher degree of generality, their most pleasing result was that of showing this problem to be equivalent to a problem concerning the location of zeroes of the characteristic polynomial associated to the matroid structure induced on the set S.

Recently, Kung, Murty and Rota succeeded in proving that an analogous problem on finite abelian groups admits a solution in terms of the location of zeroes of another function, the so-called Rèdei zeta function of a set of points in a Dirichlet lattice.

In this paper, we deal with an unified exposition of some extremal problems which can be solved in this way. In section 1,we describe the critical problem for finite abelian groups and its connection with a class of Rèdei zeta functions. In section 2,we recall Crapo and Rota's Theorem relating to the critical problem for finite vector spaces, here seen as a simple consequence of the preceding result on groups. Section 3 summarizes specializations to graph colourings. In section 4, we recall connections with the (linear) coding problem; in particular, we show that some classical results on bounds can be easily derived from purely matroid theoretic facts about Hamming spheres.

1.A *lattice of Dirichlet type* is a pair (L,ν), where

i) L is a lattice with $\hat{0}$ element

ii) $\nu: L\times L \longrightarrow \mathbf{Z}$ satisfies the identities

$$\nu(x,y) = 0 \quad \text{if} \quad x\nleq y$$

and

$$\nu(x,y) = \nu(x,z)\nu(z,y)>0 \quad \text{for every} \quad x\leq z\leq y.$$

Given a set E of elements in L, let $M(E)$ be the lattice spanned by E; the set E is called a *Rédei set* if, for every element x in $M(E)$ and every positive integer n, the number of elements y in $M(E)$ such that $\nu(x,y) = n$ is finite. In particular, every finite set is a Rédei set.

Given a Rédei set E of elements in L and an element $a\in L$, the *Rédei zeta function of E based on a* is defined as

$$\rho(s;a,E) = \sum_{A\subset E} (-1)^{|A|}\nu(a,\bar{A})^{-s},$$

where $\bar{A}$ denotes the supremum in L of the elements belonging to the finite subset A.

The following result exhibits the connection between the Rédei zeta function of a set E and the Möbius function of the lattice $M(E)$ spanned by E.

(1.1) Proposition: Let $M(E)$ be the lattice spanned by E, μ its Möbius function; then

$$\rho(s;\hat{0},E) = \sum_{x\in M(E)} \mu(\hat{0},x)\nu(\hat{0},x)^{-s}.$$

Proof. It is easily seen that we can delete elements from E until it is an antichain, without changing its Rédei zeta function: then, we can suppose that E is an antichain. Now, given $x\in M(E)$, let us consider the interval $[\hat{0},x]$ in $M(E)$; the set $E\cap[\hat{0},x]$ is a cross-cut of $[\hat{0},x]$ and, by the Cross-cut Theorem [16], we get

$$\begin{aligned}\rho(s;\hat{0},E) &= \sum_{A\subset E} (-1)^{|A|}\nu(\hat{0},\bar{A})^{-s} = \\ &= \sum_{x\in M(E)} \Big(\sum_{\bar{A}=x} (-1)^{|A|}\Big)\nu(\hat{0},x)^{-s} = \\ &= \sum_{x\in M(E)} \mu(\hat{0},x)\nu(\hat{0},x)^{-s}.\end{aligned}$$

Let G be a finite abelian group and $L(G)$ be the modular lattice of its subgroups; by setting $\nu(A,B) = |B|/|A|$ for every pair $A,B,A\subset B$ of subgroups of G, the lattice $L(G)$ turns out to be a lattice of Dirichlet type.

Let $\underline{A} = \{A_1, \ . \ ,A_n\}$ be a collection of subgroups of G; we say that a k-tuple $\underline{\chi} = (\chi_1, \ . \ ,\chi_k)$ of characters of G *distinguishes* $\underline{A}$ if, for every A_j, there exists at least a character χ_i in $\underline{\chi}$ such that χ_i is not trivial on A_j. The *critical problem* is to find the smallest k for which such a k-tuple exists.

(1.2) Theorem: Let $\underline{A} = \{A_1, \ . \ ,A_n\}$be a collection of subgroups of a finite abelian group G. The number of ordered k-tuples $\underline{\chi} = (\chi_1, \ . \ ,\chi_k)$ of characters of G distinguishing $\underline{A}$ is given by the evaluation

$$|G|^k \rho(k;\hat{0},\underline{A}) \ .$$

Proof. First of all, we recall that a character of G can be seen as an homomorphism of G into the complex unit circle (see e.g.[13]). Given the set $\underline{A} = \{A_1, \ . \ ,A_n\}$and a k-tuple $\underline{\chi} = (\chi_1, \ . \ ,\chi_k)$ of characters, we define the "kernel of $\underline{\chi}$ relative to $\underline{A}$" as the largest subgroup B in $M(\underline{A})$ - the lattice spanned by $\underline{A}$ - such that χ_i is trivial on B for every i; thus, B is the subgroup of G generated by the subcollection of all subgroups A_j such that χ_i is trivial on A_j for every i.

The proof is now by Möbius inversion over $M(\underline{A})$. Let us define two functions

$$f,g : M(\underline{A}) \longrightarrow \mathbf{Z}$$

in the following way:

f(C) = number of k-tuples of characters of G whose kernel relative to $\underline{A}$ is exactly C.

g(B) = number of k-tuples of characters of G whose kernel relative to $\underline{A}$ contains B.

Thus, we have

$$g(B) = \sum_{C \geq B} f(C)$$

for every $B \in M(\underline{A})$.

We recall now that a finite abelian group G can be splitted into a direct sum

$$C_1 \oplus C_2 \oplus \cdots \oplus C_r$$

of cyclic groups of prime power order p^{e_i}; hence, a character of G is known whenever its value on a generator of C_i is given, for every i = 1, . ,r. Since its value must be an p^{e_i}-th root of the unity in the complex field, we infer that the number of characters of a finite abelian group equals its order.

Thus, we have

$$g(B) = (|G|/|B|)^k$$

and, by Möbius inversion,

$$f(B) = \sum_{C \geq B} \mu(B,C)(|G|/|C|)^k$$

for every B in $M(\underline{A})$. By setting $B = \hat{0}$ and recalling Proposition (1.1), we get the assertion.

By Theorem (1.2), the critical problem is solved whenever zeroes of the Rēdei zeta function $\rho(s;\hat{0},\underline{A})$ of the set $\underline{A}$ are known.

2.As an instance of the preceding result, it is possible to exhibit a simple proof of the well-known result by Crapo and Rota [8] concerning the *critical problem* for finite vector spaces. This problem can be stated as follows: given a set $S = \{v_1, \ . \ ,v_n\}$ of vectors in the finite vector space V of dimension n over the Galois field GF(q), we say that a k-tuple of linear functionals $\underline{F} = (F_1, \ . \ ,F_k)$ *distinguishes* S if

$$\ker F_1 \cap \ker F_2 \cap \ . \ . \ \cap \ker F_k \cap S = \phi;$$

the critical problem is to find the smallest positive integer k such that there exists a k-tuple of linear functionals distinguishing the set S. This integer is called the *critical exponent of S* and will be denoted by c(S;q).

As stated in the introduction, the critical problem is equivalent to that of finding the largest dimension of a subspace having empty intersection with a given set of vectors. More precisely, we have

(2.1) Proposition: Let S be a set of vectors in the vector space V. The largest dimension k of a subspace U of V such that $U \cap S = \phi$ is given by

$$k = n - c(S;q).$$

We come now to the main result of this section:

(2.2) Theorem: Let S be a set of vectors in V, $M(S)$ be the matroid induced on S by restriction of V. Then, the number of ordered k-tuples of linear functionals which distinguish S equals

$$q^{k(n-r(M))}P(M(S);q^k),$$

where $P(M(S);\lambda)$ is the characteristic polynomial of the matroid $M(S)$ and $r(M)$ denotes its rank.

Proof. We can regard V as the direct sum group $G = G_1 \oplus G_2 \oplus \cdots \oplus G_{rn}$,where the G_i's are all cyclic groups of order p, $p^r = q$; furthermore, there is an obvious identifiction between linear functionals on V and characters of G. By Theorem (1.2), we have

$$\begin{aligned}|G|^k p(k;\hat{0},S) &= q^{nk} \sum_{x\in M(S)} \mu(\hat{0},x) q^{-r(x)k} = \\ &= \sum_{x\in M(S)} \mu(\hat{0},x)(q^k)^{n-r(x)} = \\ &= q^{k(n-r(M))} P(M(S);q^k).\end{aligned}$$

Let $M(S)$ be a matroid without loops, representable over GF(q). The preceding Theorem leads us to define the *critical exponent* $C(M;q)$ *of* M as the smallest positive integer k such that $P(M(S);q^k)>0$.

Obviously, if $\psi\colon S \longrightarrow V$ is any representation of $M(S)$ in V, we get

$$c(\psi(S);q) = C(M;q).$$

Furthermore, we have

(2.3) Proposition: Let $M(S)$ be a matroid without loops, representable over GF(q). Then

i) $P(M(S);q^k) \geq 0$ for every non-negative integer k

ii) $P(M(S);q^j) > 0$ for every integer $j \geq C(M;q)$.

Several bounds for critical exponents of representable matroids have been found in recent years; just as an example, we mention a result which we need in the last part of this paper.

Let $R(M)$ denote the set of simple restrictions of M, $C(M)$ the set of cocircuits of M and $\lceil\alpha\rceil$ the smallest integer greater or equal than $\alpha\in\mathbf{R}$; we have

(2.4) Theorem: If M is representable over GF(q) and it has no loops, then

$$C(M;q) \leq \left\lceil \log_q \left(2 + \max_{N\in R(M)} \left(\min_{C\in C(N)} |C|\right)\right)\right\rceil .$$

3.A *proper k-colouring* of a graph $G = (V,E)$ is a mapping γ from the vertex set V to a set $A = \{a_1, \ldots, a_k\}$ (colours) satisfying the following condition: if u and v are adjacent vertices, then $\gamma(u) \neq \gamma(v)$.

The *colouring problem* is to find the smallest positive integer k such that a proper k-colouring of the graph G exists; this integer is called the *chromatic number of G* and is usually denoted by $\chi(G)$.

Now, let $\mathbf{K}$ be any field. Set

$$R_0(\mathbf{K}) = \{f;\ f\colon V \longrightarrow \mathbf{K}\}$$

$$R_1(\mathbf{K}) = \{g;\ g\colon E \longrightarrow \mathbf{K}\}.$$

Let us orient the edges of G in some fashion; if the edge $e = \{u,v\}$ is directed from u to v, we set $e^- = u$ and $e^+ = v$, respectively.

The *coboundary operator* is the linear operator $\delta\colon R_0(\mathbf{K}) \longrightarrow R_1(\mathbf{K})$ defined as follows:

$$(\delta g)(e) = g(e^+)-g(e^-)$$

for every $e \in E$ and $g \in R_0(\mathbf{K})$.

The image space of δ is called the *coboundary space* of the graph G and will be denoted by $C(G,\mathbf{K})$. One easily checks that

$$\ker \delta = \{f\colon V \longrightarrow \mathbf{K};\ \text{if u and v are adjacent vertices, then } f(u) = f(v)\};$$

then, denoted by k(G) the number of connected components of G, we get

$$\dim (\ker \delta\ ) = k(G)$$

and

$$\dim (C(G,\mathbf{K})) = |V| - k(G).$$

Furthermore, $C(G,\mathbf{K})$ is independent of the choice of the orientation on G.

For every $e \in E$, we define a linear functional on $C(G,\mathbf{K})$ as follows:

$$\langle L_e | f\rangle = f(e)$$

for every $f \in C(G,\mathbf{K})$.

Now, it is well-known that the cycle matroid $M(E)$ of the graph $G = (V,E)$ is represented over $\mathbf{K}$ by the application

$$\psi\colon E \longrightarrow \mathrm{Hom}(C(G,\mathbf{K}),\mathbf{K})$$

such that

$$\psi(e) = L_e$$

for every $e \in E$.

Thus, $M(E)$ is replesentable over any field $\mathbf{K}$ and we can state the following

(3.1) Theorem: Set $n = |V|$, $\mathbf{K} = GF(q)$. There is a bijection between the set of all proper q^k-colourings of the graph $G = (V,E)$ and the set of all ordered k-tuples of linear functionals on $V = \mathbf{K}^n$ which distinguish the set of vectors corresponding to E.

We give two proofs of this result.

a) Let $\chi_G(\lambda)$ be the chromatic polynomial of the graph $G = (V,E)$ and let r be the rank of its cycle matroid $M(E)$. The Tutte-Grothendieck recursion in the hereditary class of graphic matroids yields the identity

$$\chi_G(\lambda) = \lambda^{k(G)} P(M(E);\lambda) \ .$$

By Theorem (2.2), recalling that $k(G)=n-r$, we get the assertion.

b) Let $\tilde{\delta}$ be the linear operator

$$\tilde{\delta} : \mathrm{Hom}(C(G,\mathbb{K}),\mathbb{K}) \longrightarrow \mathrm{Hom}(R_0(G,\mathbb{K}),\mathbb{K})$$

defined as follows:

$$\tilde{\delta}(L) = L\circ\delta$$

for every $L\in\mathrm{Hom}(C(G,\mathbb{K}),\mathbb{K})$.

The operator $\tilde{\delta}$ is one to one and hence the application

$$e \longmapsto (L_e)$$

yields a representation of $M(E)$ in $\mathrm{Hom}(R_0(G,\mathbb{K}),\mathbb{K})$.

We choose às a colour set A ($|A|=q^k$) the set of all k-tuples on $\mathbb{K}$; hence, any given mapping $\underline{f}$: $V\longrightarrow A$ can be seen as a k-tuple of linear functionals on $\mathrm{Hom}(R_0(G,\mathbb{K}),\mathbb{K})$, by setting

$$\underline{f}(v) = (f_1(v), \ . \ ,f_k(v))$$

for every $v\in V$.

Furthermore, we have:

$\underline{f}$ is a proper q^k-colouring of $G=(V,E)$ $\Longleftrightarrow$ for every $e\in E$ there exists an i such that $\delta f_i(e) \neq 0 \Leftrightarrow$ for every $e\in E$ there exists an i such that $<L_e|\delta f_i> \neq 0$ $\Longleftrightarrow$ for every $e\in E$, $(<\tilde{\delta} L_e|f_1>, \ . \ , <\tilde{\delta} L_e|f_k>) \neq (0,0, \ . \ ,0)$.

This completes the proof.

(3.2) Corollary: Let G be a graph without loops and let $M(E)$ be its cycle matroid. Then, for every prime power q, we have

$$q^{C(M;q)-1} < \chi_G \leq q^{C(M;q)} .$$

4. Let V be the vector space of dimension n over GF(q). Given a distinguished basis $B = \{b_1, \ . \ ,b_n\}$ of V, the *weight* of a vector $v\in V$ is the number $\omega(v)$ of its non-zero coordinates with respect to B.

An $[n,k,d]$ -*linear code* is a subspace C of dimension k of V, such that

$$\omega(v)\geq d$$

for every $v\in C-\{\underline{0}\}$. The integer d is called *minimum distance* of the code C.

Given $n,d\in\mathbf{Z}^{+}$, the (linear) *coding problem* is to find the largest integer k such that an $[n,k,d]$ -linear code exists.

Set

$$S_{n,q,d-1} = \{v\in V;\ v\neq\underline{0}\ ,\ \omega(v)\leq d\}\ ;$$

we call *Hamming matroid* the matroid $M(S_{n,q,d-1})$ obtained by restriction of V on the set $S_{n,q,d-1}$.

The coding problem is a special case of the critical problem for finite vector spaces. In fact, by Proposition (2.1), we get

(4.1) Proposition: An $[n,k,d]$-linear code over GF(q) exists if and only if the inequality

$$C(M(S_{n,q,d-1});q)\leq n-k$$

holds.

Now, set

$$A = \{(j_1,\ .\ ,j_n)\in\mathbb{Z}^n;\ j_1<j_2<\quad <j_n\leq n,\ j_i \text{ is non-negative for } i=1,.,n\};$$

moreover, for every $(j_1,\ .\ ,j_n)\in A$, set

$$F_{j_1,\ .\ ,j_n} = \{v = (v_1,\ .\ ,v_n)\in V;\ v_{j_i} = 0 \text{ if } j_i \neq 0\}\ .$$

The subset

$$F_{j_1,\ .\ ,j_n}\cap S_{n,q,d-1}$$

of V is a flat of the matroid $M(S_{n,q,d-1})$ and will be called *coordinate flat.*

We have

(4.2) Proposition: If F is a coordinate flat of $M(S_{n,q,d-1})$ and $r(F)\leq d-1$, then F is a modular flat.

Proof. By induction on the rank of F. If $r(F)=1$, the assumption trivially holds. Now, assume the statement true for every coordinate flat of rank smaller than $m\leq d-1$. Let F and H be coordinate flats, $r(F)=m$, $r(H)=m-1$, $H\subset F$. Let K be any other flat of $M(S_{n,q,d-1})$. We consider two cases:

i) Suppose $K\cap H\subset K\cap F$; then

$$r(H)+r(K)+1 = r(K\cap H)+r(K\cup H)+1 \leq r(F\cap K)+r(F\cup K) \leq r(K)+r(F) = r(K)+r(H)+1.$$

Hence, (F,K) is a modular pair.

ii) Suppose $K\cap H = K\cap F$. Let b_t be the element of the distinguished basis B of V which belongs to F but not to H. Assume that b_t is spanned by the set $K \cup H$; then there exists a minimal set $\{k_i\} \cup \{h_j\}$ of elements in K and H such that

$$b_t = \sum_j \mu_j h_j + \sum_i \zeta_i k_i , \qquad \mu_j, \zeta_i \in GF(q).$$

Now, if $r(F) \leq d-1$, the vector

$$\sum_i \zeta_i k_i = b_t - \sum_j \mu_j h_j$$

is in $F \cap H$ but not in $H \cap K$, and this is a contradiction. Hence, $r(K \cup H) = r(K \cup F)+1$ and (F,K) is a modular pair.

By Proposition (4.2) and Stanley's Theorem on modular elements in geometric lattices ([17] , Theorem 2), we get

(4.3) <u>Proposition</u>: The characteristic polynomial $P(M(S_{n,q,d-1});\lambda)$ has at least d-1 positive real roots r_i, namely,

$$r_i = q^i$$

is a root for every $i = 0,1, . ,d-2$.

Proof. Let F and H be coordinate flats, $H \subset F$, $r(H) = r(F)-1 \leq d-2$. The number of 1-flats of $M(S_{n,q,d-1})$ which are contained in F but not in H is given by $q^{r(H)}$. By the Theorem mentioned above, $q^{r(H)}$ is a root of $P(M(S_{n,q,d-1});\lambda)$.

(4.4) <u>Corollary</u> (The singleton bound): If an [n,k,d] -linear code exists, the inequality

$$n-k \geq d-1$$

holds.

The special case $M(S_{n,q,2})$ has been widely studied by T.Dowling in [11] (see also [9] , pag. 290 ff.). In particular, he proved that every coordinate flat of $M(S_{n,q,2})$ is a modular flat and hence its geometric lattice is a supersolvable lattice. Thus, we have

$$P(M(S_{n,q,2});\lambda) = \prod_{i=0}^{n-1} (\lambda-(q-1)i-1)$$

and this implies

(4.5) <u>Proposition</u>: An [n,k,3] -linear code over GF(q) exists if and only if the inequality

$$1+(q-1)(n-1)<q^{n-k}$$

holds.

The preceding result is nothing but the well-known Gilbert-Varshamov bound ([13], pag.34) in the case d=3, here seen to be also a necessary condition for this class of codes.

Our next aim is to derive the general form of this bound as a specialization of the general bound on critical exponents given in Theorem (2.4).

(4.6) <u>Theorem</u>: There exists an $[n,k,d]$-linear code over GF(q), provided

$$\sum_{i=0}^{d-2} (q-1)^i \binom{n-1}{i} < q^{n-k}.$$

Proof. Let $G(S_{n,q,d-1})$ be the combinatorial geometry associated to the Hamming matroid $M(S_{n,q,d-1})$. For every coordinate hyperplane H_j (j=1, . ,n) of $M(S_{n,q,d-1})$, denote by $\overline{H}_j$ the corresponding hyperplane of $G(S_{n,q,d-1})$. It is easily seen that the cardinality of $\overline{H}_j$ is

$$|\overline{H}_j| = \sum_{i=0}^{d-1} (q-1)^{i-1}\binom{n-1}{i} + 1$$

furthermore, if $\overline{H}$ is any hyperplane of $G(S_{n,q,d-1})$, its cardinality is smaller or equal than $|\overline{H}_j|$.

Choose now a 1-flat $\overline{P} \in G(S_{n,q,d-1})$; we can always find an integer j such that $\overline{P} \not\in \overline{H}_j$. Then, we have

$$\max_{N \in R(G(S_{n,q,d-1}))} \left(\min_{C \in C(N)} |C| \right) =$$

$$= \sum_{i=1}^{d-1} (q-1)^{i-1}\binom{n}{i} - \sum_{i=1}^{d-1} (q-1)^{i-1}\binom{n-1}{i} - 1 =$$

$$= \sum_{i=0}^{d-2} (q-1)^{i}\binom{n-1}{i} - 1 .$$

Recalling that $P(G(S_{n,q,d-1});\lambda) = P(M(S_{n,q,d-1});\lambda)$, the statement follows by Theorem (2.4).

References

1. G.D.BIRKHOFF, A determinantal formula for the number of ways of colouring a planar map, *Annals of Math.* **14** (1912), 42-46.

2. G.BIRKHOFF, "Lattice Theory", 3rd ed., Providence: Amer. Math. Soc. Coll. Publ. **25** (1967).

3. R.C.BOSE, Mathematical theory of symmetrical factorial design, *Sankhya* **8** (1947), 107-166.

4. A.BRINI, Improving Gilbert-Varshamov bound for linear codes, in preparation.

5. T.H.BRYLAWSKI, Intersection theory for embedding of matroids into uniform geometries, *Studies in Appl. Math.* **61** (1979), 211-244.

6. T.H.BRYLAWSKI and D.G.KELLY, "Matroids and Combinatorial Geometries", Carolina Lectures Series, Univ. of North Carolina, 1980.

7. H.H.CRAPO, Möbius inversion in lattices, *Archiv.Math.* **19** (1968), 595-607.

8. H.H.CRAPO and G.C.ROTA, "Combinatorial Geometries", MIT Press, Cambridge, Massachussets, 1970.

9. P.DOUBILET, G.C.ROTA andR.P.STANLEY, On the foundations of combinatorial theory VI: The idea of generating function, Proc. 6th Berkeley Symp. on Math. Stat. and Prob., vol.II: Probability Theory. Univ. of California, 1972, 267-318.

10. T.A.DOWLING, Codes, packings and the critical problem, Atti del Convegno di Geometria Combinatoria e sue Applicazioni, Perugia, 1971, 210-224.

11. T.A.DOWLING, A q-analog of the partition lattice, A Survey of Combinatorial Theory (J.Srivastava, Ed.), North Holland Publ.Comp.1973, 101-115.

12. J.P.KUNG, M.R.MURTY and G.C.ROTA, On the Rédei zeta function, to appear

13. N.JACOBSON, "Basic Algebra I", W.H.Freeman and Comp., San Francisco, 1970.

14. F.J.MACWILLIAMS and N.J.A.SLOANE, "The Theory of Error-Correcting Codes", North Holland Publ. Comp., 1977.

15. J.G.OXLEY, Colouring, packing and the critical problem, *Quart.J.Math.* **29** (1978), 11-22.

16. G.C.ROTA, On the foundations of combinatorial theory I: Theory of Möbius functions, Z. *Warsch.* **2** (1964), 340-368.

17. R.P.STANLEY, Modular elements in geometric lattices, *Algebra Universalis* **1** (1971), 214-217.

18. R.P.STANLEY, Supersolvable lattices, *Algebra Universalis* **2** (1972), 197-217

19. W.T.TUTTE, On the algebraic theory of graph colourings, *J. Comb. Th.***1**, (1966), 15-50.

20. W.T.TUTTE, Projective geometry and the 4-colours problem, Recent Progress in Combinatorics (W.T.Tutte,Ed.) Academic Press, 1969, 199-207.

21. D.J.WELSH, "Matroid theory", Academic Press, 1976.

22. N.WHITE, The critical problem and coding theory, Jet Prop. Lab. SPS, vol. III, section 331, 1973, 37-66.

CENTRO INTERNAZIONALE MATEMATICO ESTIVO

(C.I.M.E.)

THE TUTTE POLYNOMIAL

PART I: GENERAL THEORY

THOMAS BRYLAWSKI

Department of Mathematics
University of North Carolina
Chapel Hill, N. C. 27514

*This work was supported by N.S.F. Grant MCS-7801149 and was presented at the Third C.I.M.E. Conference on Matroid Theory and its Applications held at Varenna, Italy, August, 1980.

1. Introduction.

Matroid theory (sometimes viewed as the theory of combinatorial geometries or geometric lattices) is reasonably young as a mathematical theory (its traditional birthday is given as 1935 with the appearance of [159]) but has steadily developed over the years and shown accelerated growth recently due, in large part, to two applications. The first is in the field of algorithms. To coin an oversimplification: "when a good algorithm is known, a matroid structure is probably hidden away somewhere." In any event, many of the standard good algorithms (such as the greedy algorithm) and many important ones whose complexities are currently being scrutinized (e.g., existence of a Hamiltonian path) can be thought of as matroid algorithms. In the accompanying lecture notes of Professor Welsh the connections between matroids and algorithms are presented.

Another important application of matroids is the theory of the Tutte polynomial

$$t(M;x,y) = \Sigma a_{ij}(x-1)^{i}(y-1)^{j}$$

where a_{ij} is the number of subsets A of M with rank $r(M)-i$ and cardinality $r(M)-i+j$. The Tutte polynomial and its chief evaluation, the characteristic polynomial

$$\chi(M;\lambda) = \Sigma\mu(0,x)\lambda^{r(M)-r(x)}$$

(the sum being taken over all elements in the geometric lattice associated with M, and the rank function and Möbius function $\mu(0,x)$

being computed in that lattice), have come up in a variety of applications. The characteristic polynomial as a lattice invariant can be thought of as a generating function for the Möbius function. It has applications, of course, to other, non-geometric, lattices and its rich general theory is presented in this·volume by Professors Barnabei, Brini, and Rota.

The Tutte polynomial, on the other hand, seems to be special to matroids. It is to its general theory and applications that we address our notes. In the present volume, we present the first part, concentrating (after the next, motivational, section) on the structure of $t(M)$ for a general matroid and on the nature of a "Tutte-Grothendieck invariant." These latter invariants deserve a special treatment, and we give it in the second part to appear elsewhere. For now, as justification for our general survey we give a sampling of some of the areas in which certain evaluations of the Tutte polynomial coincide with important invariants.

- minimal flow calculations in networks [1, 27, 81, 82, 95, 103, 124, 136, 139, 140, 151, 153, 154]
- graph coloring [8, 27, 29, 39, 57, 64, 82, 95, 107, 117, 124, 135, 137, 138, 140, 142, 145, 146, 151, 153, 154, 157, 160, 172]
- percolation theory [47, 71, 115, 116, 152]
- hyperplane arrangements, convexity, and separation in affine and projective space [32, 49, 50, 76, 77, 163, 164, 167, 168, 174, 175]
- acyclic, totally cyclic, and coherent orientations of graphs and oriented matroids [16, 44, 50, 61, 76, 77, 87, 89, 90, 134, 163, 167, 170]

- zonotopes [77, 128, 163, 167]
- packing and coding theory [36, 65, 75, 107, 153, 154, 155]
- intersection numbers for subsets of points in a finite projective space and the critical problem [27, 37, 43, 60, 65, 83, 107, 144, 148, 151, 153, 154]
- electrical networks [12, 24, 33, 129, 103, 130]
- combinatorial designs [19, 62, 63, 70, 105, 162]
- quantum and statistical mechanics [9, 71, 127]
- trees [7, 27, 33]
- signed and voltage graphs [66, 67, 168, 169, 170, 172]
- Eulerian paths [91, 92, 99, 100, 149]
- covering [104]
- scoring in tournaments [76, 77, 167]
- topological dissections [164, 165]
- embedding graphs in surfaces [91, 99]
- root systems [168]

We view the fact that invariants in all the above areas are evaluations of the same polynomial as ample evidence that a general theory is merited. In addition, it often occurs that applications in one area suggest analogous formulas in another. A famous example is the critical exponent of Crapo and Rota applying ideas from the chromatic theory of graphs to coding and packing theory in finite projective spaces. In fact, the Tutte polynomial for matroids was invented by Crapo [56] as a generalization of Tutte's work in graph coloring [137, 138]. Recent examples are contained in the work of Oxley [107, 108, 109] and in [83], where the Hajos construction for graphs of chromatic number at least q is analogized to representable matroids of critical exponent at least k.

Although these notes sketch (or give references to) previously published results, much is new. In section three, we explore the nature of what is meant by a "Tutte-Grothendieck invariant," distinguishing several types while relating them to $t(M)$. In section four, we show that various operations on M (such as adding a point in free position and "tensoring" (a new operation)) affect the Tutte polynomial in predictable ways, while for others (such as the free erection), the Tutte polynomial of the resulting matroid M' cannot in general be calculated from $t(M)$. Section five concerns reconstruction: what partial information about a matroid allows one to calculate its Tutte polynomial? Conversely, what information can $t(M)$ give us about useful structural invariants (such as the number of certain closed sets)? The total number of closed sets (indexed by rank and cardinality) cannot in general be tabulated if only $t(M)$ is known, but formulas for it are given for certain classes. We explore one of these classes - near-designs, which simultaneously generalize projective spaces and paving matroids.

In the final section, we study some general identities and inequalities (such as log concavity) satisfied by the evaluations and coefficients of $t(M)$. Many inequalities depend on parameters and are sharp, becomming equalities when the matroid is in a certain class. Examples of these extremal classes are given, as we-l as a general framework to find other extremal classes and their respective sharp bounds. A few exercises and many research problems accompany each chapter.

We will assume the kind of familiarity with matroid theory obtained from [151] (or, to give the other coauthors equal treatment, [42] or [60]).

We wish to thank the C.I.M.E. for their sponsorhip of the lectures on which these notes are based and for affording an opportunity for all of us at the conference to share ideas in the beautiful surroundings of Varenna.

In addition, we thank Hazeline Lewis; Gary Gordon, Professor Rhodes Peele; Hazeline Lewis; and Professor Adriano Barlotti, respectively, for their utmost patience during the typing, proofreading, retyping, and overdue receipt of this paper.

Vorrei dedicare questi appunti a tutti i miei amici italiani ed in particolare a Brúna ed alla nostra nuova vita insieme.

2. A Prototypical Example.

In this section, we illustrate the idea of a "Tutte-Grothendieck" theorem: one which can be (easily) verified on loops and isthmuses, and which is then proved inductively on matroids of K points by showing a relationship between relevant properties of G on the one hand and the pair $(G-p, G/p)$ on the other. In the course of the proof, many ideas will be presented such as the nature of deletion and contraction for various special classes of matroids (graphic, representable, etc.).

Theorem 2.1. For a binary matroid M, the following are equivalent.

1. M is affine (i.e. M is isomorphic to a subset of some binary affine space $AG(n,2)$ with, perhaps, multiple points).

2. In a binary vector representation for M, there exists a linear functional f such that $f(\underline{v}) \neq 0$ (i.e., $f(\underline{v}) = 1$) for all $\underline{v} \in M$.

3. All circuits of M are even (i.e., have even cardinality).

4. All hyperplane complements of M^* are even.

5. M^* has a partition into circuits.

For 6 and 7 when M is viewed as a linear code C:

6. C contains the vector $(1,1,\ldots,1)$.

7. $C^{\perp}$, the dual code, is an even-weight code.

If M is graphic with graphic representation $G(M)$:

8. $G(M)$ is two-colorable.

If M is cographic with a representation $G(M^*)$ of M^* as a connected graph:

9. $G(M^*)$ has an Eulerian cycle.

10. M is loopless,and the associated geometry of M, $\bar{M}$, obeys any (or all) of the above properties.

No pair of the above equivalent properties is hard to prove directly. Some are classical ($3 \leftrightarrow 8$, $4 \leftrightarrow 9$), some are trivial ($1 \leftrightarrow 2$, $5 \leftrightarrow 6$, $3 \leftrightarrow 4$, etc.), and all have appeared in the literature. Our proof will be different than the ones usually presented as it will proceed by induction. In particular, for each i, let χ_i be the "characteristic function" of the property P_i, i.e.

$$\chi_i(M) = \begin{cases} 1 & \text{if } M \text{ satisfies } P_i \\ 0 & \text{if } M \text{ does not.} \end{cases}$$

Then each χ_i is an invariant and we will show that each obeys the following two boundary conditions:

B_1. $\chi_i(M) = 0$ if M is a loop.

B_2. $\chi_i(M) = 1$ if M is an isthmus.

Further, χ_i obeys the following recursions:

B_3. $\chi_i(M) = \chi_i(M-p) \cdot \chi_i(p)$ if p is a loop or isthmus.

B_4. $\chi_i(M) = \chi_i(M-p) - \chi_i(M/p)$ if p 'is neither a loop nor an isthmus.

It then follows that all of the properties are equivalent since $\chi_i(M) = \chi_j(M)$ on a one-point matroid (necessarily a loop or an isthmus), and, by an induction hypothesis, on smaller matroids. If, for example, M has a point p which is neither a loop nor an isthmus, $\chi_i(M) = \chi_i(M-p) - \chi_i(M/p) = \chi_j(M-p) - \chi_j(M/p) = \chi_j(M)$.

The rest of this section will be devoted to showing that χ_i obeys the system $B = \{B_1,B_2,B_3,B_4\}$ for $i = 1,2,\ldots,10$. A common thread in many of the proofs will be that $\chi_i(M)$ counts something which is positive exactly when P_i holds.

The first property is a geometric one and we will use synthetic arguments.

Proof of P_1. By considering the affine span of M, it is easy to see that M is in some binary affine space if and only if it is in AG(n-1,2), the affine space of dimension n-1 (rank n), where $n = r(M)$. Let χ_1' be the number of hyperplanes which miss M in an embedding of M in PG(n-1,2). (Clearly there is at most one since $PG(n-1,2) - \{H_1,H_2\} \simeq AG(n-1,2) - H \simeq AG(n-2,2)$, an affine space of lower rank.)

We will show that χ_1' obeys B and thus so will χ_1. There are no loops in affine space while an isthmus is isomorphic to AG(0,2). Hence, B_1,B_2, as well as B_3 when p is a loop are all trivial.

If p is an isthmus and H is a hyperplane which misses M, then clearly $H \cap \overline{M-p}$ is a hyperplane in the projective span of

M-p, $\overline{M-p}$, which misses M-p. Conversely, if H' is a hyperplane of $\overline{M-p}$ which misses M-p, then $\overline{H' \cup q}$ is a hyperplane of PG(n-1,2) which misses M, where q is the third point on some line containing p and another point of M-p. This relationship is bijective so that $\chi_1'(M) = \chi_1'(\overline{M-p}) = \chi_1'(M-p)\cdot\chi_1'(p)$.

To prove recursion B_4, it will be easier to show that $\chi_1'(M-p) = \chi_1'(M) + \chi_1'(M/p)$. For this, let H be any hyperplane which misses M-p. Then,it either contains p or it does not. In the latter case it gives a hyperplane which misses M, and in the former case there is an associated hyperplane H' = H/p in PG(n-2,2) which misses M/p. Here projection by the point p means picking a hyperplane H" which does not contain p and projecting, via lines through p, all the points of H, PG(n-1,2), and M-p respectively onto H". Conversely, if a hyperplane misses M, it gives a hyperplane which misses M-p, and if a hyperplane H' misses M/p, then $\overline{H' \cup p}$ is a hyperplane which misses M-p and passes through p. This exhausts all the cases. (For example, note that there cannot be both a hyperplane with missės M and another which misses M/p, since this would lead to two distinct hyperplanes which miss M-p.)

Proof of P_2 and P_6. A binary representation for M is an n by K matrix N where n = r(M), K = |M|, and dependency in M corresponds to linear dependency among the columns of N. A linear functional f such that $f(\underline{v}) = 1$ for all columns $\underline{v}$ of N then corresponds to a row vector $\underline{w}$ such that $\underline{w}\cdot N = \underline{1}$ where $\underline{1}$ is the vector of all ones. The existence of such a $\underline{w}$ is equivalent to the vector $\underline{1}$ being in the row space of N. However, the code C of length K and dimension n associated with a matroid M represented by a matrix N is precisely the vector subspace of F^K consisting of the $|F|^n$ vectors spanned by the rows of N. Thus χ_2 and χ_6 are equivalent and we can view our proof as an analytical formulation of the synthetic arguments for χ_1. Let χ_2' count the vectors $\underline{w}$ such that $\underline{w}\cdot N = \underline{1}$. A loop is represented (in any dimension) by a column of zeros, and thus, if M contains a loop, $\underline{w}\cdot N$ is zero in that column for any, $\underline{w}$. Further, an isthmus is represented by the matrix [1] and for this representation, the scalar vector $\underline{w} = 1$ gives the desired conclusion.

The number of vectors $\underline{w}$ such that $\underline{w}\cdot N = \underline{1}$ is preserved under row-equivalent representations of M, since if P is a nonsingular $n \times n$ matrix, $P\cdot N$ also represents M by standard theory, while $\underline{w}\cdot N = (\underline{w}\cdot P^{-1})\cdot(P\cdot N)$. Now assume that $p \in M$ is not a loop and (applying appropriate row operations if necessary) is represented by the (first) column vector $\begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix}$ of N. The matrix N is then of the following form:

$$N = \begin{bmatrix} 1 & \underline{v} \\ 0 & \\ 0 & \\ \vdots & A \\ 0 & \end{bmatrix}$$

where $\underline{v}$ is a row vector of length $K-1$, A is a matrix of size $n-1 \times K-1$, $\underline{v} = \underline{0}$ if and only if p is an isthmus, A represents

M/p, and $\left[\begin{array}{c} \underline{v} \\ - \\ A \end{array}\right]$ represents M-p.

Using these representations, it is obvious that, if p is an isthmus, $\underline{w}'\cdot A = \underline{1}$ if and only if $\underline{w}\cdot N = \underline{1}$, where $\underline{w}$ is the vector $\underline{w}'$ preceded by a one. Thus, B_3 is satisfied.

If p is not an isthmus, then some entry of $\underline{v}$ is 1. Let $\underline{w}$ be a vector such that $\underline{w}\cdot\left[\begin{array}{c} \underline{v} \\ - \\ A \end{array}\right] = \underline{1}$. Then $\underline{w}\cdot N = \underline{1}$ if and only if $\underline{w}$ has a one in its first coordinate, and $\underline{w}$ has a zero in its first coordinate if and only if $\underline{w}'\cdot A = \underline{1}$, where $\underline{w}'$ is the vector $\underline{w}$ with its first coordinate deleted. In terms of the invariant χ_2', this shows that $\chi_2'(M-p) = \chi_2'(M) + \chi_2'(M/p)$.

<u>Proof of P_3.</u> A loop is an odd circuit, and an isthmus is in no circuit, so that recursions B_1, B_2', and B_3 are trivial for $\chi_3(M)$. Now assume that p is not an isthmus, so that it must be contained in some circuit C. We prove the recusion $\chi_3(M-p) = \chi_3(M) + \chi_3(M/p)$. If $\chi_3(M-p) = 0$ then M-p contains an odd circuit C' so that M does also $(\chi_3(M) = 0)$. In addition, C' is the disjoint union of (at most two) circuits in M/p. (The subgeometry $C \cup p$ has nullity at most two, so is graphic with graphical representation a θ graph in the nullity-two case.) Thus, one of these circuits is odd, and $\chi_3(M/p) = 0$. On the other hand, assume $\chi_3(M-p) = 1$. If the circuit C containing p is odd, it is an elementary property of the circuit elimination axiom for binary matroids that all circuits containing p are odd, and that M/p contains only even circuits,

in which case $\chi_3(M/p) = 1$, and $\chi_3(M) = 0$. If C is even, so are all circuits containing p. Thus $\chi_3(M) = 1$ and $\chi_3(M/p) = 0$.

Proof of P_4. P_4 is of course a (dual) restatement of P_3 since circuits of M are bonds (complements of hyperplanes) of M^*. Let us, however, see what a direct proof (involving bonds) would involve.

Let $\chi_4^*(M) = \begin{cases} 1 & \text{if } M \text{ has all even bonds} \\ 0 & \text{otherwise.} \end{cases}$ Then,

$\chi_4^*(M) = \chi_4(M^*) = \chi_3(M^*)$, and the recursions in the proof of χ_3 become:

B_1^*. $\chi_3(M^*) = 0$ if M^* is a loop

B_2^*. $\chi_3(M^*) = 1$ if M^* is an isthmus

B_3^*. $\chi_3(M^*) = \chi_3(M^*-p)\cdot\chi_3(p)$ if p is a loop or isthmus of M^*

B_4^*. $\chi_3(M^*) = \chi_3(M^*-p) - \chi_3(M^*/p)$ if p is neither a loop nor an isthmus.

But standard matroid theory shows us that a loop is dual to an isthmus, and that deletion is dual to contraction. Thus, $B_1^* - B_4^*$ become:

B_1^*. $\chi_4^*(M) = 0$ if M is an isthmus

B_2^*. $\chi_4^*(M) = 1$ if M is a loop

B_3^*. $\chi_4^*(M) = \chi_4^*(M/p)\cdot\chi_4^*(p) = \chi_4^*(M-p)\cdot\chi_4^*(p)$ if p is an isthmus or loop

B_4^*. $\chi_4^*(M) = \chi_4^*(M/p) - \chi_4^*(M-p)$ if p is not a loop or isthmus.

Thus a proof of property P_4 is equivalent to proving recursions $B_1^* - B_4^*$ for χ_4^*, and we will use this observation in our proof of P_5.

Proof of P_5. As outlined above, we must prove conditions $B_1^* - B_4^*$ for

$$\chi_5^*(M) = \begin{cases} 1 & \text{if } M \text{ has a partition into circuits} \\ 0 & \text{otherwise.} \end{cases}$$

If M has a loop p, clearly $\chi_5^*(M) = \chi_5^*(M-p)\cdot\chi_5^*(p) = \chi_5^*(M-p)$. If M contains an isthmus, it cannot be partitioned into circuits (an isthmus being in no circuit), so we may concentrate our proof on recursion B_4^*. We use a matrix proof. When M is represented by the matrix N, it is elementary to show that M is partitioned into circuits if and only if every row of M has an even number of ones. (A set of columns of N is a disjoint union of circuits if and only if the modulo-two sum of those vectors is zero.) Assume N is as in the proof of P_2 (noting that elementary row operations preserve the property of every row being even). If A has an odd row, so do N and $\begin{bmatrix} \underline{v} \\ - \\ A \end{bmatrix}$, and $\chi_5^*(M) = \chi_5^*(M-p) = \chi_5^*(M/p) = 0$. If A has all even rows (i.e. M/p has a partition into circuits), then N has all even rows ($\chi_5^*(M) = 1$) iff $\underline{v}$ has an odd number of ones iff $\begin{bmatrix} \underline{v} \\ - \\ A \end{bmatrix}$ has an odd row ($\chi_5^*(M-p) = 0$). This handles all cases.

Proof of P_7. The dual code $C^{\perp}$ of C is the set of all vectors $\underline{w}$ such that $\underline{w}\cdot\underline{v} = 0$ for all (row) vectors $\underline{v}$ in C. Standard theory shows that when a basis for C forms the rows of a matrix N and when a basis for $C^{\perp}$ forms the rows of N', N and N' represent dual matroids. But linear combinations (over F_2) of even-weight vectors have even weight, so that $C^{\perp}$ is an even-weight code if and only if it has a representing matrix all of whose rows are even. Thus, the above proof of P_5 serves equally well for P_7.

Proof of P_8. This is perhaps the prototypical example of the theory since the recursions $B_1 - B_4$ for graph coloring have been well-known since G. D. Birkhoff's pioneering work [10] seventy years ago and were developed into a theory by Tutte [137] which anticipated for graphs the present point-of-view. Let G be a connected graph and let $\chi_\lambda(G)$ be the number of ways to color the vertices of G with λ colors so that no two vertices of the same color are connected by an edge. (It will be a consequence of our proof that $\chi_\lambda(G)$ is a polynomial in λ whose degree is the number of vertices of G.) We will show that $\chi_\lambda(G)/\lambda$ obeys the conditions B_1, B_2', B_3 and B_4 where B_2' is B_2 with 1 replaced by $\lambda-1$. Since $\chi_{\lambda=2}(G(M))/2 = \chi_8(M)$, we will then be done. (A connected graph has either zero or two two-colorings.) If G contains a loop (graphically, an edge joining a vertex to itself), it cannot be colored so that $\chi_\lambda(G) = 0$. If G is an isthmus, it consists of two vertices joined by an edge, so that $\chi_\lambda(G) = \lambda(\lambda-1)$, and B_2' is satisfied. We will prove B_3 only for trees. In the following section (3.5), we will show that this apparently weaker requirement in fact implies B_3. If G is a tree with n edges, then $\chi_\lambda(G) = \lambda(\lambda-1)^n$, each edge being an isthmus. Further, the matroid of G is the direct sum of n isthmuses, and, conversely, a direct sum of n isthmuses is represented by any tree of n edges. Thus, for trees $\frac{\chi_\lambda(G)}{\lambda} = (\lambda-1)^n = \frac{\chi_\lambda(G-p)}{\lambda}\cdot\frac{\chi_\lambda(p)}{\lambda}$. To prove B_4, we must show that $\chi_\lambda(G) + \chi_\lambda(G/p) = \chi_\lambda(G-p)$. But, if p is not an isthmus, G-p is represented by the connected graph formed by deleting the edge p, while if p is not a loop, G/p is represented by the graph formed by identifying the two vertices joined by p and then deleting the edge p. It is then elementary to show that every (proper) coloring of G-p is either a coloring of G (when the two vertices joined by p receive different colors) or corresponds in a unique manner to a coloring of G/p (where each vertex not incident with p gets the same color in G/p and G, and the new vertex gets the color of the two identified vertices).

Proof of P_9. This will be generalized later in Part II in a manner analogous to P_8. For now, we will show that χ_9^* satisfies the conditions $B_1^* - B_4^*$ using the Euler condition that a connected graph G has an Eulerian cycle if and only if every vertex of G has even degree. Certainly if G (= G(M)) has an isthmus, it cannot have an Eulerian cycle; while, if p is a loop, B_2^* and B_3^* are trivial. Now assume that p joins v and v' in G, and let d(w) denote the degree of the vertex w in G. If d(w) is odd in G for w neither v nor v', then $\chi_9^*(G) = \chi_9^*(G-p) = \chi_9^*(G/p) = 0$ (using the representations for G-p and G/p given in the proof of P_8). Assume now that d(w) is even for each of these vertices. Then $\chi_9^*(G/p) = 1$, since the identified vertex in G/p must also have even degree. (The sum of the vertex degrees of any graph is even.) If v and v' both have even degree, then $\chi_9^*(G) = 1$, while $\chi_9^*(G-p) = 0$. Conversely, if v and v' both have odd degree, then $\chi_9^*(G) = 0$ while $\chi_9^*(G-p) = 1$.

Proof of P_{10}. When χ_i is viewed as a (generalized) Tutte-Grothendieck invariant (see 3.20), P_{10} follows as a special instance of (3.15).

Research Problem. Find other properties of a matroid (perhaps in some special class) whose characteristic functions satisfy a similar recursion.

3. The Tutte Polynomial.

The underlying idea of the invariants χ_i of the previous section was that there was a recursion of the general form $f(M) = af(M-p) + bf(M/p)$ when p was neither an isthmus nor a loop,and $f(M) = f(M-p)\cdot f(p)$ otherwise. (In the previous section, $a = 1$ and $b = -1$.) But we note that M/p has rank one less than M when p is not a loop,while $r(M-p) = r(M)$ when p is not an isthmus. Thus, for each i, $f_i(M) = (-1)^{r(M)}\chi_i(M)$ obeys the additive recursion

$$(*) \qquad f_i(M) = f_i(M-p) + f_i(M/p)$$

as well as the multiplicative recursion B_3 and the boundary conditions: $f_i(\text{loop}) = 0$, $f_i(\text{isthmus}) = -1$. Many other invariants can be"fudged up" to obey the same additive recusion (*). The abundance of these invariants which we will exhibit in the following sections and, especially, Part II motivatesus to establish a general theory for all such invariants. The fundamental idea is that of a universal invariant called the *Tutte polynomial.* As we saw in the previous section, the idea is based on the work of Tutte [137] and was generalized to matroids and given its present name by Crapo [56]. The theorem below is from [27] while the general categorical framework is presented in [26]. In the following, we define a *Tutte-Grothendieck invariant* as a function on matroids taking values in a commutative ring R which satisfies conditions T1 and T2 below. To simplify the statements of such conditions as T1 and T2, we use the term *factor* to denote a point p which is a loop or isthmus. The term comes from the fact that a matroid M

factors as a direct sum into a point p and its complement: $M \approx p\oplus(M-p)$ if and only if p is an isthmus or loop. If p is neither, it is called a *nonfactor*.

Theorem 3.1 There is a unique two-variable polynomial with integer coefficients associated with any matroid M called the Tutte polynomial $t(M;x,y)$ which is an isomorphism invariant (if $M_1 \approx M_2$, then $t(M_1) = t(M_2)$), and which obeys the following four properties:

T1. $t(M) = t(M-p) + t(M/p)$ if p is a nonfactor

T2. $t(M) = t(M-p)\cdot t(p)$ if p is a factor

T3. $t(L) = y$ and $t(I) = x$, where L is a loop (one-point matroid of rank zero), and I is an isthmus (one-point matroid of rank one).

T4. If f is any *Tutte-Grothendieck invariant* with values in a commutative ring R, then $f(M) = t(M;f(I), f(L))$, where the polynomial operations take place in R.

We will present two proofs of the theorem. The first is longer and more technical but can be adapted to algebraic objects other than matroids. The second uses a more concrete matroid invariant. Abstract categorical algebra techniques similar to those used by Grothendieck show that there is a ring R' and unique invariant with values in R' which has the "universal" property of T4 with respect to conditions T1 and T2 on all matroids. The essential part of the proof is in showing that this commutative ring R' is free (i.e., a polynomial ring) so that the ring homomorphism is evaluation. We will see in the first proof that this is so because an abstract "decomposition" of M along the lines of T1 and T2 is independent of how we order the points of M.

First Proof. Consider the class M_o of *ordered matroids* $M_o((p_1,\ldots,p_k))$ and the function $t_o : M_o \to \mathbb{Z}[x,y]$ which is recursively defined by T'1-T'3 below:

T'1. $t_o(M_o((p_1,\ldots,p_k))) = t_o(M_o((p_1,\ldots,p_{k-1}))) +$
$t_o(M_o((p_1,\ldots,p_k))/p_k)$ if p_k is a nonfactor.

T'2. $t_o(M_o) = t_o(p_k)\cdot t_o(M_o-p_k)$ otherwise.

T'3. $t_o(\text{isthmus}) = x$, $t_o(\text{loop}) = y$.

This function clearly satisfies T3 and T4, and the proof consists of showing that it satisfies T1 and T2 (for any point p). This is done by showing that we can interchange the last two points (p_k and p_{k-1}) in the order and get the same polynomial. There are many cases to consider. For example, if p_{k-1} is an isthmus in $M - p_k$ but not in M, then p_{k-1} and p_k form a pair of points in series, and there is an automorphism of M which interchanges p_k and p_{k-1}. Then, if o' is the ordering $(p_1,\ldots,p_k,p_{k-1})$, we have that

$$\begin{aligned} t_o(M_o) &= t_o(M_o/\{p_{k-1},p_k\}) + (1+t_o(p_{k-1}))\cdot t_o(M_o-\{p_{k-1},p_k\}) \\ &= t_o(M_o/\{p_{k-1},p_k\}) + (1+x)\cdot t_o(M_o-\{p_{k-1},p_k\}) \\ &= t_o(M_{o'}). \end{aligned}$$

To consider one more case (the generic one) when neither p_k nor p_{k-1} is a loop or isthmus, and they are not in series or parallel, then, e,g., $(M-p_{k-1})/p_k = (M/p_k)-p_{k-1}$, and again $t_o(M_o) = t_o(M_{o'})$. We use similar arguments for the other cases, and we note that if p_k is not the last point in the order, we can still transpose it with p_{k-1}. (We apply T1' and T2' to take care of all the points p_i with $i > k$ and then transpose in each monomial.) Thus, we can filter any point $p \in M$ through the order to give a new order o" in which it is the last point, so that T1 and T2 are satisfied by t_o, and we may define t(M) by $t_o(M_o)$ where o is any ordering on the points of M.

Second Proof. We define the function

$$t'(M) = \sum_{A \subseteq S} (x-1)^{\mathrm{cor}(A)} (y-1)^{\mathrm{nul}(A)}$$

where M is a matroid on the set S, and for any subset A of S, cor(A) is the corank of A (r(S)-r(A)) and nul(A) is the nullity of A (|A|-r(A)). The function t'(M) is a well-defined polynomial obeying the boundary conditions of T3. If we show that t' also obeys T1 and T2, then induction shows that t(M) = t'(M) satisfies T4 and the theorem. Now, let p be an isthmus of M. Then,

$$t'(M) = \sum_{A \subseteq S} (x-1)^{r(S)-r(A)} (y-1)^{|A|-r(A)} ,$$

and we break up the sum according to whether the subset A contains p or not. If $p \in A$, then the subset A-p has the same corank as well as nullity in M-p as A does in M. If $p \notin A$, A has the same nullity calculated in the matroid M as in the matroid M-p, whereas $\mathrm{cor}_M(A) = \mathrm{cor}_{M-p}(A) + 1$. Therefore:

$$t'(M) = (x-1) \sum_{\substack{A \subseteq S \\ p \notin A}} (x-1)^{\mathrm{cor}_{M-p}(A)} (y-1)^{\mathrm{nul}_{M-p}(A)}$$

$$+ \sum_{\substack{A\subseteq S \\ p\in A}} (x-1)^{\mathrm{cor}_{M-p}(A-p)} (y-1)^{\mathrm{nul}_{M-p}(A-p)}$$

$$= x \sum_{A\subseteq S-p} (x-1)^{\mathrm{cor}_{M-p}(A)} (y-1)^{\mathrm{nul}_{M-p}(A)}$$

$$= t'(p)\cdot t'(M-p).$$

A similar arrangement of the summation proves T2 for the case of a loop and proves T1 when p is neither a loop nor an isthmus. In fact, it is the latter case which shows why we only use the identity T1 when p is a nonfactor: p is not a loop iff $\mathrm{nul}_{M/p}(A-p) = \mathrm{nul}_M(A)$ for all subsets A containing p (corank is preserved for any point) while for all subsets A not containing p, p is not an isthmus iff $\mathrm{cor}_{M-p}(A) = \mathrm{cor}_M(A)$ (nullity is always preserved).

Definition 3.2. For a matroid M of rank n, define the *corank-nullity polynomial* by

$$S(M;u,v) = \sum_{A\subseteq S} u^{\mathrm{cor}(A)} v^{\mathrm{nul}(A)}$$

$$= u^n \sum_{A\subseteq S} \frac{v^{|A|}}{(uv)^{r(A)}} .$$

Proposition 3.3.

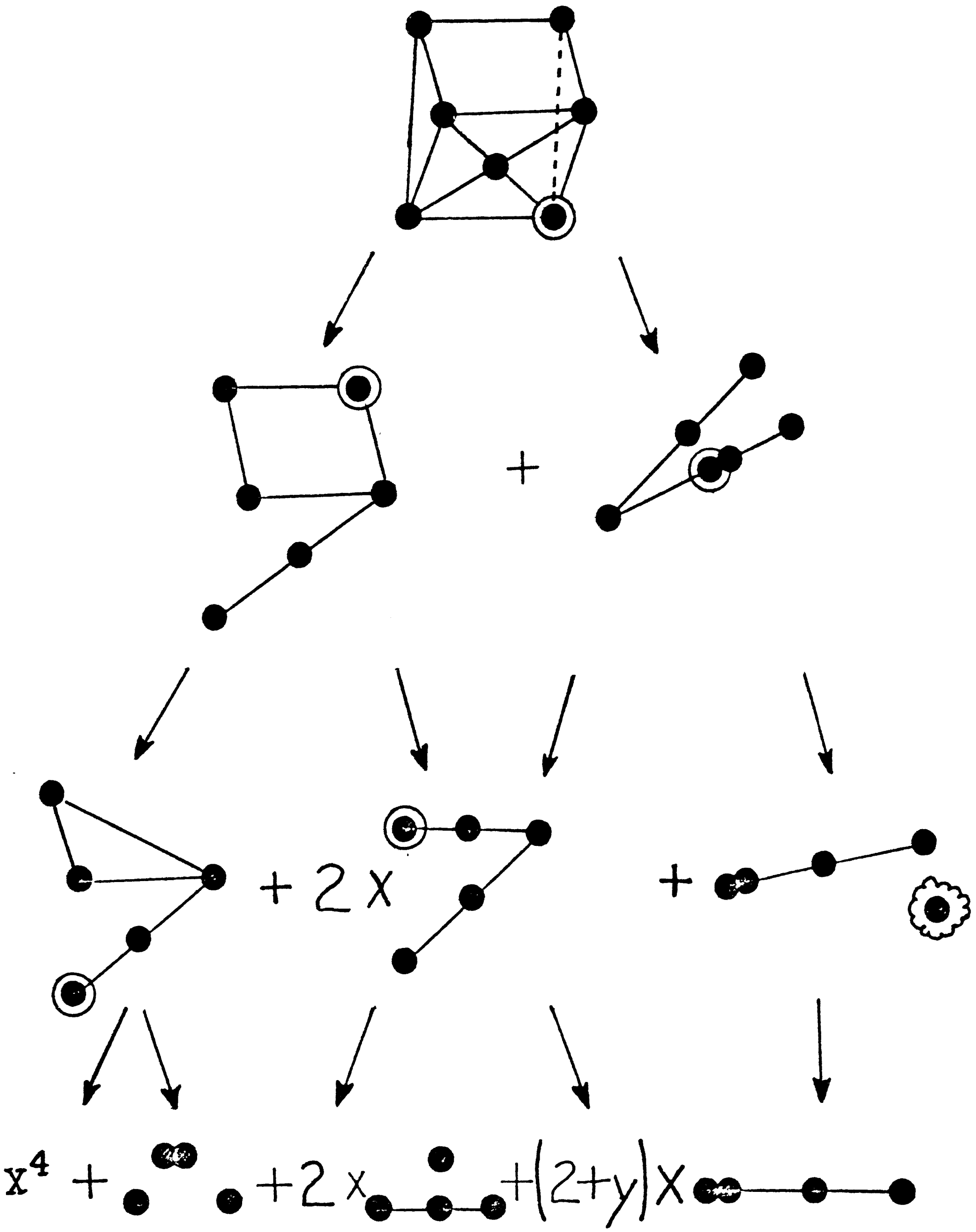
1. $S(M;u,v) = t(M;u+1,v+1)$.
2. $t(M;0,0) = 0$.
3. $t(M;1,1)$ is the number of bases of M.
4. $t(M;2,1)$ is the number of independent sets of M.
5. $t(M;1,2)$ is the number of spanning sets of M.
6. $t(M;2,2) = 2^K$, the number of subsets of M ($K = |M|$).

7. $t(M^*;x,y) = t(M;y,x)$.

Proof. The first statement follows from the second proof of Theorem 3.1 (where it is shown that $S(M)$ is a Tutte-Grothendieck invariant). An inductive proof based on the recursive definition of t gives (3.3.2), while (3.3.3) - (3.3.6) are all easily shown by appropriately evaluating $S(M)$ using (3.3.1).

The final statement, showing that the Tutte polynomial of the dual matroid is obtained by interchanging the two variables, can be proved via the corank-nullity generating function, since cor (A) computed in M is the same as nul(S-A) computed in M^*, so that $S(M^*;u,v) = S(M;v,u)$. An alternate proof can be formulated exploiting the universal property T4 of t. Define $t^*(M)$ to be $t(M^*)$. Then, elementary arguments show that t^* is a Tutte-Grothendieck invariant. Hence, $t^*(M) = t(M;t^*(I), t^*(L)) = t(M;t(L),t(I)) = t(M;y,x)$. This is essentially the proof of χ_4 and χ_5 given in the previous section.

Example 3.4. Let M be the matroid consisting of the six vertices of a triangular prism with a seventh point on the center of one of the rectangular faces. We illustrate the calculation of $t(M)$ below, where all pictures are to be viewed in the appropriate Euclidean space, decompositions are with respect to circled points, juxtaposed points represent multiple points, ☁ encloses a loop, ↙ represents deletion, ↘ represents contraction, and ↓ stands for an application of T2.


+
+ 2 x
+
x⁴ +
+ 2 x
+(2+y) x

Completing the decomposition we obtain:

$$t(M) = x^4 + x^2(x+y) + 2(x(x^2+x+y)) + (2+y)((x+y)x + y^2 + y + x)$$

$$= x^4 + 3x^3 + 4x^2 + 2x$$

$$+ 2x^2y + 5xy + 2y$$

$$xy^2 + 3y^2$$

$$+ y^3$$

In the proof of P_8 in Section 2, condition T2 was verified only for trees. The justification for that apparently weaker verification is given in the next proposition.

Proposition 3.5 Let f be an invariant which satisfies the additive recursion for all matroids M and nonfactors $p \in M$:

T1. $f(M) = f(M-p) + f(M/p)$.

Then the following are equivalent:

T2. $f(M) = f(M-p) \cdot f(p)$ for all matroids M and factors $p \in M$.

T2'. $f(M_1 \oplus M_2) = f(M_1) \cdot f(M_2)$ for all direct sums $M = M_1 \oplus M_2$.

T2". $f(B) = f(B-p) \cdot f(p)$ for all totally separable matroids (i.e., those in which every point is a factor: a boolean algebra with loops).

Proof. Clearly T2' implies T2 which in turn implies T2". We show first that T2" implies T2.

Assume that an invariant f satisfies T1 and T2". We show, by induction on the size of M, that f must, in addition, satisfy T2. Properties T2 and T2" are equivalent on one-point matroids, so let M be a matroid on $K+1$ points and assume f obeys T2 on all K-point matroids. If M has only loops and isthmuses, T2 follows from T2", so assume p is a factor of M and $q \in M$ is not a factor. Using arguments similar to those of the first proof of (3.1) we obtain:

$$\begin{aligned} f(M) &= f(M-q) + f(M/q) \\ &= f((M-q)-p) \cdot f(p) + f((M/q)-p) \cdot f(p) \\ &= (f((M-p)-q) + f((M-p)/q)) \cdot f(p) \\ &= f(M-p) \cdot f(p). \end{aligned}$$

To show that T2 implies T2', assume f is a Tutte-Grothendieck invariant, and that $M = M_1 \oplus M_2$. Property T2 is precisely property T2' with $|M_2| = 1$. The proof that T2 and T2' are equivalent in general uses induction on the cardinality of M_2 and is similar to the inductive proof above. The proof rests on the fact that deletions and contractions in a direct sum may be performed upon the whole matroid or within the appropriate direct-sum factor resulting in isomorphic matroids. For example, if $p \in M_2$, then p is an isthmus of M_2 if and only if it is an isthmus of $M = M_1 \oplus M_2$, and $M_1 \oplus (M_2 - p) \cong (M_1 \oplus M_2) - p$. Now assume $|M_2| = K+1$, and that T2' holds for all M_2 with $|M_2| = K$. If M_2 is totally separable, T2' follows easily from T2, so let $p \in M_2$ be a nonfactor. Then:

$$\begin{aligned} f(M_1 \oplus M_2) &= f((M_1 \oplus M_2)-p) + f((M_1 \oplus M_2)/p) \\ &= f(M_1 \oplus (M_2-p)) + f(M_1 \oplus (M_2/p)) \\ &= f(M_1) \cdot f(M_2-p) + f(M_1)\ f(M_2/p) \\ &= f(M_1) \cdot (f(M_2-p) + f(M_2/p)) \\ &= f(M_1) \cdot f(M_2). \end{aligned}$$

<u>Corollary 3.6</u> If t is the Tutte polynomial, then $t(M_1 \oplus M_2) = t(M_1)t(M_2)$.

We remark that Proposition 3.5 says that Tutte-Grothendieck invariants satisfy the apparently stronger T2' which is a useful property (say in computations or applications), while in verifying whether a given invariant is a Tutte-Grothendieck invariant, the multiplicative condition T2 need only be verified in the very special cases of T2".

We will come back to other applications and examples and give more properties of the Tutte polynomial, but first we discuss the nature of a Tutte-Grothendieck invariant.

The abstract algebraic idea is represented in the commutative diagram below

(3.7)
$$\begin{tikzcd}
 & R = \mathrm{FCR}[M] \arrow[dr, "\varepsilon"] & \\
M \arrow[ur, "i"] \arrow[rr, "t"] \arrow[dr, "f"'] & & R/I = \mathbb{Z}[x,y] \arrow[dl, dashed, "e"'] \\
 & R &
\end{tikzcd}$$

Here, M is the set of matroid isomorphism classes, R is the free commutative ring generated by M, i is the map which takes a matroid (isomorphism class) to its generator, and I is the ideal generated by all elements of the form $i(M)-i(M-p)-i(M/p)$ and $i(M)-i(M-q)\cdot i(q)$. Here, q is a loop or isthmus of the matroid M, and p is neither a loop nor isthmus. The map $\varepsilon : R \to R/I$ is the canonical epimorphism, and $t = \varepsilon \circ i$ assigns to any matroid its Tutte polynomial. General algebraic theory [26] states that, for any invariant f with values in a commutative ring R which is zero on the generators of I (i.e., obeys T1 and T2), there is a unique function $e : R/I \to R$ such that $f = e \circ t$. The ring R/I is called the *Tutte-Grothendieck ring* and the essence of Theorem 3.1 is that R/I is free (a polynomial ring over the integers in two variables), while e is evaluation. (Whether R/I contains 1 is a matter of taste. If it does, then one can define $t(E) = 1$, where E is the empty matroid.)

In this categorical context, Theorem 3.5 states that the ideal I contains all elements of the form $i(M)-(i(M_1)\cdot i(M_2))$ where $M = M_1 \oplus M_2$, while, on the other hand, I is generated by the relations T1 along with only relations of the form $i(B)-i(B-p)\cdot i(p)$ for totally separable matroids B. We now define some invariants with properties generalized from T1 and T2. Although each is formally different from the rest, all are related in a fairly natural way to the Tutte polynomial. It will be the purpose of the rest of this section to explain these relationships.

Definition 3.8

1. A *Tutte-Grothendieck group invariant* f is one with values in an abelian group which obeys axiom T1. That is, $f(M) = f(M-p) + f(M/p)$ for all nonfactors $p \in M$.

2. A *Tutte-Grothendieck set invariant* f is a function (with values in some set S) for which $f(M_1) = f(M_2)$ whenever $t(M_1) = t(M_2)$.

3. A *generalized Tutte-Grothendieck invariant* is one with values in an R-module in which axiom T1 is replaced by

T1'. $f(M) = af(M-p) + bf(M/p)$ for elements a and b in R (independent of M) and nonfactors $p \in M$.

4. A *geometric Tutte-Grothendieck (group) invariant* f is one which is defined for combinatorial geometries (matroids without loops or multiple points) G and which obeys

$T1_G$. $f(G) = f(G-p) + f(\overline{G/p})$ for any $p \in G$ which is not an isthmus, where $\overline{G/p}$ is the canonical combinatorial geometry associated with G/p. In $\overline{G/p}$ multiple points of G/p are identified, and it is characterized by its lattice of closed sets which is isomorphic to the interval $[p, 1]$ in the lattice of closed sets of G. It is the contraction studied by Crapo and Rota [60].

5. A *geometric Tutte-Grothendieck ring invariant* f is one which obeys $T1_G$ and

$T2_G$. $f(G) = f(G-p)\cdot f(p)$ for any isthmus $p \in G$.

Combinations of the above may also be defined in the obvious way (e.g., a geometric Tutte-Grothendieck set invariant). In the following, we will use acronyms such as T-G for Tutte-Grothendieck, etc. We now explore these invariants in more detail. First, we give the commutative diagram equivalent to (3.7) for (3.8.1) and (3.8.2).

In the following, $t(M) = \sum_{i,j} b_{ij} x^i y^j$

Proposition 3.9 Let G be the free abelian group generated by the set of matroid isomorphism classes M with $i : M \to G$ the obvious map. Further, let S be the subgroup of G generated by elements of the form $i(M)-i(M-p)-i(M/p)$. Then $G/S \simeq \mathrm{FAG}[\ldots,x^i y^j,\ldots]$, the integer polynomial ring $\mathbb{Z}[x,y]$ viewed as a free abelian group.

The Tutte polynomial $t : \mathcal{M} \to \mathcal{G}/\mathcal{S}$ serves as a universal T-G group invariant in the following commutative diagram:

$$\begin{tikzcd}
 & \mathcal{G} \cong \mathrm{FAG}[\mathcal{M}] \arrow[dr, "\varepsilon"] & \\
\mathcal{M} \arrow[ur, "i"] \arrow[rr, "t"] \arrow[dr, "h"'] & & \mathcal{G}/\mathcal{S} \cong \mathrm{FAG}[\dots,x^iy^j,\dots] \arrow[dl, dashed, "e"] \\
 & G &
\end{tikzcd}$$

Here, h is any T-G group invariant into an abelian group G, while e is evaluation on totally separable matroids:

$$f(M) = t(M)\Big|_{x^iy^j \to f(B^{ij})}$$

$$= \sum_{i,j} b_{ij} f(B^{ij})$$

where B^{ij} is the matroid consisting of i isthmuses and j loops.

Proof. See [26] or [27].

Proposition 3.10 Let $\mathcal{T}$ be the set of all Tutte polynomials. Then we have the following commutative diagram

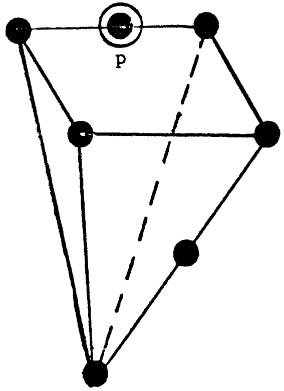
$$\begin{tikzcd}
\mathcal{M} \arrow[r, "s"] \arrow[d, "f"'] & \mathcal{M}\Big/\begin{array}{l} M_1 \sim M_2 \\ \text{if } t(M_1) = t(M_2) \end{array} \cong \mathcal{T} \arrow[dl, dashed, "f'"] \\
\mathcal{S} &
\end{tikzcd}$$

where s is the canonical surjection, and, for any T-G set invariant $f : M \to S$, there is a unique function f' with $f = f' \circ s$. Thus, f' (in theory) can be calculated from the coefficients $\{b_{ij}\}$ in t(M):

$$f(M) = f'(b_{00}, b_{10}, b_{01}, b_{20}, b_{11}, b_{02}, \ldots)$$

Clearly, any T-G ring invariant is also a T-G group invariant, and any T-G group invariant or generalized T-G invariant is a T-G set invariant. An example of a T-G group (but not ring) invariant is b_{10}, the coefficient of x in t(M) called the *Crapo beta invariant* which we will discuss later. An example of a set (but not group) invariant is the rank of M, r(M), where $r(M) = \max(i : b_{ij} \neq 0)$.

Example 3.11 Let M' be the matroid consisting of the seven points as pictured placed on a square pyramid:



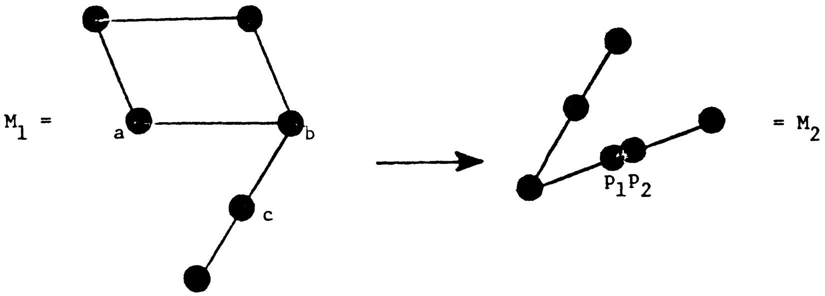
When the circled point (p) is deleted and contracted, we get the two matroids on the second line of Example 3.4. Thus, $M-p \simeq M'-p$, and $M/p \simeq M'/p$, where M is the matroid of (3.4). Hence, $t(M) = t(M')$, while $M \neq M'$. Therefore, an example of an invariant which is not a

T-G set invariant is the characteristic function $\chi_{M'}$:

$$\chi_{M'}(G) = \begin{cases} 1 & \text{if } G \cong M' \\ 0 & \text{otherwise.} \end{cases}$$

Another example is the number of three-point planes of a matroid, since M has five three-point planes while M' has six.

This example points out one way of constructing non-isomorphic matroids with the same Tutte polynomial. We relate this fact to another matroid concept: the strong map. If M_1 and M_2 are two matroids on the same set such that $r(M_2) = r(M_1)-1$, and such that each closed subset of M_2 is closed in M_1, then there is a matroid M with $M-p \cong M_1$ and $M/p \cong M_2$. The matroid M is determined up to isomorphism not just by the structure of M_1 and M_2, but also the action of the strong map (i.e. the labeling) needs to be taken into account. For example, consider the two strong maps $M-p \to M/p$ and $M'-p \to M'/p$ of (3.4) and(3.11) respectively.



(3.11')

The inverse image of the double point $\{p_1,p_2\}$ is the two-point line $\{a,d\}$ in Example 3.4, and the two-point line $\{b,c\}$ in in Example 3.11. Since no automorphism of M_1 takes $\{a,d\}$ to $\{b,c\}$, we have $M \neq M'$.

Another perspective on T-G set invariants is to define two related classes of invariants (I_2 and I_3 below):

<u>Proposition 3.12</u> Let I_0 be the class of (generalized) T-G invariants (3.8.3), and I_1 be the class of T-G set invariants.

Let I_2 be the class of invariants $f : \mathcal{M} \to S$ for which there exists a function $f_2 : \mathcal{S} \times \mathcal{S} \to \mathcal{S}$ such that

$$f(M) = f_2(f(M-p),\ f(M/p)) \quad \text{for any nonfactor } p.$$

Let I_3 be the class of invariants f for which there exists a function f_3 defined on (isomorphism classes of) matroid pairs such that

$$f(M) = f_3(M-p, M/p) \quad \text{for any nonfactor } p.$$

Then:

1. $I_3 \supsetneq I_1$.

2. $I_3 \supsetneq I_2$.

3. $I_1 \cap I_2 \supsetneq I_0$.

4. $(I_1 \cap I_2) - I_0$ contains, for example, the cardinality function $f(M) = |M|$.

5. $I_3 - (I_1 \cup I_2)$ contains, for example, the characteristic function of the desarguesian projective plane of order 9.

6. $I_1 - I_2$ contains, for example, the characteristic function of the three-point line.

7. The characteristic function of the matroid M of (3.4) is an invariant not in I_3.

Proof. 1. If $f(M) = f_1(t(M))$, let $f_3(M-p, M/p) = f_1(t(M-p) + t(M/p))$.

2. Let $f_3(M-p, M/p) = f_2(f(M-p), f(M/p))$.

3. Let $f(M) = af(M-p) + bf(M/p)$. We will prove below in Proposition 3.20 that f is a set invariant. Further, $f \in I_2$ since we may define the function f_2 by $f_2(r,s) = ar + bs$.

4. We saw earlier (3.3.6) that the cardinality function, $|M|$, is a set invariant ($|M| = \log_2(t(M;2,2))$). It is in I_2 using, e.g., $f_2(r,s) = r + 1$. It is clearly not a generalized T-G invariant.

5. We will see below (Proposition 5.15.3) that $t(M_1) = t(M_2)$ if M_1 and M_2 are rank-three combinatorial geometries with the same number of atoms and i-point lines for all i. Thus, the Tutte polynomial can not distinguish two projective planes of order nine. However, if M is the desarguesian plane, M-p is independent of p and contains 81 ten-point lines as well as 10 nine-point lines. M may be reconstructed up to isomorphism from M-p by placing p on the intersection of the nine-point lines since the contraction M/p consists of a line with ten points each of multiplicity nine iff p is on 10 ten-point lines in M. A straightforward argument then shows that if f_M is the characteristic function of M, then $f_M(M') = f_{M-p}(M'-p) \cdot f_{M/p}(M'/p)$ for all M' and p.

6. A three-point line L is the only matroid with Tutte polynomial

$x^2 + x + y$. Its characteristic function, χ_L, is certainly not in I_2 since $(\chi_L(L-p), \chi_L(L/p)) = (0,0) = (\chi_L(M-p), \chi_L(M/p))$ for almost all matroids M. (Similarly, of course, the invariant f_M in 3.12.5 is not in I_2.)

7. This was shown in (3.11).

An open problem is whether I_2 is contained in I_1. As a means of attacking the problem, we formulate it in a different manner.

Define the equivalence relation ~ on matroids recursively generated by the following relations:

E1. $M \sim M'$ if $M \simeq M'$

(3.12') E2. $M \sim M'$ if there is a nonfactor $p \in M$ and a nonfactor $q \in M'$ with $(M-p) \sim (M'-q)$ and $M/p \sim M'/q$.

Note that since both E1 and E2 are symmetric and reflexive, we need only take the transitive closure of the relations E1 and E2. Also, it is inductively well-defined, since we may determine how the equivalence relation behaves on matroids of cardinality K by knowing how it behaves on matroids of cardinality K-1.

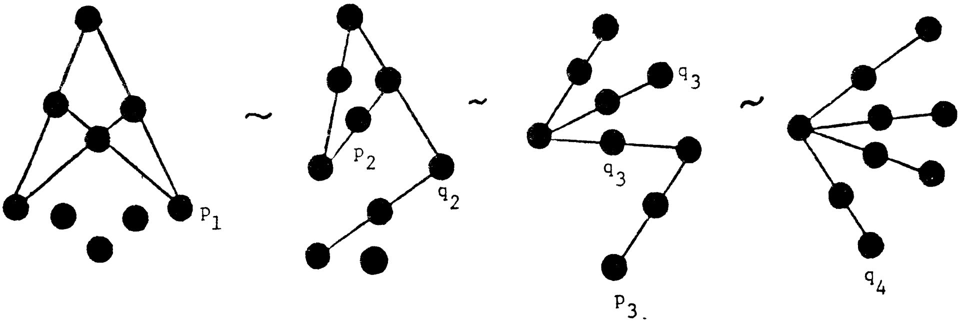
Further, if $G \sim H$ then $t(G) = t(H)$ since the latter equivalence relation ("having the same Tutte polynomial") satisfies E1 and E2.

<u>Proposition 3.13</u> The class of invariants I_2 is contained in the class of invariants I_1 if and only if $M \sim M'$ for all matroid pairs such that $t(M) = t(M')$.

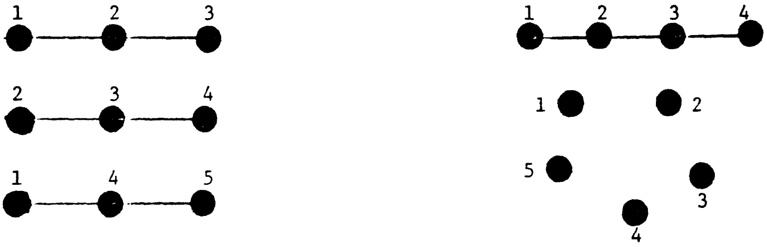
Proof. On M, define $f(M)$ to be the equivalence class of M under the relation $\sim$. We claim that f is an I_2-invariant. In fact, define $f_2(A,B)$ to be the equivalence class C containing M'' such that $f(M''-p) = A$ and $f(M''/p) = B$. Conditions E1 and E2 guarantee that the map $M \to f_2(f(M-p), f(M/p))$ is well defined. If $t(M) = t(M')$ for $M \not\sim M'$, we have $f(M) \neq f(M')$, and f is an I_2-invariant which is not an I_1-invariant.

Conversely, we will show that if, for all M and M', $t(M) = t(M')$ implies $M \sim M'$, then $t(M) = t(M')$ implies $f(M) = .f(M')$ for any I_2-invariant f. (The proof essentially rests on an argument that the function defined above which takes M to its equivalence class under $\sim$ is a universal I_2-invariant.) For a direct, inductive, proof, assume that $t(M) = t(M')$ implies $f(M) = f(M')$ for all matroids on K points, where f is an I_2-invariant with associated function f_2. Let M and M' have cardinality $K + 1$ with $t(M) = t(M')$. By assumption, $M \sim M'$, so there is a chain $M \simeq M_1 \sim M_2 \sim M_3 \sim \ldots \sim M_t \simeq M'$, with each equivalence given by E2. (The chain is finite since there are only a finite number of nonisomorphic matroids on $K + 1$ points.) For each i, there exist nonfactors p_i and q_{i+1} such that $(M_i-p_i) \sim (M_{i+1}-q_{i+1})$ and $M_i/p_i \sim M_{i+1}/q_{i+1}$. Thus, $t(M_i-p_i) = t(M_{i+1}-q_{i+1})$ and $t(M_i/p_i) = t(M_{i+1}/q_{i+1})$. Using the induction hypothesis, $f(M_i-p_i) = f(M_{i+1}-q_{i+1})$, and $f(M_i/p_i) = f(M_{i+1}/q_{i+1})$. Thus, since the arguments are the same in both cases, $f_2(f(M_i-p_i), f(M_i/p_i)) = f_2(f(M_{i+1}-q_{i+1}), f(M_{i+1}/q_{i+1}))$ for all i. Hence, $f(M) = f(M')$.

Exercises 3.14 1. We illustrate a chain of E2-equivalences for two rank-three matroids M_1 and M_4 with $t(M_1) = t(M_4)$. In each case verify that $(M_i-p_i) \simeq (M_{i+1}-q_{i+1})$, and $M_i/p_i \simeq M_{i+1}/q_{i+1}$.



2. The reader may verify that the rank-three matroids M and M' below have the same Tutte polynomials by exibiting an E2-chain between them. Each point is labeled with its multiplicity:



3. Show that there are no other essentially different strong maps $M_1 \rightarrow M_2$ in (3.11'), and, in fact, no other matroid M" with

$$t(M") = t(M) \quad \text{and} \quad M" \neq M,M'.$$

We now turn our attention to geometric T-G invariants (3.8.4) and (3.8.5). We show that, in fact, they are a special case of T-G (matroid) invariants. Consider any invariant f on combinatorial geometries and define $\bar{f}$ on matroids by:

$$(3.15')\quad \bar{f}(M) = \begin{cases} 0 \text{ if } M \text{ has a loop} \\ f(\bar{M}) \text{ otherwise, where } \bar{M} \text{ is the canonical} \\ \text{geometry associated with } M \text{ (with multiple} \\ \text{points identified).} \end{cases}$$

Similarly, let g be any invariant which is zero on matroids with loops, and such that $g(M) = g(M')$ when M and M' have the same canonical geometry. Then, clearly, there is a unique invariant f on geometries such that $\bar{f} = g$.

Proposition 3.15 The following are equivalent, where f and $\bar{f}$ are two invariants related by (3.15'),

1. f is a geometric T-G group (ring) invariant. Thus, f satisfies $T1_G$ (and $T2_G$).

2. $\bar{f}$ is a T-G group (ring) invariant with $\bar{f}(M) = 0$ if M contains a loop.

3. $\bar{f}$ is a T-G group invariant with $\bar{f}(B^{ij}) = 0$ for $j > 0$. ($\bar{f}$ is a T-G ring invariant with $\bar{f}(\text{loop}) = 0$).

Proof. We first show that for a T-G invariant $\bar{f}$, $\bar{f}(M) = 0$ whenever M has a loop if and only if $\bar{f}(M') = \bar{f}(\bar{M}')$ for any loopless matroid M' where $\bar{M}'$ is the canonical geometry. In one direction this follows from the fact that if p is a point of M' which depends on another point q (but is not a loop), then p is a nonfactor, and q is a loop of M/p. Therefore $\bar{f}(M'/p) = 0$ and

$$\bar{f}(M') = \bar{f}(M'-p) + \bar{f}(M'/p) = \bar{f}(M'-p).$$

Continuing in this matter with any multiple point, we eventually obtain $\bar{f}(M') = \bar{f}(\bar{M}')$. On the other hand, assume for all loopless matroids M', $\bar{f}(M') = \bar{f}(\bar{M};)$. For any matroid M with a single loop p, let M'' be the matroid $(M-p) \oplus M'$ where M' is the multiple point $\{q,q'\}$. Then q is a nonfactor, and

$$\bar{f}(M'') = \bar{f}(M''-q) + \bar{f}(M''/q).$$

But $\overline{M''} = \overline{M''-q}$, and $M''/q \simeq M$. Thus, $\bar{f}(M) = 0$. For k loops, we direct sum with a multiple $(k+1)$-point and proceed by induction using the above argument.

Now, assume f satisfies $T1_G$ and define $\bar{f}$ on matroids from (3.15'). We must show that for any matroid,

$$(*) \qquad \bar{f}(M) = \bar{f}(M-p) + \bar{f}(M/p).$$

If M has a loop all terms are 0, so assume M is loopless. If p is in a multiple point, $\bar{f}(M/p) = 0$ while $\bar{M} = \overline{M-p}$. If p is not a multiple point, M/p is loopless, $\overline{M-p} = \bar{M}-p$, and $\bar{M}/p = \overline{M/p}$. Thus,

$$\begin{aligned}\bar{f}(M) = f(\bar{M}) &= f(\bar{M}-p) + f(\overline{\bar{M}/p}) \\ &= \bar{f}(M-p) + \bar{f}(M/p).\end{aligned}$$

Conversely, if $\bar{f}$ satisfies $T1$ and is zero on loops, define f from $\bar{f}$ by (3.15'). Then, for any geometry G and nonfactor p, we have

$$f(G) = \bar{f}(G) = \bar{f}(G-p) + \bar{f}(G/p)$$

$$= f(G-p) + f(\overline{G/p}).$$

Thus, f satisfies $T1_G$ and (3.15.1) is equivalent to (3.15.2), in the group case.

We now show that (3.15.2) and (3.15.3) are equivalent in the group case. The case of ring invariants is treated similarly. Since B^{ij} has a loop if and only if $j > 0$, any T-G invariant which is zero on matroids with loops must be zero on all B^{ij} with $j > 0$. Conversely, assume g is a T-G group invariant with $g(B^{ij}) = 0$ for all $j > 0$. If M has a loop, then the coefficients b_{ij} in t(M) are zero whenever $j = 0$. Thus

$$g(M) = \sum_{j>0} b_{ij} g(B^{ij}) = 0.$$

Corollary 3.16 The *geometric Tutte polynomial:*

$$\bar{t}(G) = \sum_i b_{i0} x^i = t(G;x,0)$$

is a universal invariant for $T1_G$ (and $T2_G$). In particular, for any geometric T-G group invariant f:

$$f(G) = \sum_i b_{i0} f(B^{i,0})$$

where $B^{i,0}$ is the boolean algebra with i isthmuses. Further, if g is a geometric T-G ring invariant, then

$$g(G) = t(G;g(I),0)$$

where I is an isthmus. (For simplicity, we will henceforth use B^i to denote the boolean algebra $B^{i,0}$, and b_i to be the coefficient b_{i0}.)

A consequence of (3.1) and (3.2) is that the corank-nullity polynomial S(M) is a universal T-G group or ring invariant. By (3.16), t(G;x,0) is a universal T-G geometric (group or ring) invariant and thus any geometric T-G invariant can be evaluated from S(M;u,-1). However, there is a more intrinsically appealing universal geometric invariant derived from S(M), the *characteristic (or Poincaré) polynomial* of a matroid, $\chi(M)$. We also give a two-variable generalization $\bar{\chi}(M)$ called the *coboundary polynomial* by Crapo when he introduced it [56] as a generalization of Tutte's work on graphs [142]. We also define the cardinality-corank polynomial as a connection between S(M) and $\bar{\chi}(M)$.

Definition 3.17 Let M be a matroid of rank n on the set S with L(M) the geometric lattice of flats of M.

1. The *cardinality-corank polynomial* $S_{KC}(M)$ is given by

$$S_{KC}(M;z,u) = \sum_{A\subseteq S} z^{|A|}u^{\mathrm{cor}(A)}$$

$$= \sum_{i,j} a_{ij}z^i u^j$$

where $a_{ij}(M)$ is the number of subsets A of S, with i points and corank j (so that $r(A) = n-j$).

2. The *characteristic polynomial* $\chi(M)$ is defined as:

$$\chi(M;\lambda) = \begin{cases} 0 \text{ if } M \text{ contains a loop} \\ \sum_{x\in L(M)} \mu(0,x)\lambda^{\mathrm{cor}(x)} = \\ \sum_{i=0}^{n} w_i\lambda^{n-i} \quad \text{otherwise} \end{cases}$$

where $\mu(0,x)$ is the Möbius function in $L(M)$ of the interval $[0,x]$ (0, the zero of $L(M)$, is the empty (closed) set). The coefficients $\{w_i\}$ of $\chi(M)$ are called the *Whitney numbers of the first kind* of M and will be studied in section six.

3. The *Poincaré polynomial* of M is given by

$$\bar{\chi}(M;u,\lambda) = \sum_{x\in L(M)} u^{|x|}\chi([x,1],\lambda)$$

$$= \sum_{\substack{x,y\in L(M):\\ x\le y}} u^{|x|}\lambda^{\operatorname{cor}(y)}\mu(x,y) \quad .$$

Here, the interval $[x,1]$ is an upper interval in $L(M)$ and is the geometric lattice of the contraction M/x.

Proposition 3.18 We have the following relations for a matroid M of rank n:

1. $S_{KC}(z,u) = z^n S(\frac{u}{z},z)$

2. $\bar{\chi}(u,\lambda) = S_{KC}(u-1,\lambda)$

3. $S_{KC}(z,u) = z^n t(\frac{u+z}{z}, z+1)$

4. $\bar{\chi}(u,\lambda) = (u-1)^n t(\frac{u+\lambda-1}{u-1},u)$

5. $\chi(\lambda) = (-1)^n t(1-\lambda,0)$.

Proof. The first identify is immediate. The second follows from the fact that in any lattice, $\mu(0,1) = \Sigma(-1)^{|A|}$, where the sum is over all subsets A of atoms whose supremum is 1 (see [118]), and, hence, in a loopless matroid, $\mu(0,x) = \Sigma(-1)^{|B|}$ where the sum is over all sets of points B such that $\bar{B} = x$. (A complete proof can be found in [56] or [37].) The third identity follows from (3.18.1) and (3.3.1). Identity (3.18.4) follows from (3.18.2) and (3.18.3), and in turn implies (3.18.5) by setting $u = 0$.

From (3.18.5) and (3.16), we may deduce the following.

Corollary 3.19 1. If f is a geometric T-G ring invariant, then:

$$f(G) = (-1)^{r(G)}\chi(G;1-f(I)) \quad \text{where } I \text{ is an isthmus.}$$

2. If f is a geometric T-G group invariant, then

$$f(G) = (-1)^{n} \sum_{i} (-1)^{i}(\sum_{j} \binom{n-j}{i} w_{j}) f(B^{i})$$

where $n = r(G)$, and B^{i} is the i-point boolean algebra.

So far, in this section, we have shown that from the Tutte polynomial of a matroid we may evaluate any invariant which obeys either of the additive recursions T1 or $\mathrm{T1}_G$. The reader may ask himself why we went into such detail for invariants satisfying T1 and have thus far neglected invariants which satisfy T1', the generalized additive recursion, especially in view of the fact that the invariants χ_i of section two all satisfied a recursion of this type (with $a = 1$, $b = -1$). The reason is that the Tutte polynomial allows us to evaluate these invariants also without developing a more general theory. The following proposition (3.20.2) first appeared explicitly (for ring invariants) in [116] but is implicit in [27] and [75].

Proposition 3.20 Let f be an invariant with values in an R-module P such that for all matroids M and nonfactors $p \in M$,

T1'. $f(M) = af(M-p) + bf(M/p)$ for fixed elements a and b of R.

Then,

1. $f(M) = \sum_{i,j} b_{ij} \cdot a^{\mathrm{nul}(M)-j} \cdot b^{r(M)-i} \cdot f(B^{ij})$ (where, as usual, b_{ij} is the coefficient of $x^i y^j$ in $t(M)$).

2. If f, in addition, satisfies T2 (here $R=P$), then

$$f(M) = a^{\mathrm{nul}(M)} \cdot b^{r(M)} \cdot t(M; \frac{f(I)}{b}, \frac{f(L)}{a}).$$

3. If f is a geometric ring invariant which satisfies T1'$_G$. $f(G) = f(G-p) + bf(\overline{G/p})$, then

$$f(G) = b^{r(G)} \cdot t(G; \frac{f(I)}{b}, 0).$$

Proof. 1. Let $f'(M)$ denote the right-hand side of (3.20.1). Since $t(B^{ij}) = x^i y^j$, for totally separable matroids, we have only one nonzero term in the summation: $f'(B^{ij}) = a^{j-j} b^{i-i} f(B^{ij}) = f(B^{ij})$. It now suffices for an inductive proof to show that f' obeys T1'. Let $t(M-p) = \Sigma b'_{ij} x^i y^j$, and $t(M/p) = \Sigma b''_{ij} x^i y^j$. Then:

$$\begin{aligned} af'(M-p) + bf'(M/p) &= a(\Sigma b'_{ij} a^{\mathrm{nul}(M-p)-j} b^{r(M-p)-i} \cdot f(B^{ij})) \\ &\quad + b(\Sigma b''_{ij} a^{\mathrm{nul}(M/p)-j} \cdot b^{r(M/p)-i} \cdot f(B^{ij})) \\ &= \Sigma a^{\mathrm{nul}(M)-j} b^{r(M)-i} \cdot (b'_{ij} + b''_{ij}) f(B^{ij}) \\ &= f'(M). \end{aligned}$$

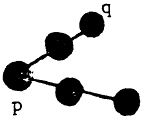
2. If f obeys T2, then $f(B^{ij}) = (f(I))^{i}(f(L))^{j}$, so that

$$f'(M) = a^{\mathrm{nul}(M)}b^{r(M)} \sum_{i,j} b_{ij}\left(\frac{f(I)}{b}\right)^{i}\left(\frac{f(L)}{a}\right)^{j}$$

$$= a^{\mathrm{nul}(M)}b^{r(M)}t(M;\ \frac{f(I)}{b},\ \frac{f(L)}{a}).$$

3. Define $\bar{f}$ from f as in (3.15'). Then, as in the proof of (3.15), $\bar{f}$ is a matroid invariant which obeys T1' with $a = 1$. The rest of the proof imitates (3.15).

We note that there is no more general geometric analog for T1' when $a \neq 1$. One reason for this is that $\mathrm{nul}(\overline{G/p})$ cannot be calculated from $\mathrm{nul}(G)$. Thus, the Tutte-Grothendieck ring for the recursion $f(G) = af(G-p) + bf(\overline{G/p})$ is not a polynomial ring. The reader may easily verify this by decomposing the matroid

G =


in two different ways. Starting with p, we obtain

$$f(G) = af(\colon\ \colon) + bf(\cdot\ \ \cdot)$$

$$= a^{2}f(B^{3}) + (a^{2}b+b)f(B^{2}) + ab^{2}f(B^{1}).$$

First deleting and contracting q, we obtain:

$$f(G) = a^{2}f(B^{3}) + 2abf(B^{2}) + b^{2}f(B^{1}).$$

We also note that every step in the proofs of section two have been verified since, for all i,

$$\chi_i(M) = (-1)^{r(M)} t(M;-1,0).$$

In those arguments, M was always binary but this affords no problem since the entire theory of this section holds when M is replaced by any *hereditary subclass* M' of matroids (where if $M \approx M'$, and M is in M', so are M', M-p, and M/p).

Research Problems 3.21. 1. When a matroid M on K points is decomposed as in (3.4), what is the expected number of nonisomorphic matroids which appear in the decomposition? (An upper bound is 2^K, but this is too high. As our example shows, partial decompositions can be combined.) Note that if this number can be shown to be always p(K) for graphic matroids and a polynomial p, then results in Part II will show that all nondeterministic polynomial algorithms have a polynomial counterpart if there is a polynomial check for graph isomorphism (i.e., the graph isomorphism problem is NP-complete).

2. Is the equivalence relation (3.12') the same as Tutte equivalence? In particular, are all projective planes of order n equivalent? If we modify (3.12') for geometries specifying that $\overline{M/p} \sim \overline{M'/q}$, does this correspond to having the same chromatic polynomial?

3. Characterize algebraically the "Tutte-Grothendieck ring" for invariants which satisfy $T1'_G$ in (3.20.3) for $a \neq 1$.

4. Matroid Constructions

In this section, we will review some basic matroid operations and show how they affect the Tutte polynomial. Of course, the prototypical operations for which the Tutte polynomial can be computed are duality: $(t(G^*;x,y) = t(G;y,x))$, and direct sum: $(t(G\oplus H) = t(G)\cdot t(H))$. We will see that for other operations (such as truncation), the Tutte polynomial can be calculated directly from the polynomial(s) of the operand(s) or from related polynomials. First, we treat the operation of adding a point in general position.

Definition 4.1 For a matroid $M(S)$ the *free extension* of M by a point p, $M + p$, is the matroid on the set $S \cup p$ whose independent sets are the independent sets of M along with subsets consisting of p, along with any independent nonbasis of M. It is related to the *truncation* of M in the following way: $T(M) = (M+p)/p$, while $M+p = T(M\oplus p)$. $T(M)$ is most easily described by its closed sets which consist of the closed sets of M except for the hyperplanes. It is not defined if $r(M) = 0$. The free coextension of M by p, $M \times p$, is defined by $M \times p = (M^* + p)^*$.

Proposition 4.2 If $t(M) = \Sigma b_{ij}x^iy^j$, we have the following formulas:

1. $t(M+p) = \sum_j \left[b_{0j}y^{j+1} + \sum_{i>0} b_{ij}(x^i+x^{i-1}+\ldots+x+y)y^j\right].$

2. $t(T(M)) = \sum_j \left[b_{0j}(y^{j+1}-y^j) + b_{1j}y^{j+1} + \sum_{i>1} b_{ij}(x^{i-1}+x^{i-2}+\ldots+ x + y)y^j\right].$

3. $t(M\times p) = \sum_i \left[b_{i0}x^{i+1} + \sum_{j>0} b_{ij}x^i(y^j + y^{j-1} + \ldots + y + x\right].$

Proof. 1. It should be familiar by now that many identities involving the Tutte polynomial may be proved by showing that the identity holds for totally separable matroids M and are "linear" in that they are preserved under deletion-contraction decomposition by nonfactors. If $M = B^{ij}$, then $M+p$ is an $(i+1)$-element circuit along with j loops. Thus, its Tutte polynomial is $(x^i + x^{i-1} + \ldots + x + y)y^j$ if $i > 0$ and y^{j+1} otherwise. In any case (4.2.1) holds. If q is a nonfactor of M, it remains so in $M+p$. Further, $(M+p)-q = (M-q)+p$, and $(M+p)/q = (M/q)+p$. It is then an easy matter to show that (4.2.1) holds for $M+p$ when it does for $(M+p)-q$ and $(M+p)/q$.

2. $t(T(M)) = t((M+p)/p) = t(M+p) - t((M+p)-p) = t(M+p)-t(M)$. Thus, we may subtract $t(M)$ from the right-hand side of (4.2.1).

Formula (4.1.3) follows from (4.1.1) by duality (see 3.3.7), as docs a formula for the *free lift*, $FL(M) = (T(M^*))^*$.

Example 4.3 1. Let M_1 be the matroid consisting of two intersecting three-point lines. Then
$$t(M_1) = x^3 + 2x^2 + x + 2xy + y + y^2,$$
and $t(M_1+p) = t(M_1) + t(L_5) = t(M_1) + x^2 + 3x + 3y + 2y^2 + y^3$. Here, $L_5 = T(M_1)$ is a five-point line. The reader easily checks that $t(M_1+p) = t(M_2)$, where M_2 is the six-point rank-three matroid consisting of two (parallel) three-point lines. In fact, they are the unique smallest pair of nonisomorphic matroids with the same Tutte polynomial. These examples have the following consequences:

- One cannot tell from $t(M)$ whether M contains a point in free position.

- $t(E(M))$ cannot be calculated from $t(M)$, where $E(M)$ is the "adjoint" operation of truncation: the free erection of Crapo [58]. In fact, $t(E(M_1+p)) = t(M_1 \oplus p) = xt(M_1)$, which is not equal to $t(E(M_2)) = t(L_3 \oplus L_3) = (x^2+x+y)^2$.

2. We cannot even determine from $t(M)$ whether M has a non-trivial erection. For example, let $S = \{a,b,c,d,A,B,C,D\}$ and let $M_1(S)$ and $M_2(S)$ be two rank-four combinatorial geometries both of which have as dependent flats: S and hyperplanes aAbB, bBcC, cCdD, dDaA, and aAcC. Further, assume M_1 has the additional dependent hyperplane bBdD, while M_2 has the additional dependent hyperplane abcd. Then, M_1 is erectable, while M_2 is not, but results from the next section (5.15.3) show that $t(M_1) = t(M_2)$.

Another operation which we have studied is the forming of the canonical geometry $\bar{M}$, where loops of a matroid M are eliminated, and multiple points identified. Information about $t(\bar{M})$ is contained in the following proposition and example.

Proposition 4.4

1. $r(M) = \max_{b_{ij}>0} (i)$. (Dually, $\mathrm{nul}(M) = \max_{b_{ij}>0} (j)$.)

2. If $r(M) = n$, then $b_{nj} = \delta(j,m)$, where M contains m loops. (Dually, if $\mathrm{nul}(M) = k$, then $b_{jk} = \delta(j,i)$, where M contains i isthmuses.)

3. Let M' be the matroid M with its loops removed. Then, $t(M') = t(M)/y^m$ where $b_{nm} = 1$ and $b_{ij} = 0$ for all $i > n$ and all j.

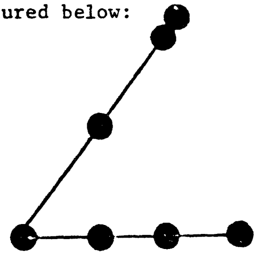
4. $\bar{t}(\bar{M}) = \bar{t}(M') = t(M';x,0)$.

5. Although $\bar{t}(\bar{M})$ can be calculated from $t(M)$ (and, in fact, from $\bar{t}(M)$ when M is loopless), $t(\bar{M})$ cannot be determined in general from $t(M)$.

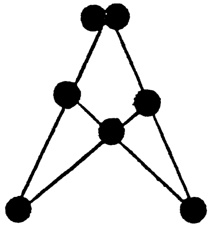
Proof. The first three statements are easily proved by deletion-contraction. (4.4.4) is Corollary 3.16, while (4.4.5) follows from (4.4.3), (4.4.4), and Example 4.5 below.

Example 4.5 1. The duals M^* and M'^* of the matroids in (3.11) are pictured below:

$M'^* =$



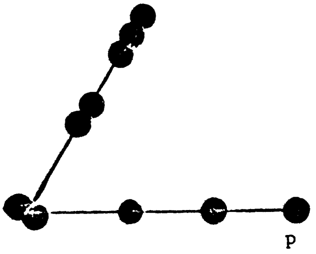
$M^* =$



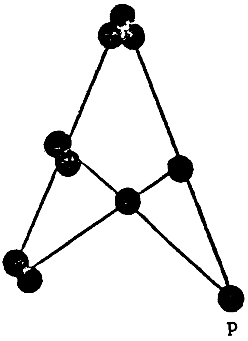
They have the same Tutte polynomial and $\bar{t}(\overline{M'^*}) = \bar{t}(\overline{M^*}) = x(x+1)(x+2)$. However, the reader may readily check that $t(\overline{M'^*}) \neq t(\overline{M^*})$.

2. The above matroids may be modified to obtain other matroid pairs with identical Tutte polynomials. Deleting and contracting p we can see that $t(M_1) = t(M_2)$ for the following matroids:

$M_1 =$



$M_2 =$



Another important operation is the matroid union of Edmonds and Fulkerson [69] and Nash-Williams [106]: $M_1(S) \vee M_2(S) = (M_1 \vee M_2)(S)$, where the independent sets of $M_1 \vee M_2$ are subsets of S which can be partitioned into independent subsets of M_1 and M_2 respectively. Clearly, nothing can be said about $t(M_1 \vee M_2)$ in general from $t(M_1)$ and $t(M_2)$, since different orderings on the points of M_2 don't change $t(M_2)$ but do result in vastly different matroid unions. We might, however, ask about $M \vee M$. That $t(M \vee M)$ cannot in general be recovered from $t(M)$ can be checked by the reader by counting the number of subsets of size five and rank four in $M_1 \vee M_1$ and $M_2 \vee M_2$ respectively in (4.5.2). However, $r(M \vee M)$ can be recovered from $t(M)$. The result was motivated by remarks of Las Vergnas [92].

Proposition 4.6 Let $M(S)$ be a matroid with $t(M) = \Sigma b_{ij} x^i y^j$. The rank of the union of M with itself is given by:

$$r(M \vee M) = |S| + r(M) - \max_{b_{ij}>0} (i+j)$$

$$= 2 \max_{b_{ij}>0} (i) + \max_{b_{ij}>0} (j) - \max_{b_{ij}>0} (i+j).$$

First Proof. Note that $\max_{b_{ij}>0} (i+j) = \max_{a_{ij}>0} (i+j)$, where a_{ij} is the number of subsets of M of corank i and nullity j (3.2, 3.3). It is then an easy application of the formula for the rank function of $M \vee M$ to show that

$$\begin{aligned}\max_{a_{ij}>0} (i+j) &= \max_{A\subseteq S} (|A| - r(A) + r(M) - r(A)) \\ &= r(M) - \min_{A\subseteq S} (2r(A) - |A|) \\ &= |S| + r(M) - \min_{A\subseteq S} (2r(A) + |S-A|) \\ &= |S| + r(M) - r(M\vee M).\end{aligned}$$

Second Proof. A second method of proof is by our standard method of deletion-contraction. Note that one way of interpreting both proofs is that, together, they give a deletion-contraction proof that $r(M\vee M) = \min_{A\subseteq S} (2r(A) + |S-A|)$. If $M = B^{ij}$, then $t(M) = x^i y^j$, $M\vee M = B^{ij}$, and $r(M\vee M) = i = 2i+j - (i+j)$ which is the right-hand side of (4.6). Now, let $f_1(M) = |S| + r(M)$. For any nonfactor q, the triple $(f_1(M-q), f_1(M/q), f_1(M))$ is equal to $(r,r-1,r+1)$ for some r. Similarly, if $f_2(M) = \max_{b_{ij}>0} (i+j)$, the triple $(f_2(M-q), f_2(M/q), f_2(M))$ will take one of the forms $(m,m+1,m+1)$, $(m+1,m,m+1)$, or (m,m,m) for some m. The reason for this is that $\max_{b'_{ij}>0} (i+j)$ in $t(M-p)$ can never differ by more than one from $\max_{b''_{ij}>0} (i+j)$ in $t(M/p)$. In fact, for any subset $A \subseteq S-p$, $f(A) = \text{cor}(A) + \text{null}(A)$ always differs by one in $M-p$ and M/p. If $p \in \bar{A}$ (in M), then A has the same corank in both M/p and $M-p$, while its nullity is one more in M/p. If $p \notin \bar{A}$, the nullities are equal, but the corank of A is one less in M/p. Combining these two invariants, we see that

$f_1 - f_2$ obeys one of the following triples: (k,k-2,k), (k-1,k-1,k), or (k,k-1,k+1) for appropriate k (=r-m). We will be done when we show that r(MvM) obeys the same recursion. Note that, in any case, $r(M/q \vee M/q) \leq r(M-q \vee M-q) \leq r(M/q \vee M/q) + 2$. By definition, r(MvM) equals the size of the union of two maximally disjoint bases of M. Call them B and B'. Consider the three possible triples in turn.

(k,k-2,k). This is the case when there exist such bases B and B' such that $q \notin B \cup B'$.

(k-1,k-1,k). This is when there exist such B and B' with $q \in B \cap B'$.

(k-1,k-2,k). For all such B and B', $q \in B-B'$ or $q \in B'-B$.

Details are left to the reader. Note that, for example, the first two cases are mutually exclusive: if $q \in B_1 \cap B_2$ and $q \notin B_1' \cup B_2'$, then, by basis exchange, we could find two bases more disjoint (see Proposition 7 in [25]).

Certainly, if t(M) is known and $p \in M$, then one cannot, in general, compute either t(M-p) or t(M/p) (although their sum is known). One way to remedy this situation (see (4.8.2) and (4.8.3) below) is to be found in [24] where basepointed matroids were introduced.

<u>Definition 4.7</u> Let $\mathcal{M}_P$ denote the class of *pointed matroids*, where $M_q \in \mathcal{M}_P$ if M is a matroid, and q is a (distinguished) point of M. An invariant for the class of such pointed matroids is

a four-variable version of the Tutte polynomial $t_p(M_q;x',x,y',y)$, in which the point q is saved for last in the decomposition ordering used in the first proof of Theorem 3.1. We then may modify (3.1) to show that the *pointed Tutte polynomial* $t_p(M_q;x',x,y',y)$ may be defined such that:

$T1_P$. $t_P(M_q) = t_P(M_q-p) + t_P(M_q/p)$ if p is a nonfactor and $p \neq q$.

$T2_P$. $t_P(M_q) = t_P(M_q-p)\cdot t(p)$ if p is a factor and $p \neq q$.

$T3_P$. $t_P(q) = x'$ if q is an isthmus, and $t_p(q) = y'$ if q is a loop

In the above rules, $M_q-p = (M-p)_q$ is the matroid $M-p$ with distinguished point q. Similarly for $M_q/p = (M/p)_q$

Two important operations on pointed matroids are the *series connection* $S(M_q,M'_{q'})$ and the *parallel connection* $P(M_q,M'_{q'})$. The parallel connection is defined (following [24]) as the matroid pointed by $\bar{q}$ on the set $(M-q) \uplus (M'-q') \uplus \bar{q}$, whose closed sets are all sets of the form $A \cup A'$ or $B \cup B' \cup \{\bar{q}\}$ where A and $B \cup \{q\}$ are closed in M, while A' and $B' \cup \{q'\}$ are closed in M'. We may then define the series connection dually: $S(M_q,M'_{q'}) = (P(M^*_q,M'^*_{q'}))^*$. A related operation is the *two-sum* of Seymour [125]. For our purposes, we may define this operation as $P'(M_q,M'_{q'}) = P(M_q,M'_{q'}) - \bar{q}$.

We now list some useful facts, all of whose proofs may be found in [24] (except for (4.8.7) which follows from (4.8.2) and (4.8.5)).

Proposition 4.8 Let M_q and $M'_{q'}$ be pointed matroids on disjoint sets, where $q \in M$ and $q' \in M'$ are both nonfactors. Further, let $t_p(M_q) = x'f(x,y) + y'g(x,y)$, $t_p(M'_{q'}) = x' f'(x,y) + y' g'(x,y)$, L denote a loop, and I denote an isthmus. We have the following formulas:

1. $t(M) = xf(x,y) + yg(x,y)$.

2. $t(M_q - q) = (x-1)\cdot f + g \; (t(M_L - L) = g, \; t(M_I - I) = f)$.

3. $t(M_q/q) = f + (y-1)\cdot g \; (t(M_L/L) = g, \; t(M_I/I) = f)$.

4. $(x + y - xy)\cdot t_p(M_q) = x'\cdot(t(M/q) - (y-1)\cdot t(M-q)) +$
   $y'\cdot(t(M-q) - (x-1)\cdot t(M/q))$.

(Formulas 5, 6, and 7 below are valid with q = L or I, where, appropriately, f or g=0).

5. $t_p(P(M_q, M'_{q'})) = x'\cdot f\cdot f' + y'((y-1)\cdot g\cdot g' + f\cdot g' + g\cdot f')$.

6. $t_p(S(M_q, M'_{q'})) = x'((x-1)\cdot f\cdot f' + f\cdot g' + g\cdot f') + y'\cdot g\cdot g'$.

7. $t(P'(M_q, M'_{q'})) = (x-1)\cdot f\cdot f' + (y-1)\cdot g\cdot g' + f\cdot g' + g\cdot f'$.

8. $P(M_q, M'_{q'})/\bar{q} = M_q/q \oplus M'_{q'}/q'$.

Conversely, if $\bar{M}_{\bar{q}}$ is any connected matroid such that $\bar{M}_{\bar{q}}/\bar{q} = M_1(S_1) \oplus M_2(S_2)$, then $\bar{M}_{\bar{q}} = P(\bar{M}_{\bar{q}} - S_2, \bar{M}_{\bar{q}} - S_1)$.

9. $S(M_q, M'_{q'}) - \bar{q} = (M_q - q) \oplus (M'_{q'} - q')$.

Conversely, if $\bar{M}_{\bar{q}}$ is any connected matroid such that $\bar{M}_{\bar{q}} - \bar{q} = M_1(S_1) \oplus M_2(S_2)$, then $\bar{M}_{\bar{q}} = S(\bar{M}_{\bar{q}}/S_2, \bar{M}_{\bar{q}}/S_1)$.

We remark that there is no particular reason to save just one point for last, and a theory could also be developed where a matroid $M(S)$ is "pointed" by a subset $A \subseteq S$. The reader interested in this generalization is referred to [93].

From the formula in (4.8.5), we see that

$\bar{t}_P(P(M_q, M'_{q'})) = x'\cdot(f \cdot f')(x,0) = \dfrac{\bar{t}_P(M_q)\cdot \bar{t}_P(M'_q)}{x'}$. In particular, $\bar{t}(P(M_q, M'_{q'})$ is independent of the choice of points q and q', and we have the following formulas:

10. $\bar{t}(P(M_q, M'_{q'})) = \bar{t}(M)\cdot\bar{t}(M')/x.$

11. $\chi(P(M_q, M'_{q'})) = \dfrac{\chi(M)\cdot\chi(M')}{\lambda - 1}.$

Formula (4.8.10) has a generalization which is explored in [29]. Given two combinatorial geometries $G(S)$ and $H(T)$ on disjoint sets, assume that a geometry x is isomorphic to a flat $H(T')$ of H and isomorphic to a modular flat $G(S')$ of G. Then, the *generalized parallel connection* $P_x(G_x, H_x)$ is defined to be the matroid on the set of points $(S-S') \dot\cup (T-T') \dot\cup x$ whose closed sets are all the subsets A such that $A \cap S$ is closed in G (here, S' and x are identified), and $A \cap T$ is closed in H. We then have the following:

12. $\chi(P_x(G_x, H_x)) = \dfrac{\chi(G)\chi(H)}{\chi(x)}$.

We now define a new operation on matroids which encompasses some of the ideas of Bixby [12], Brylawski [24], and Seymour [125].

Definition 4.9 Let M be a matroid on the set $\{p_1,\ldots,p_k\}$, and let M'_q be a pointed matroid. The *tensor product* $M \otimes M'_q$ is the matroid formed by making a two-sum of M'_q at each point of M. Formally, $M \otimes M'_q = M^k$ where $M^0 = M$, and for all $i : 1 \leq i \leq k$, $M^i = P'(M^{i-1}_{p_i}, M'_q)$. The reader may readily convince himself that this definition is independent of the ordering on the points of M and includes as special cases: replacing all the points of M with multiple points or with comultiple points (points in series). The tensor product is only defined when q is a nonfactor.

Proposition 4.10 If $t(M) = f(x,y)$, and $t_p(M'_q) = x'f'(x,y) + y'g'(x,y)$, then the Tutte polynomial of the tensor product of M and M'_q is given by:

$$t(M \otimes M'_q) = (f'(x,y))^{\mathrm{nul}(M)} \cdot (g'(x,y))^{r(M)} \cdot f\left(\frac{(x-1)f'+g'}{g'}, \frac{f'+(y-1)g'}{f'}\right).$$

Proof. Fix M'_q, and let $f(M) = t(M \otimes M'_q)$. We will show that f satisfies the (weighted) T-G recursions T2 and T1' with $a = f'$ and $b = g'$. We may then invoke (3.20.2). First, if L is a loop then $f(L) = t(L \otimes M'_q) = t(M'_q/q) = f' + (y-1)\cdot g'$ by (4.8.3). If I is an isthmus, then $f(I) = t(I \otimes M'_q) = t(M'_q-q) = (x-1)\cdot f' + g'$ by (4.8.2). If p is a factor of M, then

$$P'(M_p, M'_q,) = \begin{cases} (M'_q-q) \oplus (M-p) & \text{if } p \text{ is an isthmus} \\ (M'_q/q) \oplus (M-p) & \text{if } p \text{ is a loop.} \end{cases}$$

Thus, $f(M) = t((M-p) \otimes M'_q)\cdot t(p \otimes M'_q) = f(M-p)\cdot f(p)$, and T2 holds.

Finally, let $p \in M$ be a nonfactor, and let $S \cup q$ denote the points of M'_q. Deleting and contracting the points of S simultaneously in M'_q and $M \otimes M'_q$, we see that when q becomes an isthmus giving $I \oplus \bar{M}$ for the decomposition in M'_q, the tensor product becomes $((M-p) \otimes M'_q) \oplus \bar{M}$. Similarly, when q becomes a loop giving $L \oplus \bar{\bar{M}}$ in the decomposition of M'_q, the tensor product becomes $((M/p) \otimes M'_q) \oplus \bar{\bar{M}}$. Thus, when all the points of S are deleted and/or contracted, we get, for $t(M \otimes M'_q)$, the Tutte polynomial of $(M-p) \otimes M'_q$ multiplied by f' (the coefficient of x' in $t(M'_q)$) plus the Tutte polynomial of $(M/p) \otimes M'_q$ multiplied by g'. This is precisely recursion T1' for f.

Example 4.11 If M'_q has a transitive automorphism group, then we may define the tensor product $M \otimes M'$ unambiguously without specifying a particular point $q \in M$ as the distinguished one. In fact, even when $t(M'-q) = t(M'-q')$ for all $q, q' \in M'$, we will see in the next section on reconstruction (5.2) that $t(M'-q)$ and $t(M'/q)$ may be computed from $t(M')$. Thus, $t(M \otimes M'_q)$ may be computed from $t(M)$ and $t(M')$.

For now, let M^k be a point of multiplicity k (a k-point rank-one loopless matroid). Then:

$$t_p(M^k_q) = x' + (y^{k-2} + y^{k-3} + \dots + y + 1)y',$$

$$t(M^k-p) = y^{k-2} + y^{k-3} + \dots + y + x,$$

and $$t(M^k/p) = y^{k-1}.$$

Given a matroid M, let $M^{(k)} = M \otimes M^{k+1}$, where M^{k+1} is defined above. Then $M^{(k)}$ replaces each point of M by a point of multiplicity k. Further,

$$t(M^{(k)}) = (y^{k-1} + \ldots + y + 1)^{r(M)} t(M; \frac{y^{k-1}+\ldots+y+x}{y^{k-1}+\ldots+y+1}, y^k).$$

In particular, for example, the number of bases of $M^{(k)}$ is $t(M^{(k)};1,1) = k^{r(M)} t(M;1,1)$, its number of independent sets is $k^{r(M)} t(M;\frac{k+1}{k},1)$, and the number of spanning sets is $(2^k-1)^{r(M)} t(M;1,2^k)$.

Even though we cannot, in general, calculate $t(M-p)$ from $t(M)$, we certainly know that (for nonfactors) $t(M-p) \leq t(M)$ in the sense that the coefficient b'_{ij} of $x^i y^j$ in $t(M-p)$ is less than or equal to the corresponding b_{ij} in $t(M)$. This remark generalizes as follows:

Proposition 4.12 If M' is a minor of the connected matroid M, then M' can be obtained from M by a sequence of deletions and conttactions by nonfactors, and $t(M') \leq t(M)$.

Proof. This was shown in [27]. The proof involves showing that any connected minor M' can be obtained by a series of deletions and contractions by points such that at every step a connected matroid (and thus one without loops or isthmuses) is obtained. Hence, $t(M) \geq t(M-p) \geq t(M-p/q) \geq t(M-p/q/r) \geq \ldots \geq t(M')$. ' en M' is separable, say $M' = M'_1 \oplus M'_2$, then somewhere in the decomposition a deletion (or contraction) gives a separable matroid $M_1 \oplus M_2$ with M'_i a minor of M_i. Then, in the step immediately preceding that deletion (or contraction) there was a series connection $S(\bar{M}_1,\bar{M}_2)$ by (4.8.9) (or a parallel connection by (4.8.8)). In any event, $t(M'_i) \leq t(\bar{M}_i)$ by induction, and formula (4.8.6) gives the desired result.

Another operation for which something can be said about the Tutte polynomial is that of the action of a rank-preserving bijective weak map. This will be explored later in Proposition 6.16.

5. Reconstruction.

Two celebrated open problems in graph theory are whether any graph G may be reconstructed up to isomorphism from either its multiset of isomorphism classes of vertex-deleted subgraphs or from its edge-deleted subgraphs. In an attempt to solve these problems, there is a wealth of literature reconstructing various invariants of G from the subgraphs. Both vertex and edge deletions have analogs in matroid theory (bond and point deletions respectively), and while a general matroid cannot be reconstructed, its Tutte polynomial can be computed from selected minors as we shall see below. In the following, we will often use the cardinality-corank generating function and the Poincaré polynomial along with the formulas of Proposition 3.18 relating each to the Tutte polynomial. First, we give an invertible formula for the Tutte polynomial of a matroid from the weighted sum of the polynomials of its point deletions.

Proposition 5.1 Let M be a matroid of rank n and cardinality K with Tutte polynomial $t(M;x,y)$ and cardinality-corank polynomial $S_{KC}(M;z,u)$. We then have the following formulas.

1. $$\sum_{p:p \text{ is not a loop}} t(M/p) + (y-1) \sum_{p:p \text{ is a loop}} t(M/p) = [n + (y-1)\frac{\partial}{\partial y} - (x-1)\frac{\partial}{\partial x}]t(M;x,y).$$

2. $$\sum_{p:p \text{ is not an isthmus}} t(M-p) + (x-1) \sum_{p:p \text{ is an isthmus}} t(M-p) = [K-n + (x-1)\frac{\partial}{\partial x} - (y-1)\frac{\partial}{\partial y}]\ t(M;x,y).$$

3. $\sum\limits_{p} S_{KC}(M/p) = \frac{\partial}{\partial z} S_{KC}(M;z,u)$.

4. $S_{KC}(M;z,u) = \int\left(\sum\limits_{p} S_{KC}(M/p)\right)dz + u^n$, where $\int dz$ is the (formal) integral operator: $\int z^n u^m dz = \frac{z^{n+1}u^m}{n+1}$.

5. $$t(M;x,y) = (x-1)^n + (y-1)^{-n}\cdot\left(\int x^{n-1} T\left(\frac{x+y}{x},\ x+1\right)dx \,\Bigg|_{\substack{x \mapsto y-1 \\ y \mapsto (x-1)(y-1)}}\right)$$

where $T(M;x,y) = \sum\limits_{p:p \text{ is not a loop}} t(M/p) + (y-1) \sum\limits_{p:p \text{ is a loop}} t(M/p)$.

6. $$t(M;x,y) = (y-1)^{K-n} + (x-1)^{-K+n}\cdot\left(\int y^{K-n-1} T'\left(y+1, \frac{x+y}{y}\right)dy \,\Bigg|_{\substack{y \mapsto x-1 \\ x \mapsto (x-1)(y-1)}}\right)$$

where $T'(M;x,y) = \sum\limits_{p:p \text{ is not an isthmus}} t(M-p) + (x-1) \sum\limits_{p:p \text{ is an isthmus}} t(M-p)$.

Proof. We could proceed by first verifying (5.1.3). Note that any subset $A \subseteq S$ of cardinality i and corank j contributes one to the coefficient of $z^i u^j$ in $S_{KC}(M)$. Then, for each of the i points p in A, $A - p$ contributes one to the coefficient of $z^{i-1}u^j$ in $t(M/p)$. The other formulas follow from the identities of (3.18) and duality.

An alternate proof is based on recursion.

1. If $t(M) = x^n y^{K-n}$, then both sides of (5.1.1) equal

$$nx^{n-1}y^{K-n} + (y-1)\cdot(K-n)\cdot x^n y^{K-n-1} .$$

Now, assume that q is a nonfactor of M, and that q is in a multiple point with m other points ($m \geq 0$). We partition the points of

S - q as follows: P_1 is the set of loops of M, P_2 is the (possibly empty) set of m points in parallel with q, and P_3 is the set of all other points (the nonloops of M/q). Let M' denote M/q with P_2 removed, and let $\mathcal{O}_{n'}$ be the differential operator

$$n' + (y-1)\frac{\partial}{\partial y} - (x-1)\frac{\partial}{\partial x} .$$

We then have the following:

$$\mathcal{O}_{r(M)}t(M)$$

$$= \mathcal{O}_{r(M)}(t(M-q) \ + t(M/q))$$

$$= \mathcal{O}_{r(M-q)}t(M-q) + \mathcal{O}_{r(M/q)}t(M/q) + t(M/q)$$

$$= (y-1)\sum_{p\epsilon P_1} t(M-q/p) + \sum_{p\epsilon P_2} t(M-q/p) + \sum_{p\epsilon P_3} t(M-q/p)$$

$$+ (y-1)\sum_{p\epsilon P_1} t(M/q/p) + (y-1)\sum_{p\epsilon P_2} t(M/q/p) + \sum_{p\epsilon P_3} t(M/q/p) + t(M/q)$$

$$= (y-1)\sum_{p\epsilon P_1} (t(M/p-q) + t(M/p/q)) + \sum_{p\epsilon P_3} (t(M/p-q) + t(M/p/q))$$

$$+ m\cdot y^{m-1}\cdot t(M') + m\cdot(y-1)\cdot y^{m-1}\cdot t(M') + y^m t(M')$$

$$= (y-1)\sum_{p\epsilon P_1} t(M/p) + \sum_{p\epsilon P_3} t(M/p) + (m+1)\cdot y^m\cdot t(M')$$

$$= (y-1)\sum_{p:p \text{ is a loop of } M} t(M/p) \qquad + \sum_{p:p \text{ is not a loop}} t(M/p) \qquad .$$

2. When (5.1.2) and (5.1.1) are added together, both sides equal K·t(M).

3. $\frac{\partial}{\partial z} S_{KC}(z,u) = \frac{\partial}{\partial z}(z^n \cdot t(\frac{z+u}{z}, z+1)) = (nz^{n-1} + z^n \frac{\partial}{\partial z})t(\frac{z+u}{z}, z+1)$.

By the chain rule, $\frac{\partial}{\partial z} t(\frac{z+u}{z}, z+1) = (\frac{-u}{z^2} \frac{\partial}{\partial x} + \frac{\partial}{\partial y})t(x,y)$, where $x = \frac{z+u}{z}$ and $y = z+1$ (so that $z = y-1$ and $u = (y-1)(x-1)$). Under this substitution:

$$\frac{\partial}{\partial z} S_{KC}(z,u)$$

$$= (n\cdot(y-1)^{n-1} + (y-1)^n(\frac{1-x}{y-1} \frac{\partial}{\partial x} + \frac{\partial}{\partial y}))t(x,y)$$

$$= (y-1)^{n-1}[n + (y-1)\frac{\partial}{\partial y} - (x-1)\frac{\partial}{\partial x}]t(x,y)$$

$$= (y-1)^{n-1}[\sum_{\text{nonloops}} t(M/p) + (y-1) \cdot \sum_{\text{loops}} t(M/p)]$$

$$= (y-1)^{n-1} \cdot \sum_{\text{nonloops}} t(M/p;x,y) + (y-1)^n \cdot \sum_{\text{loops}} t(M/p;x,y)$$

$$= \sum_{\text{nonloops}} z^{n-1} t(M/p;\frac{z+u}{z}, z+1) + \sum_{\text{loops}} z^n t(M/p;\frac{z+u}{z}, z+1)$$

$$= \sum_p S_{KC}(M/p;z,u).$$

4. We integrate both sides of (5.1.3) with respect to z and note that the constant of integration is a function of u. Thus,

$$S_{KC}(M;z,u) = \int(\sum_p S_{KC}(M/p))dz + S_{KC}(M;0,u), \quad \text{and} \quad S_{KC}(M;0,u) = u^n$$

(the term corresponding to the empty set of cardinality zero and corank $n = r(M)$).

5. This formula comes from converting the Tutte polynomial to the cardinality-corank polynomial and applying (5.1.4).

6. Formula (5.1.6) is dual to formula (5.1.5). (It can also be proved in analogy with (5.1.4) and (5.1.5) by means of the cardinality-nullity polynomial.) We now apply the above formulas to homogeneous matroids. In (5.2.3), we use (4.8.4).

Corollary 5.2 Assume M is a matroid on K points of rank n: $0 < n < K$, with $t(M/p) = t(M/q)$ for all $p, q \in S$. (Thus, all deletions also have the same Tutte polynomial). This occurs, in particular, when all contractionsare isomorphic,or when M has a transitive automorphism group. Then:

1. $$t(M/p) = \frac{1}{K}[n + (y-1)\frac{\partial}{\partial y} - (x-1)\frac{\partial}{\partial x}]\ t(M;x,y)$$

2. $$t(M-p) = \frac{1}{K}[K-n + (x-1)\frac{\partial}{\partial x} - (y-1)\frac{\partial}{\partial y}]\ t(M;x,y)$$

3. The pointed Tutte polynomial of (4.7) is given by:

$$t_p(M_q;x',y',x,y) =$$

$$= (x+y-xy)^{-1}\left[(x'+y' - \frac{n}{K}\,xy' - \frac{K-n}{K}\,x'y) + \frac{1}{K}(x'y-xy')(1-x)\frac{\partial}{\partial x}\right.$$
$$\left. + \frac{1}{K}(xy'-x'y)(1-y)\frac{\partial}{\partial y}\right]\ t(M;x,y).$$

Examples 5.3

1. In the matroid M_2 of Example 4.3.1, all six contractions are isomorphic to a line L with three single points and one double point. Equation 5.2.1 then becomes:

$$t(L) = \frac{1}{6}[3+(y-1)\frac{\partial}{\partial y} - (x-1)\frac{\partial}{\partial x}](x^3+3x^2+4x+2xy+4y+3y^2+y^3)$$

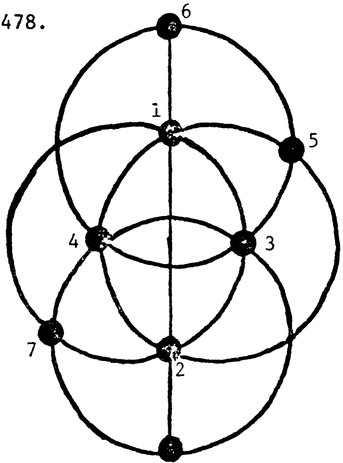
$$= \frac{1}{6}((3x^3+9x^2+12x+6xy+12y+9y^2+3y^3) + (2xy-2x+4y-4+6y^2-6y+3y^3-3y^2)$$

$$+ (3x^2-3x^3+6x-6x^2+4-4x+2y-2xy)) = x^2+2x+xy+2y+2y^2+y^3.$$

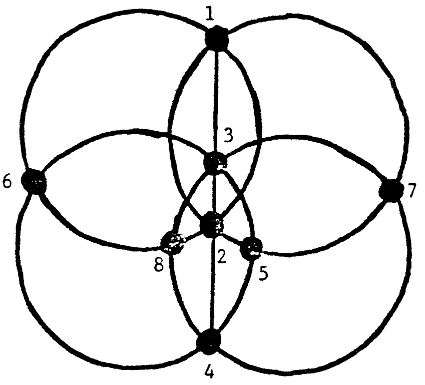
The polynomial $6t(L)$ is also the sum of the Tutte polynomials of the contractions of the matroid $M_1 + p$ in (4.3.1), but these contractions do not all have the same Tutte polynomial. Thus, $t(M)$ cannot, in general, determine whether all contractions have the same Tutte polynomial (i.e., whether $t(M/p) = t(M/q)$ for all p and q).

2. Assume $M(S)$ and $M'(S')$ are two matroids such that, for some ordering on the points of S and S' respectively, $t(M/p_i) = t(M'/p_i')$ for all i. Then, a consequence of (5.1) is that $t(M) = t(M')$. (A trivial exception is when M has all loops, and M' is a multiple point, since only in that case can we not determine from the set $\{t(M/p)\}$ whether a particular contraction was by a loop.) From the study of non-desarguesian projective planes and Steiner systems, examples abound of nonisomorphic matroids M_1 and M_2 (of the same rank) such that $M_1 - p_i \cong M_2 - p_i$ for all i (see, e.g., [37]). We exhibit the smallest pair below in "Möbius representation," i.e., both are rank-four paving matroids, each with five four-point planes represented below by lines and circles. In particular, the dependent planes of M_1 are 1237, 1245, 1268, 3456, and 3478; while those of M_2 are 1234, 1257, 1268, 3456, and 3478.

M_1 =



M_2 =



The respective duals of these matroids are minimum examples of non-isomorphic matroids with isomorphic contractions.

3. Surprisingly, the geometric Tutte polynomial cannot be reconstructed by geometric contraction (upper intervals of corank one). In particular, let G be the planar geometry $AG(2,3)$; and let G' be the nine-point combinatorial geometry $PG(2,3)-Q$, where Q is a quadrilateral. Then all rank-two upper intervals are isomorphic: for any point p, $\overline{G/p} \simeq \overline{G'/p} \simeq L_4$, a four-point line. However, G has 12 three-point lines; while G' has 6 two-point lines, 4 three-point lines, and 3 four-point lines. Thus, $16 = |\mu(G)| \neq |\mu(G')| = 15$.

We now turn to the hyperplane reconstruction of $t(M)$. Details may be found in [40]. In the following, let the set $A_k = \{\alpha^k\}$ index isomorphism classes of matroids of rank k. Thus, F_{α^3} stands for a rank-three matroid isomorphism class, and it has $|\overline{F_{\alpha^3}}|$ atoms. Now, for a fixed matroid M, let $n(F_{\alpha^k},M)$ denote the number of flats of M isomorphic to F_{α^k} and let $n(F_{\alpha^i},F_{\alpha^{i+1}})$ denote the number of flats isomorphic to F_{α^i} in any matroid isomorphic to $F_{\alpha^{i+1}}$. The hyperplane reconstruction theorem asserts that, for $r(M) = n$, we may calculate $t(M)$ from $n(F_{\alpha^{n-1}},M)$ for all $\alpha^{n-1} \in A_{n-1}$. We first give a formula for $n(F_{\alpha^k},M)$ $(k < n)$.

Lemma 5.4 The number of flats x of M isomorphic to F_{α^k} is given for all $k < n = r(M)$ and $\alpha^k \in A_k$ by the formula:

$$n(F_{\alpha^k},M) =$$

$$= \sum_{\alpha^{n-1}} n(F_{\alpha^{n-1}},M) \sum_{\alpha^{n-2},\ldots,\alpha^{k+1}} \prod_{i=k+1}^{n-1} \frac{n(F_{\alpha^{i-1}},F_{\alpha^i})(|\bar{F}_{\alpha^i}|-|\bar{F}_{\alpha^{i-1}}|)}{(m-|\bar{F}_{\alpha^{i-1}}|)}$$

where $m = |\bar{M}|$ is the unique integer (greater than the size of any hyperplane) which satisfies the equation:

$$1 = \frac{1}{m} \sum_{\alpha^{n-1}} n(F_{\alpha^{n-1}},M) \sum_{\alpha^{n-1},\ldots,\alpha^1} \prod_{i=2}^{n-1} \frac{n(F_{\alpha^{i-1}},F_{\alpha^i})(|\bar{F}_{\alpha^i}|-|\bar{F}_{\alpha^{i-1}}|)}{(m-|F_{\alpha^{i-1}}|)}$$

Essentially, the first formula counts, in two ways, independent sequences of atoms $(a_{k+1},\ldots,a_{n-1})$ in M such that for all i, $a_i \vee F_{\alpha^{i-1}} \simeq F_{\alpha^i}$. The second formula comes from the fact that there is a unique flat in M of rank zero.

We may now reconstruct $S_{KC}(M)$:

Proposition 5.5

$$S_{KC}(M;z,u) = (z+1)^K - \sum_{k:k<n} \left[(u^{n-k}-1) \cdot \sum_{\alpha^k \in A^k} n(F_{\alpha^k},M) S_K(F_{\alpha^k};z) \right].$$

Here, $S_K(M',z)$ is the spanning-set polynomial of M', so, if a_i is the number of i-element subsets of S which span M', then $S_K(M',z) = \sum_i a_i z^i$. Further, $n = r(M) = r(F_{\alpha^{n-1}}) + 1$, and

$K = |M| = \ell + \sum_{\alpha^1} n(F_{\alpha^1}, M)(|F_{\alpha^1}| - \ell)$, ℓ being the number of loops in M (or, equivalently, in any hyperplane).

Knowing the Tutte polynomial of M is equivalent to knowing, for all parameters, the number of all sets in M of fixed cardinality and corank. It is related, though not as strongly, to the number of all closed sets of fixed cardinality and corank. In fact, from $t(G)$ we have seen how to compute the number of loops (4.4.2), and it is not hard to get the number of k-point atoms for all k (essentially from the polynomial coefficient of λ^{n-1} in the Poincaré polynomial). However, in general, the number of flats of larger rank cannot be deduced from $t(M)$. This was seen in Example 3.11 where for two matroids M and M', with the same Tutte polynomial, M had 5 three-point planes, while M' had 6 such three-point planes. In Example 4.5.1, M^* had 2 two-point lines, while M'^* had 3 two-point lines. Conversely, even if we know the cardinality and rank of all flats, we still cannot in general recover the Tutte polynomial as the following example shows:

Example 5.6 Let M_1 and M_2 be the matroids of (4.5.2), let M'^* and M^* be as given in (4.5.1), let L_3 be a three-point line, and let B^3 be a three-point boolean algebra. Then, letting $T^{-3}(M)$ be truncation of M to the plane, the reader may easily verify that $M_3 = T^{-3}(M_2 \oplus M'^* \oplus M'^* \oplus M'^* \oplus L_3)$ and $M_4 = T^{-3}(M_1 \oplus M^* \oplus M^* \oplus M^* \oplus B^3)$ have the same number of flats of cardinality i and rank j for all i and j. However, $t(M_3) \neq t(M_4)$.

The Poincaré polynomial is a summation of polynomials over closed sets, and thus can count certain of them. The reason one cannot recover all the closed sets from $\bar{\chi}(M)$ is that certain characteristic polynomials $\chi([x,1],\lambda)$ "get lost" when summed with characteristic polynomials of flats x' of the same cardinality but greater corank. This is precisely what happens in (4.5.1), where the characteristic polynomial for the double point "shadows" those for the two-point lines. What can be determined from the number of certain closed sets is the "border polynomial" of the Tutte polynomial.

Definition 5.7 Let M be a matroid of cardinality K and rank n. The *Tutte-Grothendieck border polynomial* is the polynomial:

$$t_B(M) = \sum_{\substack{i,j:b_{ij}>0,\text{ and } b_{i'j'}=0\\ \text{for } i'>i,j'>j}} b_{ij}\, x^i\, y^j$$

We similarly have the *corank-nullity border polynomial:*

$$S_B(M) = \sum_{\substack{i,j:a_{ij}>0,\text{ and}\\ a_{i'j'} = 0\\ \text{for } i'>i,j'>j}} a_{ij}\, u^i\, v^j$$

and the *closed-set border polynomial*

$$F_B(M) = \sum_{i,j} f_{ij}\, s^i\, t^j$$

where f_{ij} is the number of closed sets of M of corank i and nullity j, and the sum is again over all indices (i,j) such that $f_{ij} > 0$, while $f_{i'j'} = 0$ for $i' > i$, $j' > j$.

The *corners* of a polynomial $\sum c_{ij}x^iy^j$ are indexed coefficients c_{ij} such that $c_{ij} \neq 0$ but $c_{i'j} = c_{ij'} = 0$ for $i' > i$, $j' > j$. Two corners $c_{i,j}$ and $c_{i',j'}$ with $(n-i,j) < (n-i',j')$ are *consecutive* if there is no corner $c_{i'',j''}$ with $(n-i,j) < (n-i'',j'') < (n-i',j')$. It is clear that terms in the border polynomial are given below (with not all coefficients necessarily nonzero):

$$\ldots + c_{i,j-1}x^iy^{j-1} + c_{ij}x^iy^j + c_{i-1,j}x^{i-1}y^j + c_{i-2,j}x^{i-2}y^j + \ldots c_{i'j}x^{i'}y^j$$

$$+ c_{i',j+1}x^{i'}y^{j+1} + \ldots + c_{i'j'}x^{i'}y^{j'} + c_{i'-1,j'}x^{i'-1}y^{j'} + \ldots$$

where c_{ij} and $c_{i'j'}$ are consecutive corners. Some elementary remarks about the border polynomials are contained in the following proposition.

Proposition 5.8 1. For a matroid M of rank n on a set S of cardinality K, the corank-nullity border polynomial has $K + 1$ positive terms beginning with x^n and ending with y^{K-n}. A coefficient a_{ij} in S_B counts the subsets $A \subseteq S$ such that $|A| = n-i + j$, $r(A)=n-i$, and no subset of the same cardinality has larger corank (or, equivalently, larger nullity).

2. The three border polynomials defined above all have the same corners ($a_{ij} = b_{ij} = f_{ij}$). These numbers count the subsets A of M of corank i and nullity j such that every smaller subset has less nullity and every bigger subset has greater rank. Each such subset A is closed and cyclic (a union of circuits).

3. The closed-set border polynomial has at most $K + 1$ terms and has exactly $K + 1$ (positive) terms if and only if M has closed sets of every cardinality (and, thus, has an isthmus and no loops). The Tutte-Grothendieck border polynomial has at most $K + 1$ terms and has exactly $K + 1$ terms

whenever M is connected and not the truncated boolean algebra $T^{K-n}(B^K)$.

Proof. 1. The empty set is the unique subset of nullity 0 and (maximal) corank n, while S is the unique subset of (maximal) nullity $K-n$ and corank 0. Let k be an integer between 0 and K, and let $i(k)$ be the maximal corank of a subset A of S with $|A| = k$. Then, A has nullity $j(k) = k-n + i(k)$, and $a_{i(k),j(k)}x^{i(k)}y^{j(k)}$ is a term in the corank-nullity border polynomial. Each k gives a different index pair.

2. Let a_{ij} be a corner of $S_B(M)$. Then, there are a_{ij} subsets A of S each of cardinality $n-i+j$ and rank $n-i$. Since $a_{i+1,j} = a_{i,j+1} = 0$, any set smaller than A has less nullity, and every larger set has greater rank. Thus, A is closed and (as a subgeometry) has no isthmuses, and these sets A all contribute to $f_{i,j}$. Since, clearly, $f_{i,j} \leq a_{i,j}$ for all i and j in $F(M)$ and $S(M)$ respectively, $f_{i,j}$ is a corner of $F_B(M)$. If a_{ij} is a corner of $S(M)$, then $t(M;x,y) = S(M;x-1,y-1) = \sum_{i',j'} a_{i'j'}(x-1)^{i'}(y-1)^{j'} = a_{ij}x^iy^j$

$+ \sum_{i',j'} b_{i'j'}x^{i'}y^{j'}$, where either $i' < i$ or $j' < j$. Thus, $b_{ij} = a_{ij}$ is a corner of $t(M)$, and a similar argument shows that each corner of $t(M)$ is a corner of $S(M)$.

3. We have seen that $f_{ij} \leq a_{ij}$ for all coefficients of $F(M)$ and $S(M)$ respectively. Since $S(M;u,v) = t(M;u+1,v+1)$, $b_{ij} \leq a_{ij}$ for all coefficients of $t(M)$ and $S(M)$. Since $F(M)$, $S(M)$, and $t(M)$ have the same corners, $F_B(M) \leq S_B(M)$ and $t_B(M) \leq S_B(M)$ (with

term-wise ordering). Thus, $F_B(M)$ and $t_B(M)$ each have at most $K + 1$ terms. If M has a closed set of size k, then there is a minimal-rank such set. Conversely, contributions to different border terms have different cardinalities. Results of the next section (see (6.5)) show that if b_{ij} is a nonzero term in $t(M)$ for a connected M with $i > 0$ and $j > 0$, then $b_{i-1,j} > 0$ and $b_{i,j-1} > 0$. Thus, the border is a connected polygonal path of positive coefficients in $t(M)$ as long as $b_{11} > 0$. But (6.5) shows that $b_{11} > 0$ if M is a connected matroid which is not free.

Using the above proposition, we define the pair $(i(k),j(k))$ to be the index of the term of $S_B(M)$ with $n-i(k) + j(k) = k$. Thus, each term of $t_B(M)$ and $F_B(M)$ is indexed by the pair $(i(k),j(k))$ for some k. The essence of the following proposition is that $S_B(M)$, $t_B(M)$, and $F_B(M)$ can all be derived from each other. In particular, note that any coefficient appearing below is in the border. We also remark that arguments could be based on the Poincaré polynomial, where $f_{i(k),j(k)}$, if nonzero, is the coefficient of $u^k\lambda^{i(k)}$.

Proposition 5.9

1. $$a_{i(k),j(k)} = \sum_{j\geq j(k)} \binom{k+j-j(k)}{k} f_{i(k),j} = \sum_{j\geq j(k)} \binom{n-i(k)+j}{n-i(k)+j(k)} f_{i(k),j}$$

2. $$f_{i(k),j(k)} = \sum_{j\geq j(k)} (-1)^{j-j(k)} \binom{k+j-j(k)}{k} a_{i(k),j}$$

3. $$b_{i(k),j(k)} = \sum_{j\geq j(k)} (-1)^{j-j(k)} \binom{j}{j(k)} a_{i(k),j} + \sum_{i>i(k)} (-1)^{i-i(k)} \binom{i}{i(k)} a_{i,j(k)}$$

4. $$a_{i(k),j(k)} = \sum_{j\geq j(k)} \binom{j}{j(k)} b_{i(k),j} + \sum_{i>i(k)} \binom{i}{i(k)} b_{i,j(k)}$$

5. $$b_{i(k),j(k)} = \sum_{j\geq j(k)} \binom{n-1-i(k)+j-j(k)}{j-j(k)} f_{i(k),j} + \sum_{i>i(k)} (-1)^{i-i(k)} \binom{i}{i(k)} f_{i,j(k)}$$

6. $$f_{i(k),j(k)} = \sum_{j\geq j(k)} (-1)^{j-j(k)} \binom{n-i(k)}{j-j(k)} b_{i(k),j} + \sum_{i>i(k)} \binom{i}{i(k)} b_{i,j(k)} .$$

Proof. 1,2. The coefficient $a_{i(k),j(k)}$ is the number of subsets A of cardinality k and corank $i(k)$. For each such subset A, $\bar{A}$ is tabulated in $f_{i(k),j}$ with $j \geq j(k)$. Conversely, for each closed set F of corank $i(k)$ and nullity j, there are $\binom{n-i(k)+j}{n-i(k)+j(k)} = \binom{k+j-j(k)}{k}$ subsets of cardinality k. Each such subset has corank $i(k)$, since if it had greater corank, there would be a subset A' of corank i' and nullity j' with $i' > i(k)$ and $j' > j \geq j(k)$. This contradicts the definition of $a_{i(k),j(k)}$. Formula (5.9.2) inverts (5.9.1) by standard techniques.

3,4. These formulas come from the reciprocal evaluations $t(M;x,y) = S(M;x-1,y-1)$, $S(M;u,v) = t(M;u+1,v+1)$, and the fact that no other terms than the ones listed contribute to $b_{i(k),j(k)}$.

5,6. Combining (5.9.3) and(5.9.1), we obtain:

$$b_{i(k),j(k)} = \sum_{j'\geq j\geq j(k)} (-1)^{j-j(k)} \binom{j}{j(k)} \binom{n-i(k)+j'}{j'-j} f_{i(k),j'} + \sum_{i>i(k)} (-1)^{i-i(k)} \binom{i}{i(k)} f_{i,j(k)} .$$

The identity $\sum_{j:j'\geq j\geq j(k)} (-1)^{j-j(k)} \binom{j}{j(k)} \binom{n-i(k)+j'}{j'-j} = \binom{n-1-i(k)+j'-j(k)}{j'-j(k)}$

comes from calculating the coefficient of $x^{j'-j(k)} = x^{j-j(k)} \cdot x^{j'-j}$

in $(1+x)^{n-1-i(k)+j'-j(k)} = \dfrac{(1+x)^{n-i(k)+j'}}{(1+x)^{j(k)+1}}$. (5.9.6) inverts (5.9.5)

by similar identities.

Proposition 5.10 Let $F_B(M^*) = \sum_{k=0}^{K} f^*_{i*(k),j*(k)} s^i t^j$ be the closed-set border polynomial of M^*. Then, $(i^*(k),j^*(k)) = (j(K-k),i(K-k))$, and

$$c_{i(K-k),j(K-k)} = f^*_{j(K-k),i(K-k)} = \sum_{\substack{i\geq i(K-k)\\ j\geq j(K-k)}} (-1)^{i-i(K-k)} \binom{k+i-i(K-k)}{k} \cdot \binom{K-k+j-j(K-k)}{K-k} f_{i,j}$$

$$= \sum_{i\geq i(K-k)} (-1)^{i-i(K-k)} \binom{k+i-i(K-k)}{k} f_{i,j(K-k)}$$

$$+ \sum_{j>j(K-k)} \binom{K-k+j-j(K-k)}{K-k} f_{i(K-k),j} .$$

Here, c_{ij} is the number of cycles of M of corank i and nullity j.

Proof. A set A is closed in M^* if and only if $S-A$ is a cycle (union of circuits) in M. Also, the corank in M^* of A is equal to the nullity in M of $S-A$. Thus, $f^*_{i,j}$ is a corner of $F_B(M^*)$ if and only if $f_{j,i}$ is a corner of $F_B(M)$ (see (5.8.2)). But $f^*_{i,j}$ counts (dual-closed) sets of cardinality $K-n-i+j = K-(n-j+i)$. Thus, $(i^*(k),j^*(k)) = (j(K-k),i(K-k))$.

We have already seen that if $S(M^*) = \sum_{i,j} a^*_{ij} u^i v^j$, then $a^*_{ij} = a_{ji}$ (see (3.3.7)). By (5.9.2),

$$f^*_{i*(k),j*(k)} = \sum_{j\geq j*(k)} (-1)^{j-j*(k)} \binom{k+j-j*(k)}{k} a^*_{i*(k),j} .$$

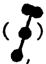
Thus,

$$f^*_{j(K-k),i(K-k)} = \sum_{i\geq i(K-k)} (-1)^{i-i(K-k)} \binom{k+i-i(K-k)}{k} a^*_{j(K-k),i} .$$

Here, $a^*_{j(K-k),i} = a_{i,j(K-k)} = \sum_{j\geq j(K-k)} \binom{K-k+j-j(K-k)}{K-k} f_{i,j}$ by (5.9.1), and (5.10) follows. (Note that if $(i,j) \geq (i(K-k),j(K-k))$, then at least one of the coordinates is equal.)

<u>Example 5.11</u> 1. Let M^* be as in (4.5.1). It then has the closed-set polynomial:

$$\begin{aligned} &s^3 + 5s^2 + 2s \\ &\quad + s^2t + 3st \\ &\qquad + 2st^2 \\ &\qquad\quad + t^4. \end{aligned}$$

The corners are $f_{3,0} = 1$, $f_{2,1} = 1$, $f_{1,2} = 2$, and $f_{0,4} = 1$ corresponding to closed sets of cardinality 0 ($\emptyset$), 2 ( ),4 (), and 7 (M^*) respectively. Thus, $F_B(M^*) = s^3 + 5s^2 + s^2t + 3st + 2st^2 + t^4$. Note that the only positive term in $F(M^*) - F_B(M^*)$ is $2s$. $F_B(M^*) = F_B(M'^*)$ where M'^* is as in (4.5.1), since both have the same Tutte polynomial. However, $F(M'^*) - F_B(M'^*) = 3s$.

From $F_B(M^*)$, one computes: $t_B(M^*) = x^3 + 3x^2 + x^2y + 5xy + {}$
$+ 2xy^2 + 4y^2 + 3y^3 + y^4$,

which agrees with the (dual) calculation in (3.4) for $t(M)$. Further,

$$\begin{aligned} F(M) = s^4 + 7s^3 + 15s^2 &+ 5s \\ &+ 2s^2t + 6st \\ &\qquad + st^2 \\ &\qquad\qquad + t^3 \end{aligned}$$

The border polynomial, $F_B(M) = \Sigma f_{ij}s^it^j$, can then be calculated from $F_B(M^*) = \Sigma f^*_{ij}s^it^j$ with $K = 7$. For example, in M^*, $j(7-4) = i(7-4) = 1$, and $f_{11} = 6 = f^*_{1,1} - \binom{4+2-1}{4}f^*_{2,1} + \binom{3+2-1}{3}f^*_{1,2} = 3-5+8$.

2. In general, one cannot compute $F(M^*)$ from $F(M)$. For example, the matroids M_3 and M_4 of (5.6) have the same closed-set polynomials, but the reader readily checks that M_3 has 38 three-point circuits, while M_4 has 37 three-point circuits. Thus,

$$F(M^*_3) = \ldots + 38st + \ldots \neq F(M^*_4).$$

The above suggests that $t(M)$ can be reconstructed from $F(M)$ if the closed sets are all enumerated in $F_B(M)$. This is the case of a special class of matroids called *near-designs*.

Definition 5.12 A matroid is a *near-design* if all closed sets of rank m have the same cardinality $k(m)$ for $m = 0,1,\ldots,n-2$. Thus, all atoms, lines, ..., and colines respectively have the same size. Special cases of near-designs are rank-three combinatorial geometries (where $k(0) = 0$, $k(1) = 1$), paving matroids (where for all m above, $k(m) = m$), and *homogeneous* matroids (see [37]) like projective and affine geometries, where, in addition, all hyperplanes have the same cardinality.

Operations which preserve near-designs are truncation, minors $M(S')/T$ where S' is a flat, and tensoring with a multiple point (see 4.11).

We parametrize near-designs with the vector $(k(0),k(1),\ldots,k(n-2);f_{1,0},f_{1,1},f_{1,2},\ldots,f_{1,K-n};k(n) = K)$, where $f_{1,i}$ is the number of hyperplanes of nullity i (and, hence, cardinality $n-1 + i$).

Note that we may generalize the notion of a near-design to a matroid which has no flats F and F' with $r(F) > r(F')$ and $|F| \leq |F'|$ (a necessary and sufficient condition for $F_B(M) = F(M)$). For these matroids, $t(M)$ and $F(M)$ should be also mutually derivable. Examples of such more general matroids are projective geometries $PG(n,q)$ with various multiplicities (up to q) on the points.

When all the flats of fixed rank (including the hyperplanes) are equicardinal, we term the matroid a *perfect matroid design* (*design* for short). We now give some known properties for designs.

Lemma 5.13 Let M be a design with parameters $(k(0),k(1),\ldots,k(n-1),k(n) = K)$.

1. Every interval $[x,y]$ with $r(x) = r$ and $r(y) = s$ is a design of rank $s-r$ with $f(r,i,s)$ flats of rank $i-r$ in its lattice. Thus, $f(r,i,s)$ is the number of flats in M of rank i which contains or equals a fixed flat x of rank r and is contained in or equal to a fixed flat y $(y \geq x)$. Further,

$$f(r,i,s) = \prod_{m=r}^{i-1} \frac{k(s)-k(m)}{k(i)-k(m)} .$$

(Here $r \leq i \leq s$, and empty products are equal to one.)

In particular, the number of closed sets of M of corank n-i and nullity k(i)-i is given by:

$$(*) \qquad f_{n-i,k(i)-i} = f(0,i,n) = \prod_{m=0}^{i-1} \frac{K-k(m)}{k(i)-k(m)} \quad .$$

2. The value of the Möbius function $\mu(x,y)$ (with $x \leq y$) in the lattice of flats of M depends only on the rank of x and the rank y. In particular, if $r = r(x)$, and $s = r(y)$, then

$$\mu(x,y) = \mu(r,s) = (-1)^{s-r} \prod_{t=r+2}^{s} (f(r,t-1,t)-f(r+1,t-1,t))$$

$$= (-1)^{s-r} \prod_{m=r+1}^{s-1} \frac{k(s)-k(m)}{k(m)-k(r)} \quad .$$

3. The characteristic polynomial of the contraction of M by a flat x of corank i is independent of the choice of x and is given by:

$$\chi(M/x) = \chi(i) = \sum_{y:y\geq x} \mu(x,y)\lambda^{n-r(y)}$$

$$= \sum_{j=0}^{i} f(n-i,n-j,n)\mu(n-i,n-j)\lambda^{j}$$

$$= \sum_{j=0}^{i} \chi(i,j)\lambda^{j} \ ,$$

where $\chi(i,j) = (-1)^{i-j} \left[\prod_{j'=1}^{i-j} \frac{k(n)-k(n-i+j'-1)}{k(n-i+j')-k(n-i)} \right]$

4. The coefficients in the Poincaré polynomial,

$$\bar{\chi}(M;u,\lambda) = \sum_{i,j} c_{ij} u^{k(i)} \lambda^{n-j} ,$$

are given by:

$$c_{ij} = \sum_{\substack{x,y: \\ r(x)=i \\ r(y)=j}} \mu(x,y)$$

$$= \begin{cases} \displaystyle\prod_{m=0}^{j-1} \frac{K-k(m)}{k(i)-k(m)} & (j=i) \\ \displaystyle\frac{k(i)-K}{k(j)-k(i)} \prod_{\substack{m=0 \\ m\neq i}}^{j-1} \frac{K-k(m)}{k(i)-k(m)} & (j>i) \\ 0 & (j<i) \end{cases}$$

Proof. 1. The identify for $f(r,i,s)$ can be found in the papers by Edmonds, Murty, and Young which introduced perfect matroid designs ([70] and [162]). An interval of a design is itself a design whose parameters can be given by $k'(0) = k(i)$, $k'(1) = k(i+1), \ldots,$ $k'(j) = K' = k(i+j)$. Thus, we need only prove the formula for $f(0,i,n)$. This comes from counting, in two different ways, the i-tuples of independent points much as was done for atoms in (5.4). (Note that, in this context, (5.4) could be thought of as a generalization of the Young-Murty-Edmonds formula.)

2. That $\mu(x,y)$ depends only on ranks appears in [66] and [37]. The first formula above for $\mu(r,s)$ appears in [19], and a simplification of the identity:

$$(-1)^{s-r} \prod_{t=r+2}^{s} \left[\prod_{m=r}^{t-2} \frac{k(t)-k(m)}{k(t-1)-k(m)} - \prod_{m=r+1}^{t-2} \frac{k(t)-k(m)}{k(t-1)-k(m)} \right]$$

gives the second formula.

3. When the elements $\chi(i,j)$ are tabulated into an $(n+1) \times (n+1)$ matrix,it is the inverse of the matrix $W^2(i,j) = f(n-i,n-j,n)$. (See [66] or [37].) The formula for $\chi(i,j)$ then follows by inverting $W^2(i,j)$. Note that we could get an alternate proof of (5.13.3) from (5.13.2); or, equivalently, could prove (5.13.2) from (5.13.3).

4. The Poincaré polynomial is given by

$$\bar{\chi}(M) = \sum_{x \le y} \mu(x,y) u^{|x|} \lambda^{\mathrm{cor}(y)} \quad .$$

Thus, the coefficient of $u^{k(i)} \lambda^{n-j}$ is $\Sigma\mu(x,y)$ over all pairs $x \le y$ with $r(x) = i$ and $r(y) = j$ $(i \le j)$. Using the above formulas we obtain:

$$\Sigma\mu(x,y) = f(0,i,j) \cdot \mu(i,j) \cdot f(0,j,n)$$

$$= (-1)^{j-i} \prod_{m=0}^{i-1} \frac{k(j)-k(m)}{k(i)-k(m)} \cdot \prod_{m=i+1}^{j-1} \frac{k(j)-k(m)}{k(m)-k(i)} \cdot \prod_{m=0}^{j-1} \frac{K-k(m)}{k(j)-k(m)} \quad .$$

When $i = j$, the formula is obvious (it is $f(0,i,n)$); and when $i < n$, terms in the above product cancel to give the desired result.

We now generalize these results to near-designs.

Proposition 5.14 1. A near-design can be recognized by its Tutte polynomial. In particular, if $r(M) = n$, then M is a near-design if and only if, in the Poincaré polynomial,

$$\begin{aligned}\bar{\chi}(M;u,\lambda) &= (u-1)^n t(M;\tfrac{u+\lambda-1}{u-1},u)\\ &= \Sigma c'_{ij} u^i \lambda^j\\ &= \sum_{i=0}^{K} u^i p_i(\lambda),\end{aligned}$$

there are precisely $n-1$ polynomials

$$\{p_{i_0}(\lambda), p_{i_1}(\lambda), \dots, p_{i_{n-2}}(\lambda) : i_0 < i_1 < \dots < i_{n-2}\}$$

of degree at least two.

Further, in this case, the parameters $(\dots,k(j),\dots;\dots,f_{1,i},\dots;K)$ of M are recoverable from $\bar{\chi}(M)$:

$k(j) = i_j$

$f_{1,i}$ is the coefficient of $u^{n-1+i}\lambda$ (when $c'_{n-1+i,2} = 0$), and

$K =$ the u-degree of $\bar{\chi}(M) = i_0 + (i_1 - i_0)\cdot c'_{i_1,n-1}$ $(n > 2)$.

2. Equivalently, M is a near-design if and only if there are precisely $n-1$ nonzero terms of s-degree greater than one in $F_B(M)$ (see (5.7)), where $F_B(M)$ is computed from $t(M)$ by (5.9.6). (The parameters can then be obtained from the degrees of the terms and from the nonzero coefficients $\{f_{1,j}\}$.)

3. If M is a near-design with parameters $(\dots,k(j),\dots;\dots,\hat{f}_{1,j},\dots;K)$, then the nonzero coefficients $\{f_{ij}\}$ in $F(M) = F_B(M)$ are given by:

$$f_{n,k(0)} = 1,$$

$$f_{n-i,k(i)-i} = \prod_{m=0}^{i-1} \frac{K-k(m)}{k(i)-k(m)} \qquad (1 \le i \le n-2)$$

$$f_{1,j} = \hat{f}_{1,j} \qquad (j = 0,\dots,K-n; \hat{f}_{1,j} \neq 0)$$

$$f_{0,K} = 1.$$

4. If the parameters of a near-design M are given as in (5.12), then the Poincaré polynomial of M is given by:

$$\bar{\chi}(M;u,\lambda) = u^K + \sum_s f_{1,s} \cdot u^{n-1+s}(\lambda-1) + \sum_{i=0}^{n-2} u^{k(i)} p_i(\lambda)$$

where, for all i:

$$p_i(\lambda) = \left(\prod_{m=0}^{i-1} \frac{K-k(m)}{k(i)-k(m)}\right) \bullet (\lambda^{n-i}-1) + \sum_{j=i+1}^{n-2} \left(\left(\frac{k(i)-K}{k(j)-k(i)}\right) \cdot \left(\prod_{\substack{m=0\\ m\neq i}}^{j-1} \frac{K-k(m)}{k(i)-k(m)}\right) \bullet (\lambda^{n-j}-1)\right) - \sum_s \left(f_{1,s} \left(\prod_{\substack{m=0\\ m\neq i}}^{n-2} \frac{(n-1+s)-k(m)}{k(i)-k(m)}\right) \bullet (\lambda-1)\right).$$

5. The Tutte polynomial of a near-design is equal to:

$t(M;x,y) = \sum a_{ik}(x-1)^{n-i}(y-1)^{k-n+i}$, where

$$a_{ik} = \binom{k(i)}{k} \cdot \left(\prod_{m=0}^{i-1} \frac{K-k(m)}{k(i)-k(m)} \right) + \sum_{i'=0}^{i-1} \left(\binom{k(i')}{k} \cdot \left(\frac{k(i)-K}{k(i')-k(i)} \right) \cdot \left(\prod_{\substack{m=0 \\ m \neq i'}}^{i-1} \frac{K-k(m)}{k(i')-k(m)} \right) \right)$$

$$(i \leq n-2),$$

$$a_{n-1,k} = \sum_{s} \left(\binom{n-1+s}{k} + \sum_{i=0}^{n-2} \left(\binom{k(i)}{k} \cdot \left(\frac{n-1+s-K}{n-1+s-k(i)} \right) \cdot \left(\prod_{\substack{m=0 \\ m \neq i}}^{n-2} \frac{K-k(m)}{k(i)-k(m)} \right) \right) \cdot f_{1,s} \right)$$

$$a_{n,k} = \binom{K}{k} - \sum_{i=0}^{n-1} a_{ik} \quad .$$

Proof. 1. The λ-polynomial coefficient, $p_i(\lambda)$, of u^i in $\bar{\chi}(M;u,\lambda)$ is,by definition,a sum of characteristic polynomials of flats of size i. The degree of a nonzero $p_i(\lambda)$ is the maximal corank of such a flat. Thus, the number of distinct polynomials of degree at least two is the number of sizes of flats of corank at least two. This number is clearly at least $r(M) - 1$ (there is at least one polynomial $p(\lambda)$ of every degree corresponding to the largest flat of that corank). For near-designs, this number equals $r(M)-1$. Further, if the flats of fixed corank were not all the same size, let j be the maximum corank for which there were $k > 1$ different flat sizes. Then, there would be k polynomials $\{p_i(\lambda)\}$ of degree j, and thus there would be more than $r(M) - 1$ polynomials $\{p_i(\lambda)\}$ of degree greater than two. The formulas for the parameters follow from the definition of $\bar{\chi}(M;u,\lambda)$ where K, the number of points of M, is given by the number of loops (the exponent i_0 of the u-co-fficient of λ^n in $\bar{\chi}$) plus the sum of the (nonloop) multiplicities of all atoms. But,if $n > 2$, all $|\bar{M}|$ atoms have the same nonloop multiplicities, $(i_1 - i_0)$.

Here, i_1 is the exponent of u in the unique polynomial $u^{i_1}p_{i_1}(\lambda)$ of λ-degree $n-1$, and $|\bar{M}|$, the number of atoms, is the coefficient $c'_{i_1,n-1}$ of the leading term of this polynomial (corresponding to the number of characteristic polynomials summed).

2. By the definition of a near-design, all nonzero terms in $F(M)$ appear on the border.

3. These formulas come from the fact that the truncation of M, $T(M)$, is a design, so that we may use the identity (*) developed in (5.13.1).

4. The formulas for $p_i(\lambda)$ come from the fact that

$$p_i(\lambda) = \sum_{x:r(x)=i} \left(\sum_{y:y\geq x} \mu(x,y)\lambda^{\operatorname{cor}(y)} \right) .$$

If $\operatorname{cor}(y) \neq 0$, then the interval $[x,y]$ is a design and we recognize the formula in (5.13.4). Thus, the formula for $p_i(\lambda)$ is correct up to a constant (the coefficient of $\lambda^{\operatorname{cor}(M)}$). But this term is correct also, since $p_i(\lambda)$ is a sum of (nontrivial) characteristic polynomials, and thus $p_i(1) = 0$.

5. We could prove these identities from the polynomial formula in (3.18.4). However, we will argue directly, as it shows a typical Möbius inversion argument and prefigures methods to appear in Part II. From formula (3.3.1), we see that (5.14.5) is equivalent to showing that a_{ik} is the number of subsets $A \subseteq S$ of rank i and cardinality k. Thus: $a_{ik} = \sum_{x:r(x)=i} Sp(x,k)$ where $Sp(x,k)$ counts the size-k spanning sets of x. We now invert the following formula for a fixed flat y of rank i:

$$\binom{k(i)}{k} = \sum_{x:x\leq y} Sp(x,k)$$

to obtain:

$$Sp(y,k) = \sum_{x:x\leq y} \binom{|x|}{k}\mu(x,y).$$

Hence,

$$a_{ik} = \sum_{y:r(y)=i}\ \sum_{x:x\leq y} \binom{|x|}{k}\ \mu(x,y)$$

$$= \sum_{i'=0}^{i} \binom{k(i')}{k}\ c_{i'j} \qquad \text{where } c_{i'j} \text{ is given}$$

in (5.13.4).

Various instances of (5.13) and (5.14) have appeared in the literature and we list some below. Formula (5.15.5) is in [37] and the rest are in [27]. Note, that if some truncation of a matroid is a near-design, then the parameters of the truncation may be recovered from t(M); and, conversely, some knowledge of t(M) may be obtained from those parameters by using (5.14) along with (4.2).

Corollary 5.15 Let M be a matroid of rank n and cardinality K, with $t(M) = \Sigma b_{ij}x^iy^j$.

1. All p-element subsets of M are independent if and only if $b_{n-q,j} = 0$ for all $q < p$, $j > 0$. If all p-element subsets of M are independent (so that $T^{n-p-1}(M)$ is a near-design with parameters $k(i) = i$), then the number of flats of corank k and nullity j is counted for $k \geq n-p$ and all j by:

$$f_{k,j} = \sum_{s=k}^{n}\ \sum_{t=0}^{n-s} (-1)^t \binom{n-s}{t}\binom{s}{k} b_{s,j+t}\ .$$

The Whitney number of the second kind $W_{n-k} = \sum_j f_{k,j}$ is then given (for $n-k \le p$) by

$$W_{n-k} = \binom{n}{k} + \sum_{s=k}^{n-1} \sum_{i=0}^{n-s-1} (-1)^i \binom{n-s-1}{i} \binom{s}{k} b_{si} .$$

2. If all p-element subsets of M are independent, then for all $s \ge n-p$,

$$b_{sj} = \sum_{v \ge j} \binom{n-1-s+v-j}{n-1-s} \sum_{q \ge s} (-1)^{q-s} \binom{q}{s} f_{q,v} .$$

3. M is a paving matroid (a near-design with $k(n-2) = n-2$) if and only if $b_{ij} = 0$ for all $i \ge 2$ and $j \ge 1$. Further,

$$b_{i0} = \binom{K-i-1}{n-i} \quad \text{for all} \quad i \ge 2$$

$$b_{10} = \sum_v \binom{n-2+v}{n-2} f_{1,v} - \binom{K-1}{n-2} - \binom{K-2}{n-2}$$

$$b_{1j} = \sum_{v \ge j} \binom{n-2+v-j}{n-2} f_{1,v}$$

$$b_{0j} = \binom{K-j-1}{n-1} - \sum_{v \ge j} \binom{n-1+v-j}{n-1} f_{1,v} .$$

In particular, M is a truncated boolean algebra if and only if $b_{ij} = 0$ for all $i \cdot j \ne 0$. In this case,

$$t(T^{K-n}(B^K)) = \sum_{p=0}^{n-1} \binom{K-n-1+p}{p} x^{n-p} + \sum_{q=0}^{K-n-1} \binom{n-1+q}{q} y^{K-n-q} .$$

4. M is a combinatorial geometry if and only if $b_{n-1,j} = 0$ for all $j \ge 1$. In this case:

$$b_{n-2,0} = \left(\sum_v (v+1) f_{n-2,v} \right) - K(n-1) + \binom{n}{2} ,$$

and

$$b_{n-2,j} = \sum_v (v+1-j)f_{n-2,v} \quad (j > 0).$$

The number of points, W_1, is given by $K = n+b_{n-1,0}$, and the number of lines, W_2, is given by:

$$\binom{n}{2} + b_{n-2,0} - b_{n-2,1} + (n-1)b_{n-1,0}$$

$$= b_{n-2,0} - b_{n-2,1} + K(n-1) - \binom{n}{2} \quad .$$

5. If M is a design with parameters $k(i)$ for all i, then

$$t(M;x,y) = (x-1)^n \, S_{KN} \, (M;\frac{1}{x-1},(x-1)(y-1))$$

where S_{KN}, the cardinality-nullity polynomial, is given by:

$$S_{KN}(M;y,z) = (1+yz)^{k(0)}\int\bar{k}(1)(1+yz)^{n(1)}\int\ldots\int\bar{k}(i)(1+yz)^{n(i)}\ldots\int\bar{k}(n)(1+yz)^{n(n)} (dy)^n$$

where the "i^{th} excess nullity" $n(i)$, equals $k(i) - k(i-1) - 1$; $\bar{k}(i) = K-k(i-1)$, and $\int dy$ is the formal integral operator defined in (5.1).

Exercises 5.16 1. Prove the formulas in (5.15) from the general formulas in (5.14).

2. Extend Example 5.6 by finding an example of two combinatorial geometries G_1 and G_2 such that $F(G_1) = F(G_2)$, but either $t(G_1) \neq t(G_2)$ or $F(G_1^*) \neq F(G_2^*)$. What is the smallest such pair?

Research Problems 5.17

1. Find, if possible, two matroids M_1 and M_2 which are not isomorphic, but such that with a suitable relabeling of their points,

$$M_1 - p_i \cong M_2 - p_i \quad \text{and} \quad M_1/p_i \cong M_2/p_i$$

for all i.

2. What relationships other than (5.10) exist between the closed set-cardinality numbers $\{f_{ij}\}$ and those for the dual $\{f^*_{i,j}\}$ (i.e., the cycle-cardinality numbers $\{c_{i,j}\}$)?

3. Find examples of near-designs (without loops or multiple points) which are not designs or paving matroids.

4. Extend the formulas in (5.14) to matroids all of whose flats of rank $i + 1$ are larger than the flats of rank i for all i. For example, show that for such matroids M (where $F(M) = F_B(M)$), $t(M)$ can be reconstructed from $F(M)$.

5. Can the Tutte polynomial of a matroid be reconstructed from the Tutte polynomials of its hyperplanes?

6. Identities, Inequalities, and Extremal Matroid Theory.

"Research Problems" 6.1 1. Is the following the Tutte polynomial of a matroid?

$$\begin{array}{lll} x^3 + 108x^2 + 891x & & \\ & + 999xy & + 891y \\ & + 888xy^2 & + 1782y^2 \\ & \vdots & \vdots \\ & + (10-j)\cdot 111\cdot xy^j & + \left[\binom{110-j}{2} - 111\cdot\binom{11-j}{2}\right]y^j \\ & \vdots & \vdots \\ & + 111xy^9 & \\ & & + y^{108} \end{array}$$

By (5.15.4), we see that if such an M could be found, it would be a planar geometry with $K = 111$ points, $f_{1,9} = 111$, and $f_{1,j} = 0$ for $j \neq 9$. Thus, it must be a projective plane of order 10. Clearly such a problem will not be resolved using Tutte-Grothendieck recursion! Related problems include the following:

2. Assume that in $t(M)$: $b_{k,0} = 1$, $b_{k-1,0} = 3$, $b_{1,2} = 0$, and $b_{2,0} = 2b_{1,0} \neq 0$. Is $\frac{\sqrt{4k+9}-1}{2}$ a prime power? To answer this question, consider M^*. From $b_{k,0} = 1$, $b_{k-1,0} = 3$ and $b_{10} \neq 0$, it is not hard to show that M^* is connected, has rank three, and has cardinality $K = k+3$. Since $b^*_{2,1} = 0$, it is a planar geometry. But for a planar geometry, M^*, with K points, (5.15.4) gives the number of lines, W_2, as $b^*_{1,0} - b^*_{1,1} + 2K-3 = b^*_{1,0} - b^*_{1,1} + 2b^*_{2,0} + 3$. Thus,

$W_2 - W_1 = b^*_{1,0} - b^*_{1,1} + b^*_{2,0}$ which by (6.4) below is equal to $2b^*_{0,1} - b^*_{0,2}$. This is zero if and only if M^* has an equal number of points and lines (i.e., is a connected projective plane). For such a plane of order n, we would have $n^2 + n + 1 = k+3$, so that $n = \frac{\sqrt{4k+9}-1}{2}$.

3. Can we have a Tutte polynomial where, for $n > 6$, $b_{n,0} = 1$, $b_{2,1} = 0$, $b_{1,0} \neq 0$, and

$$\sum_{s=1}^{n} s \cdot \left[\sum_{t=0}^{n-s} (-1)^t \binom{n-s}{t} \right] b_{s,t} = 0 \text{ ?}$$

The above initial conditions mean that M would be a connected paving matroid of rank at least seven. The equation, by (5.15.1), reflects the fact that in M, $f_{1,0} = 0$. Thus, M has no independent hyperplanes. Thus, the set of hyperplanes H of M have the property that each has at least n points, and that any subset of $n-1$ points is in exactly one hyperplane. Thus, H forms a t-design (with perhaps multiple non-trivial blocks) for $t > 5$, and any such t-design gives a paving matroid. The existence of t-designs with $t > 5$ is at present a famous open problem.

The examples above show that it is as impossible to characterize the image of the map $M \to \mathbb{Z}[x,y]$ of (3.7) (i.e., determine all possible Tutte polynomials) as it is to characterize its domain (determine all matroids). The kernel of the map is equally intractable.

We have seen many examples (3.11, 3.14, 4.3, 4.5) of two (or more) matroids with the same Tutte polynomial. An elementary counting argument shows that for large K this situation only gets worse: there are many more matroids than Tutte polynomials.

Proposition 6.2. For any $\varepsilon > 0$, there is a K sufficiently large, so that while there are more than $2^{2^{K(1-\varepsilon)}}$ nonisomorphic matroids all with the same Tutte polynomial, there are less than 2^{K^3} distinct Tutte polynomials of matroids of size K.

Proof. Let M be a paving matroid of cardinality K and rank n all of whose hyperplanes have nullity 0 or 1. Then, since every $(n-1)$-element subset is in a unique hyperplane, we have $f_{1,0} = \binom{K}{n-1} - nf_{1,1}$, while $f_{1,j} = 0$ for $j > 1$. A consequence of (5.15.3) is then that all such matroids with a fixed number $f_{1,1}$ of dependent hyperplanes have the same Tutte polynomial. Results of Knuth ([86], or see [151]) show that, when $n = \left[\frac{K}{2}\right]$, there exists a family F_K of $a_K \geq \binom{K}{\left[\frac{K}{2}\right]}/2K > \frac{2^K}{c\cdot K^{3/2}}$ subsets of K, each subset of size $\left[\frac{K}{2}\right]$, such that any subfamily of F_K can be the family of nullity-one hyperplanes of such a paving matroid. Letting b_K be the number of subfamilies of F_K each containing $f_{1,1} = \left[\frac{a_K}{2}\right]$ members, we obtain $b_K = \binom{a_K}{f_{1,1}} > \frac{2^{a_K}}{c\cdot\sqrt{a_K}}$ matroids all with the same Tutte polynomial. Dividing by $K!$ and using elementary estimates we get the first statement.

To count the number of distinct Tutte polynomials observe that, in the corank-nullity polynomial, there are $(K+1)^2$ coefficients $\{a_{ij}\}$ all of which are nonnegative and which sum to 2^K. Thus, there are at most $\begin{pmatrix} 2^K+K^2+2K \\ K^2+2K \end{pmatrix} < 2^{K^3}$ choices for coefficients (and distinct polynomials).

Although the estimate above for the number of distinct Tutte polynomials is small compared with the number of matroids, the actual number of Tutte polynomials is even smaller. Aside from those subtle considerations pointed out in (6.1), there are several identities and equalities which the coefficients $\{b_{ij}\}$ must satisfy. The identities can be characterized completely with reasonable ease,while the search for inequalities leads into many areas of matroid theory and more general mathematics,and seems endless. We begin by characterizing all (affine linear) identities which hold among the coefficients of $\{t(M)$: M has rank n, cardinality K, and is free of loops, multiple points, and isthmuses $\}$. We make these restrictions,since most applications involve combinatorial geometries (no multiple points),while (4.4.2) and the dual of (4.4.3) show how to reduce to the isthmus-free case.

Proposition 6.3. Let $G_{K,n}$ be the class of all isthmus-free combinatorial geometries of rank n and cardinality K. Further, let $M_{K,n}$ be the affine variety spanned by the set of all $(K+1) \times (n+1)$ matrices $\{M_{K,n}\}$ such that the (i,j)-th entry of $M_{K,n}$ is the coefficient a_{ij} in the cardinality-corank polynomial (see 3.17.1) $S_{KC}(G;z,u)$ for some $G \in G_{K,n}$.

1. **The dimension of** $M_{K,n}$ equals $(n-2)\cdot(K-n-1)$. A basis **for the relations** which define $M_{K,n}$ follow:

a. $\mathbf{M(i,n) = 0}$ $\qquad (1 \le i \le K)$

b. $\mathbf{M(i,n-1) = 0}$ $\qquad (i = 0,\ 2 \le i \le K)$

c. $\mathbf{M(i,j) = 0}$ $\qquad (0 \le j \le n-2,\ 0 \le i \le n-1-j)$

d. $\mathbf{M(i,j) = 0}$ $\qquad (1 \le j \le n-2,\ K-j \le i \le K)$

e. $$\mathbf{M(i,n-i)} = \binom{K}{i} - \sum_{j=n-i+1}^{n} M(i,j) \qquad (0 \le i \le n)$$

f. $$\mathbf{M(i,0)} = \binom{K}{i} - \sum_{j=1}^{n-2} M(i,j) \qquad (n+1 \le i \le K)$$

2. **The** following identities form a basis for the relations which **hold among** the coefficients (with nonnegative subscripts) in the Tutte **polynomial**

$$\{b_{ij} : t(G) = \Sigma b_{ij} x^i y^j,\ G \in G_{K,n}\}:$$

a. $b_{i,j} = 0 \qquad (i > n,\ j \ge 0)$

b. $b_{n,0} = 1\ ;\ b_{n,j} = 0 \qquad (j > 0)$

c. $b_{n-1,0} = K-n\ ;\ b_{n-1,j} = 0 \qquad (j > 0)$

d. $b_{i,j} = 0 \qquad (1 \le i \le n-2,\ j \ge K-n)$

e. $b_{0,K-n} = 1\ ;\ b_{0,j} = 0 \qquad (j > K-n)$

f. $$I_k = \sum_{s=0}^{k} \sum_{t=0}^{k-s} (-1)^t \binom{k-s}{t} b_{s,t} = 0 \quad (0 \le k \le K-3).$$

Proof. **1.** These identities are found in [38] where they are shown **to be a basis.**

2. One easily checks that identities (a-f) are independent since each involves a coefficient b_{ij} not found in any previous one. (For example, I_k can be interpreted as an equation for $b_{n-2,k-n+2}$ if $n-2 \le k \le K-3$, and as an equation for $b_{k,0}$ if $0 \le k < n-2$.)

Further, identities (a-e) leave an $(n-1)$ by $(K-n)$ rectangle of coefficients undetermined, and adding in identities $\{I_k : 0 \le k \le K-3\}$ gives the dimension of $M_{K,n}$ for the number of degrees of freedom. Thus, by (3.18.3) which can be thought of as giving an invertible affine map between the coefficients of S_{KC} and those of t, there are no more identities.

Identities (a-e) are obvious. For example, $b_{i,K-n} = \delta(i,0)$ follows from the fact that G has no isthmuses, and (c) reflects the fact that the loopless geometry G has no multiple points. To prove (f), we first note that it is independent of n and only uses K in a bound on k. In fact, we will prove $\{I_k\}$ for all matroids M' with $|M'| > k$. These identities first appeared in [27]. Our alternate proof below uses equation (3.18.3) evaluated at $u = 1$. Let M' be any matroid of rank k and cardinality K'. Then,

$$S_{KC}(M';z,1) = z^k t(M';\frac{z+1}{z}, z+1), \quad \text{so that}$$

$$(z+1)^{K'} = \sum_{i,j} b_{ij}(z+1)^{i+j} z^{k-i}.$$

Letting $v = z+1$, we get:

$$v^{K'} = \sum_{i,j} b_{ij} v^{i+j}(v-1)^{k-i}, \quad \text{or}$$

$$v^{K'-k} = \sum_{i,j} b_{ij} \sum_{m=0}^{k-i} (-1)^m \binom{k-i}{m} v^{j-m} .$$

Considering the constant term on the right $(m=j)$, we get that whenever $K' > k$,

$$\sum_{s,t} (-1)^t \cdot \binom{k-s}{t} \cdot b_{s,t} = 0.$$

This is precisely identity I_k if $r(M') = k$. To show I_k for a general M', we use induction on $|r(M') - k|$. First, let $r(M') = n' > k$, and assume that we have proved I_k on all matroids of size at least $k+1$ and rank $n'-1$. Using a second induction on the number of nonfactors of M', we get that I_k certainly holds if M' is totally separable, since then the nonzero coefficient $b_{n',j}$ in $t(M')$ does not appear in I_k. But, if p is a nonfactor, then $|M'| \geq k+2$, $t(M') = t(M'-p) + t(M'/p)$, and I_k holds, by induction on the number of nonfactors, in $M'-p$, and, by induction on rank, in $t(M'/p)$. Thus, by linearity, it holds in $t(M')$.

Now, assume $k > n'$, and that we have proved I_k for all matroids of rank $n' + 1$ (and cardinality at least $k+1$). Let M' have rank n' and size at least $k+1$. M' is certainly not a boolean algebra so that we may make a free coextension, adding a nonfactor p freely to M'^* obtaining M''^* with $M''/p = M'$. Then, $t(M') = t(M'') - t(M''-p)$. The two matroids M'' and $M''-p$ have rank $n'+1$ and size at least $k+1$, so I_k holds for each. Thus, it holds for $t(M')$.

We now list the first few instances of $\{I_k\}$ for future reference, using identities $I_{k'}$, with $k' < k$ to simplify I_k.

<u>Corollary 6.4</u> The following identities $\{I_k\}$ hold on the coefficients of the Tutte polynomial $t(M)$ for any matroid M with $|M| > k$.

I_0. $b_{0,0} = 0$

I_1. $b_{10} = b_{01}$

I_2. $b_{20} - b_{11} + b_{02} = b_{10}$

I_3. $b_{30} - b_{21} + b_{12} - b_{03} = b_{11} - 2b_{02} + b_{10}$.

We now turn our attention to inequalities involving the coefficients $\{b_{ij}\}$. Clearly, the most obvious one is that $b_{ij} \geq 0$ for all (i,j). However, this can be sharpened.

Proposition 6.5 Let M be a connected matroid, and assume that $b_{ij} > 0$ in its Tutte polynomial. Then $b_{i',j'} > 0$ for all $(i',j') \neq (0,0)$ with $(i',j') \leq (i,j)$.

Proof. If $b_{ij} > 0$ in $t(M)$, then, somewhere in a decomposition of M (see (3.1), (3.4)), there is the term B^{ij}, and thus M has this totally separable matroid as a minor. Thus, it has $B^{i',j'}$ as a minor for all $(i',j') : (0,0) < (i',j') \leq (i,j)$. We may now apply (4.12).

A special case of (6.5) (and I_1 of (6.4)) is the theorem of Crapo [53] that, for any matroid M with at least two points,

$b_{10} = b_{01} = \beta(M)$ is positive if and only if M is connected.

We will explore the invariant $\beta(M)$ in more detail below ((6.15),(6.22.2,3), (6.24.2), (6.26.4)).

To determine which b_{ij} can be positive for a general matroid M, we may first assume that M has no loops or isthmuses, since otherwise we can reduce to this case by (4.4). The number of connected (direct-sum) components of M can be determined from $t(M)$ and is equal to k, where (in $t(M)$), $b_{k,0} > 0$ and $b_{k-1,0} = 0$.

For such matroids with k connected components, an easy application of (3.6) shows that $b_{i,k-i}=c > 0$ for all $i : 0 \leq i \leq k$, and that $b_{i,j} = 0$ for all $i+j < k$. Therefore, in theory, the possibilities for which b_{ij} are positive can be reduced to the connected case since the possible positive b_{ij} of a matroid with rank n, cardinality K, and k components come from all possibilities of nonzero terms in $t(M_1)\cdot t(M_2)\cdot\ldots\cdot t(M_k)$ where each M_i is connected, $\sum_i |M_i| = K$, and $\sum_i r(M_i) = n$. In particular, we note that the set of indices $\{(i,j) : b_{ij} > 0\}$ forms a rectilinear convex set in the integer lattice $\mathbb{Z} \times \mathbb{Z}$ in the following sense. The sequence $b_{K,0}, b_{K-1,0},\ldots,b_{k,0}, b_{k-1,1},\ldots,b_{k-j,j},\ldots,b_{0,k},b_{0,k+1},\ldots,b_{0,K-n}$ gives the "northeast boundary" of positive coefficients, and the border sequence of (5.7) gives the "southwest boundary". Further, $b_{ij} > 0$ if and only if it "lies within the boundaries" (e.g., if there is a positive $b_{ij'}$, in the northeast boundary and a $b_{ij''}$ in the southwest boundary with $j' \leq j \leq j''$). To complete our analysis, we give the possibilities for border terms in connected matroids. As a preliminary, we discuss an interesting class of matroids introduced in [114] which will also be useful later (see (6.23)).

<u>Definition 6.6</u> A *nested matroid* (of cardinality K and rank n) is one in which the cyclic flats are totally ordered in that if F and F' are cyclic flats with $|F| \leq |F'|$, then $F \subseteq F'$. These matroids were first defined in [114]. An alternate definition is that there exists an ordered basis $B = \{b_1,\ldots,b_n\}$ such that every point

p not in the basis (and not a loop) forms a circuit with an initial segment $\{b_1,\ldots,b_k\}$ for some k. The cyclic flats are then subsets of the form $C_k = \{b_1,\ldots,b_k\} \cup P'_k$ where P'_k is the set of points which form circuits with some (initial or empty) subset of $B_k = \{b_1,\ldots,b_k\}$. This is clearly closed and is a union of circuits precisely when $P'_k - P'_{k-1}$ is nonempty (i.e., when b_k is not an isthmus in $\bar{B}_k$).

The following facts are either found in [114] or can be easily demonstrated by the reader.

1. A nested matroid is determined up to isomorphism by the sequence $(a_0,a_1,\ldots,a_n)$, where a_0 is the number of loops, and, for $i > 0$, $a_i = 1 + |P'_i - P'_{i-1}| = |\bar{B}_i - \bar{B}_{i-1}|$. Here, of course, $\sum_i a_i = K$, and M is a geometry if and only if $a_0 = 0$ and $a_1 = 1$. We will hereafter refer to the (unique) nested matroid $N(a_0,\ldots,a_n)$. Note that any sequence $(a_0,\ldots,a_n)$ gives a nested matroid of rank n if $a_0 \geq 0$ and $a_i > 0$ for all $i > 0$.

2. $N(a_0,\ldots,a_n)$ is connected if and only if it has no loops $(a_0 = 0)$ and no isthmuses $(a_n > 1)$.

3. The connected nested matroid $N(a_0,\ldots,a_n)$ of rank n and nullity K is determined by the sequence:

(*) $$((i_0,j_0), (i_1,j_1),\ldots,(i_m,j_m)),$$

with $$0 = i_0 < i_1 < \ldots < i_m = n, \text{ and}$$

$$0 = j_0 < j_1 < \ldots < j_m = K-n.$$

Here, $i_k = r(C_k)$, the rank of the k^{th} largest cyclic flat C_k, and $j_k = |C_k| - r(C_k)$, the nullity of C_k. Any such sequence of pairs parameterizesa connected nested matroid. In particular, $N(a_0,\ldots,a_n)$, with $a_0 = 0$ and $a_n > 1$, has a nonempty cyclic flat of rank i and nullity j if and only if $a_i > 1$, in which case $j = \sum_{k=0}^{i} a_k - i$. Conversely, given any sequence of pairs satisfying (*), let $a_{i_k} = 1 + j_k - j_{k-1}$ if (i_k,j_k) is in the sequence (*), while $a_i = 1$ otherwise (conventionally, $j_{-1} = 1$).

4. The class of nested matroids is closed under the following operations:

a. Truncation: $T(N(a_0,\ldots,a_n)) = N(a_0,\ldots,a_{n-2},a_{n-1} + a_n)$.

b. Free extension: $N(a_0,\ldots,a_n) + p = N(a_0,\ldots,a_n + 1)$.

c. Deletion: $N(a_0,\ldots,a_n) - p_i = N(a_0,\ldots,a_i-1,\ldots,a_n)$

where $p_i \in \bar{B}_i - \bar{B}_{i-1}$. We use the conventions that, for $i > 0$, $N(a_0,\ldots,0,a_{i+1},\ldots,a_n) = N(a_0,\ldots,1,a_{i+1}-1,\ldots,a_n)$, and that $N(a_0,\ldots,a_{n-1},0) = N(a_0,\ldots,a_{n-1})$.

d. Contraction: $N(a_0,\ldots,a_n)/p_i = N(a_0,\ldots,a_{i-2},a_{i-1} + a_i-1, a_{i+1},\ldots,a_n)$.

e. Free coextension: $N(a_0,\ldots,a_n) \times p = N(0,a_0 + 1,a_1,\ldots,a_n)$.

f. Duality: If a nested matroid N of rank n and cardinality K is parameterized by its sequence of cyclic flats as in (*) above, then N^* has rank K-n and has the sequence $((i_0^*,j_0^*),\ldots,(i_m^*,j_m^*))$ where $(i_k^*, j_k^*) = (K-n-j_{m-k},n-i_{m-k})$. (For this, recall that A is a cyclic flat of M^* iff S-A is a cyclic flat of M.)

We leave as an exercise to the reader the explicit formula for a_i^* when

$$N(a_0^*,\ldots,a_{K-n}^*) = (N(a_0,\ldots,a_n))^*.$$

5. The hereditary class of nested matroids has,as excluded minors, the sequence

$$M_i = T^{i-2}(T(B^i) \oplus T(B^i)) \qquad (i \geq 2).$$

Thus, M_2 is a line with two double points, M_3 is the matroid M_2 of (4.3.1), and, in general, M_i consists of two disjoint i-point circuits otherwise freely placed in a space of rank i.

6. To get the Tutte polynomial $t(N(a_0,\ldots,a_n))$, we will use the cardinality-corank polynomial and apply (3.18.3). If S' is a subset consisting of s_i points in $\bar{B}_i - \bar{B}_{i-1}$ $(i = 0,\ldots,n)$, then $r(S')$ is given recursively by $f_n(s_0,\ldots,s_n) = f_n(\underline{s})$, where, for all i, $f_0(\underline{s}) = 0$, and $f_i(\underline{s}) = \min(f_{i-1}(\underline{s}) + s_i, i)$. This is easily shown by induction since each point of $S_i' = S' \cap (\bar{B}_i - \bar{B}_{i-1})$ is in free position in rank i, and so adds one to the rank of S' (unless rank i is reached). Thus:

$$S_{KC}(N(a_0,\ldots,a_n);z,u)$$

$$= \sum_{s_0=0}^{a_0}\cdots\sum_{s_n=0}^{a_n} \binom{a_0}{s_0}\cdots\binom{a_n}{s_n}\cdot z^{s_0+\ldots+s_n}\cdot u^{n-f_n(\underline{s})}$$

Proposition 6.7 Necessary and sufficient conditions for possible sets S of indices $\{(i,j)\}$ of positive coefficients in t(M) for a connected matroid M $(|M| > 1)$ are that:

1. $(0,0) \notin S$

2. For some i, $(i,0) \in S$ and $(i+1, 0) \notin S$. In this case,

$(i,j) \notin S$ for all $j > 0$. Similarly, for some j, $(0,j) \in S$ and $(0,j+1) \notin S$. Then, $(i,j) \notin S$ for all $i > 0$.

3. If $(i,j) \in S$ then $(i',j') \in S$ for all $(i',j') \leq (i,j)$. $((i',j') \neq (0,0).)$

Proof. The necessity of (6.7.1) and (6.7.3) were shown in (6.5). Condition (6.7.2) comes from the fact that M, being connected, has no loops or isthmuses. The sufficiency of the above conditions amounts to showing that any set of indices:

$$\{(i_0,j_0),\ldots,(i_m,j_m) : i_0 > i_1 > \ldots > i_m = 0,$$

$$0 = j_0 < j_1 < \ldots < j_m \quad , \quad m \geq 2\}$$

is possible for the corners of $t_B(M)$, where M is a connected matroid (see (5.7), (5.8)). But, when each i_j is subtracted from i_0 (converting corank to rank), this is precisely condition (*) in (6.6.3). Thus, there is a connected nested matroid with these corners.

We mention some more subtle inequalities on the set $\{b_{ij}\}$.

Proposition 6.8 1. Let G be a geometry of rank $n > 2$ and cardinality K. Then:

$$b_{n-2,1} - b_{n-2,0} \leq K(n-2) - \binom{n}{2} .$$

Equivalently:

$$b_{n-2,1} \leq b_{n-2,0} + (n-2)b_{n-1,0} + \binom{n-1}{2} - 1.$$

Further, equality holds if and only if $n=3$ and G is modular.

2. For any matroid M with Tutte polynomial $t(M) = \Sigma b_{ij}x^i y^j$, we have

$$\sum_{i,j;i',j'} a^i \cdot b^{i'} \cdot (d^j c^{j'} - c^j d^{j'}) \cdot b_{ij} \cdot b_{i'j'} \geq 0,$$

and $$\sum_{i,j;i',j'} j \cdot d^{j'} \cdot d^{j-1} \cdot (i' \cdot b^{i'-1} b^i - i \cdot b^{i'} b^{i-1}) \cdot b_{ij} \cdot b_{i'j'} \geq 0$$

for all a, b, c, and d with $0 \leq a \leq b$, $0 \leq c \leq d$, and $(b-1)(d-1) \geq 1$.

Proof. 1. This is the line-point inequality for geometries: $W_2 \geq W_1$ with equality if and only if G is a modular plane (see (5.15.4)).

2. These, and other, inequalities come from the FKG inequality of statistical mechanics interpreted for $t(M)$ in [127].

We remark that there are two types of inequalities which we have considered. One type (e.g., $b_{10} > 0$ for connected matroids) can be proved inductively using properties of the Tutte decomposition (T1 and T2), while the other type (such as (6.8.1)) use other arguments and cannot be (directly) deduced from the decomposition. Obviously, those of the latter type are more difficult to discover and prove.

The coefficients of $t(M)$ which have received the most attention by researchers in matroid theory are those of the geometric Tutte polynomial

$$\bar{t}(G) = \sum_{i=1}^{n} b_i x^i$$

and the related Whitney numbers of the first kind: the coefficients

$\{w'_i\}$ of the characteristic polynomial

$$\chi(G) = \sum_{i=0}^{n} w'_i\lambda^{n-i} = (-1)^{n}\cdot\bar{t}(G;1-\lambda)$$

Here, we assume G is a geometry, and we will henceforth treat the *unsigned Whitney numbers.*

$$w_i = |w'_i| = (-1)^{i}\cdot w'_i$$

Thus,

$$\text{(6.9.1)} \qquad |\chi|(G) = \sum_{i=0}^{n} w_i\lambda^{n-i} = \bar{t}(G;\lambda+1), \qquad \text{so that}$$

$$\text{(6.9.2)} \qquad w_{n-i} = \sum_{m=i}^{n} \binom{m}{i} b_m \ .$$

The principal conjecture is that the sequence $(w_0 = 1,\ w_2 = K, \ldots, w_n = |\mu(G)|)$ is unimodal, logarithmically concave, or strongly log concave in a sense which we will define below. First, note that there are several analogies of the two kinds of Whitney numbers (both of which are conjectured to give log concave sequences). (Proofs are easy applications of (6.9.2).)

$$\text{(6.9.3)} \qquad W_i = \sum_{r(x)=i} 1 \ \le\ w_i = \sum_{r(x)=i} |\mu(0,x)|\,, \text{ with equality,}$$

$$\text{(6.9.4)} \qquad w_i = W_i = \binom{K}{i}, \text{ iff all } (i+1)\text{-element subsets of } G$$

are independent.

(6.9.5) $w_0 \le w_1 \le \ldots \le w_{\left[\frac{n}{2}\right]}$. That $W_0 \le W_1 \le \ldots \le W_{\left[\frac{n}{2}\right]}$ is still only a conjecture.

(6.9.6) $w_{n-i} \ge w_i$ for all $i \le \left[\frac{n}{2}\right]$. That $W_{n-i} \ge W_i$ is yet unproved.

It is not even known at the present time whether (for $n \ge 5$) $W_{n-2} \ge W_2$, or whether, $W_3 \ge W_2$ for $n \ge 4$.

However, it is known that, for all i different from 0 and n, $K \leq w_i$ and $K \leq W_i$.

We now make some definitions and elementary remarks about unimodality and related concepts.

Definition 6.10 1. A sequence of nonnegative integers $a_0, a_1, \ldots, a_n$ with $a_0 = 1$ is said to be *unimodal* if, for some ℓ, $a_0 \leq a_1 \leq \ldots \leq a_\ell \geq a_{\ell+1} \geq \ldots \geq a_n$. This is equivalent to the property that $a_m \geq \min(a_j, a_k)$ for all triples $j < m < k$.

2. The sequence (a_i) is *strongly unimodal* if for some $\ell \leq k$: $a_0 < a_1 < \ldots < a_\ell = a_{\ell+1} = \ldots = a_k > a_{k+1} > \ldots > a_n$. These sequences are characterized by the local properties that for all i, $a_i \geq \min(a_{i+1}, a_{i-1})$, and that, if $a_{i-1} = a_i$, then $a_{i-2} \leq a_i \geq a_{i+1}$. Equivalently, define $\Delta_j = a_{j+1} - a_j$. Then, $\Delta_j \geq 0$ implies $\Delta_{j-1} \geq 0$, and $\Delta_j > 0$ implies $\Delta_{j-1} > 0$.

3. Stronger conditions which guarantee unimodality are also amenable to local considerations. The most obvious such is concavity, the discrete analog of having a nonnegative second derivative. Here $a_i \geq \frac{a_{i+1} + a_{i-1}}{2}$.

Unfortunately, the Whitney numbers of the first (or second) kind are seldom concave (usually, $w_2 \approx \frac{w_1^2}{2}$). However, since (strictly) monotonic functions preserve unimodality (and nonunimodality), a way to prove strict unimodality would be to find a strictly monotonic function whose values on the sequence were concave. It is customary to choose the logarithm function, and a (unimodal) sequence is said to be *log concave* if, for all i, $a_i^2 \geq a_{i-1}a_{i+1}$.

4. We say a sequence is *strongly log concave* if $a_1 = K \geq n$, and the sequence $(a_i' = \frac{a_i}{\binom{K}{i}})$ is log concave. A motivation for this definition is that it includes all sequences arising from truncations of polynomials $p(x)$ with all negative integer roots:

$$p(x) = x^{n+m} + a_1 x^{n+m-1} + \ldots + a_n x^m + \ldots$$

$= \prod_{i=1}^{n+m} (x+c_i)$. Further, for such truncated polynomials, the inequality will be strict $(a_i'^2 > a_{i-1}' a_{i+1}')$ unless all $c_i = 1$. (See [79].) We introduce this concept because it is known to hold for many well-studied sequences of Whitney numbers such as binomial coefficients and Stirling numbers of the first kind. Further, strong log concavity is preserved by the truncation operator since

$$w_i(T^m(G)) = w_i(G) \quad \text{if} \quad i < n-m$$

and

$$w_{n-m}(T^m(G)) = w_{n-m}(G) - w_{n-m+1}(G) + \ldots \quad .$$

It is easy to see that Whitney numbers of the first kind for geometric lattices which come from truncations of boolean algebras, partition lattices, or modular geometries are all strongly log concave. (The polynomials are, respectively, $(x+1)^n$, $\prod_{i=1}^{n} (x+i)$, and $\prod_{i} \prod_{j_i=0}^{n_i} (x+q_i^{j_i})$.)

5. We conjecture that the Whitney numbers of the first kind are strongly log concave.

Thus, we conjecture that

$$(6.10.6) \qquad \frac{w_i^2}{\binom{K}{i}} \geq \frac{w_{i-1}}{\binom{K}{i-1}} \cdot \frac{w_{i+1}}{\binom{K}{i+1}} \quad .$$

Equivalently,

$$(6.10.7) \qquad w_i^2 \geq \left(\frac{K-i+1}{K-i}\right)\left(\frac{i+1}{i}\right) w_{i-1} w_{i+1} .$$

This reflects the feeling that truncated boolean algebras give the "least concave" Whitney numbers (see [101] for analogous conjectures for (W_i)). The related conjecture for the coefficients of $\bar{t}(G)$ is that the sequence:

$$(6.10.8) \qquad b_i' = \frac{b_i}{\binom{K-1-i}{K-1-n}}$$

is log concave and we call this condition strong log concavity for $\bar{t}(G)$. Equivalently, we conjecture that

$$b_i^2 \geq \left(\frac{K-i-1}{K-i}\right)\left(\frac{n-i+1}{n-i}\right) b_{i-1} b_{i+1} \quad .$$

Thus, again for sequences of Tutte coefficients (b_i), truncated boolean algebras are thought to be the "least log concave." (See (5.15.3), or use (4.2).)

Research problems 6.11 1. Find the explicit characterization for the indices of positive b_{ij} for a matroid with k components (see (6.7)).

2. Show that if, for G_1 and G_2, the Whitney numbers or Tutte coefficients are strongly log concave, then

so are these numbers for $G_1 \oplus G_2$. This amounts for Whitney numbers, essentially, to showing that if

(*) $$\sum_{i=0}^{n+m} d_i x^i = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} c_i x^i\right),$$ and if the sequences $\left(a'_i = \frac{a_i}{\binom{n}{i}}\right)$ and $\left(c'_i = \frac{c_i}{\binom{m}{i}}\right)$ are log concave, then so is the sequence $\left(d'_i = \frac{d_i}{\binom{n+m}{i}}\right)$.

This latter inequality (*) may not be hard to prove and is interesting in its own right. It is probably true since it holds when the two polynomials $p(x) = \Sigma a_i x^i$ and $q(x) = \Sigma c_i x^i$ have real negative roots.

Further, it is true for isthmuses, since (*) is proved in [79] for the degree-one case. We also note that the analogous result for the log concavity of (d_i) was shown by Harper (see [81]).

by Harper (see [81]).

2. If $\left(b'_i = \frac{b_i}{\binom{K-1-i}{K-1-n}}\right)$ is log concave, are the coefficients of $\chi(G)$ strongly log concave? In particular, show that the log concavity of (b'_i) implies the log concavity of

$$w'_{n-i} = \sum_{j=i}^{n} \frac{\binom{j}{i}\binom{K-1-j}{K-1-n}}{\binom{K}{n-i}} b'_j .$$

3. Find classes of geometries (such as dual paving matroids as we show below) which give unimodal or strongly log concave Tutte coefficients or Whitney numbers.

4. We cover our bets by offering the problem of finding a geometry whose Whitney numbers are not unimodal.

We will illustrate some techniques with the next two propositions. The first shows that if (b_i) is log concave, then so is (w_i). Again, this is not surprising since if (b_i) came from a polynomial $p(x)$ with real negative roots, then (w_i) would be the coefficients of $p(x+1)$, another polynomial with real negative roots. We begin with a lemma presenting the combinatorial arguments we will use.

Lemma 6.12 1. Let $(a_i : i \geq 0)$ and $(a'_i : i \geq 0)$ be two nonnegative eventually zero sequences, and let $\bar{a}_r = \sum_{i=0}^{r} a_i$ denote the r^{th} partial sum (where $\bar{a}_\infty = \sum_{j=0}^{\infty} a_j$). Assume that (a_i) *dominates* (a'_i) in the sense that, for all i, $\bar{a}_i \geq \bar{a}'_i$.

Further, let $(b_i : i \geq 0)$ and

$(b'_i : i \geq 0)$ be two nonnegative sequences such that, for all i, $b_i \geq b'_i$ and $b_i \geq b_{i+1}$. Then, $\overline{(a \cdot b)}_\infty \geq \overline{(a' \cdot b')}_\infty$.

2. If for all $i \geq 0$, $\frac{a_{i+1}}{a_i} \leq \frac{a'_{i+1}}{a'_i}$ (with $\frac{0}{0} = 0$), and if $\bar{a}_\infty \geq \bar{a}'_\infty$, then $\bar{a}_i \geq \bar{a}'_i$ for all i.

3. Let k and i be fixed. Then, the sequence

$$(a_0 = \binom{k}{i}^2, \ a_j = 2\binom{k+j}{i}\binom{k-j}{i} \ : j \geq 1)$$

dominates the sequence

$$(a'_0 = \binom{k}{i+1}\binom{k}{i-1},\ a'_j = \binom{k+j}{i+1}\binom{k-j}{i-1}+\binom{k+j}{i-1}\binom{k-j}{i+1}\ : j \geq 1)\ .$$

Further, the sequence

$$(b_j = 2\binom{k+j+1}{i}\binom{k-j}{i}\ : j \geq 0)$$

dominates the sequence

$$(b'_j = \binom{k+j+1}{i+1}\binom{k-j}{i-1} + \binom{k+j+1}{i-1}\binom{k-j}{i+1}\ : j \geq 0).$$

<u>Proof</u>. 1. $\overline{(ab)}_\infty = \sum_{r=0}^{\infty} \bar{a}_r(b_r-b_{r+1})$ (where we can assume that (b_i) is eventually zero)

$$\geq \sum_{r=0}^{\infty} \bar{a}'_r(b_r-b_{r+1})$$

$$= \sum_{i=0}^{\infty} a'_i b_i$$

$$\geq \sum_{i=0}^{\infty} a'_i b'_i\ .$$

2. Assume that for some r, $\bar{a}_r < \bar{a}'_r$ and let r be minimal with this property. Then, $a_r < a'_r$, and, for all $s \geq r$, $a_s \leq a'_s$. Thus, $\bar{a}_s < \bar{a}'_s$ for all $s > r$ which contradicts the hypothesis that $\bar{a}_\infty \geq \bar{a}'_\infty$.

3. An elementary combinatorial argument shows that $\bar{a}_\infty = \bar{a}'_\infty = \binom{2k+1}{2i+1}$, while $\bar{b}_\infty = \bar{b}'_\infty = \binom{2k+2}{2i+1}$. Simplifying the proportions $a_{i+1} : a_i :: a'_{i+1} : a'_i$ and $b_{i+1} : b_i :: b'_{i+1} : b'_i$, and applying (6.12.2) yields the result.

We are now ready to prove the log concavity of (w_i) from the log concavity of (b_i). The same proof gives the stronger result that if $(b_i : 1 \le i \le n)$ is log concave, so is $(\hat{w}_i : 0 \le i \le n-1)$, the sequence of *reduced Whitney numbers*.

Reduced Whitney numbers are motivated by the fact that $\chi(G;1) = 0$, so that $\lambda-1$ divides the characteristic polynomial of G. (Equivalently, there is no constant term in $\bar{t}(G)$.) Therefore,

$$(6.12.4) \qquad \frac{|\chi|(G;\lambda)}{\lambda+1} = \sum_{i=0}^{n-1} \hat{w}_i \lambda^{n-i} ,$$

$$(6.12.5) \qquad w_i = \hat{w}_{i+1} + \hat{w}_i , \quad \text{and}$$

$$(6.12.6) \qquad \hat{w}_{n-i-1} = \sum_{m=i}^{n-1} \binom{m}{i} b_{m+1} .$$

Proposition 6.13 Assume that the sequence (b_i) of coefficients of $\bar{t}(G)$ is log concave. Then, the Whitney numbers (w_i) and reduced Whitney numbers $(\hat{w}_i)$ are also log concave.

Proof. By (6.9.2), we have $(w_{n-i})^2 = \left[\sum_{m=i}^{n} \binom{m}{i} b_m\right]^2$. Symmetrizing the expansion of the right-hand side, we obtain:

$$(w_{n-i})^2 = \sum_{k=i}^{n} \left[\binom{k}{i}^2 b_k^2 + 2\sum_{j\ge1} \binom{k+j}{i}\cdot\binom{k-j}{i} b_{k+j} b_{k-j}\right]$$
$$+ \sum_{k=i}^{n} \left[\sum_{j\ge0} 2\binom{k+j+1}{i}\cdot\binom{k-j}{i} b_{k+j+1} b_{k-j}\right].$$

Similarly,

$$w_{n-i-1}\cdot w_{n-i+1} = \sum_{k=i}^{n}\left[\binom{k}{i+1}\cdot\binom{k}{i-1}\cdot b_k^2 + \sum_{j\ge 1}\left[\binom{k+j}{i+1}\cdot\binom{k-j}{i-1} + \binom{k+j}{i-1}\cdot\binom{k-j}{i+1}\right]b_{k+j}b_{k-j}\right]$$

$$+ \sum_{k=1}^{n}\left[\sum_{j\ge 0}\left[\binom{k+j+1}{i+1}\cdot\binom{k-j}{i-1} + \binom{k+j+1}{i-1}\cdot\binom{k-j}{i+1}\right]b_{k+j+1}b_{k-j}\right] .$$

Let k be fixed. By the log concavity of (b_i), $(b_{k+j}\cdot b_{k-j})$ and $(b_{k+j+1}\cdot b_{k-j})$ are both nonnegative decreasing sequences. Further, the sequence of binomial coefficients under each summation sign in the expansion of $(w_{n-i})^2$ dominates the respective sequence of binomial coefficients in the expansion of $w_{n-i-1}\cdot w_{n-i-1}$ by (6.12.3). Therefore, the conditions in (6.12.1) are met, and, for each k, $x_k \ge x'_k$ and $y_k \ge y'_k$ in $(w_{n-i})^2 = \sum_{k=i}^{n} x_k + \sum_{k=i}^{n} y_k$ and $w_{n-i-1}\cdot w_{n-i+1} = \sum_{k=i}^{n} x'_k + \sum_{k=i}^{n} y'_k$.

The proof for $(\hat{w}_i)$ is exactly the same.

<u>Proposition 6.14</u> Let G be a paving matroid. Then the coefficients in both $\bar{t}(G)$ and in $\bar{t}(G^*)$ are (strictly) unimodal.

<u>Proof.</u> We use the formulas in (5.15.3). Since, for all $i \ge 2$, $b_i = \binom{K-i-1}{n-i} > \binom{K-i-2}{n-i-1} = b_{i+1}$, the sequence $(b_i(G))$ is trivially unimodal. In fact, since $b_1 \le \binom{K-2}{n-1}$, the sequence is strongly log concave.

Now, let $b_j^* = b_{0j}(G) = b_j(G^*)$. Then, by (5.15.3), for $j > 0$,

$$b_j^* = \binom{K-j-1}{n-1} - \sum_{i\ge j+n-1}\binom{i-j}{n-1}a_i,$$

where G has a_i hyperplanes of cardinality i. We use (6.10.2).

Then, $\Delta_j = b^*_{j+1} - b^*_j = \sum_{i\geq j+n-2} \binom{i-j}{n-2} a_i - \binom{K-j-2}{n-2}$. If G has an isthmus, then $\chi(G^*) = 0$ and there is nothing to prove. So, assume G is free of isthmuses. Thus, if $a_i > 0$, then $i \leq K-2$.

Let j be such that $\Delta_j \geq 0$ (i.e., $b^*_{j+1} \geq b^*_j$). Then,

$$\sum_{i\geq j+n-2} \binom{i-j}{n-2} a_i \geq \binom{K-j-2}{n-2}$$

and, for all i,

$$\binom{i-j+1}{n-2} \Big/ \binom{i-j}{n-2} \geq \binom{K-j-1}{n-2} \Big/ \binom{K-j-2}{n-2} .$$

Thus, as we pass from Δ_j to Δ_{j-1}, each term on the left-hand side increases in ratio as least as fast as the single binomial coefficient on the right (and perhaps new terms become nonzero). So we have $\Delta_{j-1} \geq \Delta_j$; $b^*_j \geq b^*_{j-1}$; and, finally, that (b^*_j) is unimodal.

For future reference, we now review some of the important invariants which, for special classes of matroids (such as graphic and oriented matroids), have interesting interpretations. We then relate these invariants using the constructions presented in section four.

Remarks 6.15 1. The T-G group invariants below have the following formulas.

a. The number of independent sets of rank r:

$$I_r = \sum_{i,j} \binom{i}{n-r} b_{ij}$$

b. The (absolute) r^{th} Whitney number:

$$w_r = \sum_i \binom{i}{n-r} b_i$$

c. The reduced r^{th} Whitney number:

$$\hat{w}_r = \sum_i \binom{i-1}{n-1-r} b_i = \sum_{s>r} (-1)^{s-r-1} w_s = \sum_{s\leq r} (-1)^{r-s} w_s$$

d. The beta invariant:

$$\beta(G) = b_1$$

$$= \frac{\partial}{\partial x} t(M;0,0) = (-1)^{n+1} \frac{d}{d\lambda}\chi(M;1)$$

e. The (absolute) Möbius function:

$$\mu(M) = |\mu(0,1)| = \sum_i b_i$$

$$= t(M;1,0) = |\chi(M;0)| = w_0 = \hat{w}_0$$

f. The *acyclic* or *alpha invariant* and *reduced alpha invariant*:

$$\alpha(M) = \sum_i 2^i b_i$$

$$= t(M;2,0) = \sum_i w_i = (-1)^n \chi(M;-1)$$

$$\hat{\alpha}(M) = \sum_i 2^{i-1} b_i$$

$$= \frac{1}{2} t(M;2,0) = \sum_i \hat{w}_i \ .$$

g. The *complexity* b(M) (number of bases), independence number i(M) (number of independent sets), and *subset number* s(M):

$$b(M) = I_n = \sum_{i,j} b_{ij} = t(M;1,1),$$

$$i(M) = \sum_{i,j} 2^i b_{ij} = \sum_r I_r = t(M;2,1),$$

$$s(M) = \sum_{i,j} 2^{i+j} b_{ij} = t(M;2,2).$$

2. These invariants are related by the following inequalities

$$\begin{tikzcd}
 & \alpha(M) \arrow[r, phantom, "\geq"] & \hat{\alpha}(M) \arrow[dr, phantom, "\geq" sloped] & \\
s(M) \geq i(M) \arrow[ur, phantom, "\geq" sloped] \arrow[dr, phantom, "\geq" sloped] & & & \mu(M) \geq \beta(M) \geq 0 \\
 & b(M) \arrow[urr, phantom, "\geq" sloped] & &
\end{tikzcd}$$

Further,

$s(M) > i(M) > \alpha(M)$, and

$b(M) > \mu(M)$

unless M is a boolean algebra;

$i(M) > b(M)$ unless $r(M) = 0$,

$\alpha(M) > \hat{\alpha}(M)$ unless M has a loop,

$\hat{\alpha}(M) > \mu(M) > \beta(M)$ unless M has a loop or $r(M) = 1$, and

$\beta(M) > 0$ unless M is a loop or is separable.

3. These invariants are also related through the following constructions.

a. For truncation:

$$b(T^{n-r}(M)) = I_r(M).$$

$$i(T(M)) = i(M) - b(M).$$

$$\beta(T(M)) = \mu(M) - \beta(M).$$

$$\hat{\alpha}(M) = \sum_{i=0}^{n-1} \mu(T^i(M)).$$

$$\hat{\alpha}(T(M)) = \hat{\alpha}(M) - \mu(M)$$

$$\mu(T(M)) = \sum_i (i-1)b_i$$

b. For free extension:

$$I_r(M+p) = I_r(M) + I_{r-1}(M)$$

$$\beta(M+p) = \mu(M)$$

$$\mu(M+p) = \mu(T(M)) + \mu(M)$$

$$\hat{\alpha}(M+p) = \alpha(M) - \mu(M)$$

c. For free coextension:

$$\hat{w}_r(M\times p) = I_r(M)$$

$$\hat{\alpha}(M\times p) = i(M)$$

$$\mu(M\times p) = b(M)$$

d. For duality:

$$\beta(M^*) = \beta(M)$$

e. For direct sum with an isthmus:

$$\hat{w}_i(M\oplus p) = w_i(M)$$

$$\hat{\alpha}(M\oplus p) = \alpha(M)$$

$$\mu(M\oplus p) = \mu(M).$$

All the above can be easily proved using the formulas of (6.15.1) along with those of (3.18) and (4.2). Some of the above formulas have generalizations or "combinatorial proofs" (one-to-one correspondences between two families of subsets of S, each counted by a side of the identity).

For example, results of [35] show that I is an independent subset of $M(\{1,2,\ldots,K\})$ (and contributes to I_r) if and only if $I \cup \{0\}$ is a "χ-independent subset" of $M \times 0$. Thus, I also contributes to $\hat{w}_r$ and (6.15.3c) follows. A consequence of (6.15.3c) is that the log concavity of $(\hat{w}_r)$ (or of (b_i) by (6.13)) for all matroids (with a cofree point) implies the log concavity of (I_r) for all matroids. Other combinatorial correspondences appear in Part II.

As an example of a lattice-theoretic generalization of (6.15.3b), Zaslavsky [163] showed that, for any point $p \in S$,

$$\beta(G) = \Big| \sum_{\substack{x \in L(G): \\ x \not\geq p}} \mu(0,x) \Big| . \quad \text{When} \quad G = M + p,$$

the (signed) right-hand side is easily shown to be equal to

$$\sum_{\substack{x \in L(M): \\ x \neq 1}} \mu(0,x) = -\mu_M(0,1).$$

(A combinatorial proof of the above identity appears in [46].)

A useful technique for proving inequalities among T-G invariants is the use of *bijective rank-preserving weak maps* (see [97]). A matroid $M_1(S)$ is said to be *freer* than a matroid $M_2(S)$ if there is a rank-preserving weak map between M_1 and M_2 which is the identity on S. This is equivalent to saying that each basis of M_2 is a basis of M_1. If $M_1 \neq M_2$, we say that M_1 is *strictly freer* and that the map is *non-trivial*. We denote this case by writing $M_1 >_w M_2$.

Essential to the proof of all the inequalities below is that if $M_1 >_w M_2$, then, for any nonfactor p, $M_1-p \geq_w M_2-p$ and $M_1/p \geq_w M_2/p$ where, in at least one of the inequalities, the M_1 minor is strictly freer and no new loops are created. Further, $M_1^* >_w M_2^*$, and, for any matroid M of rank n and cardinality K, we have that $T^{K-n}(B_K) \geq_w M \geq_w B^{n,K-n}$.

Thus, for any T-G group invariant $f : \mathcal{M} \to \mathbb{R}$, if $f(M) > f(B^{n,K-n})$ for all loopless matroids M of rank n and cardinality K, then $f(M_1) > f(M_2)$ whenever M_1 is loopless and $M_1 >_w M_2$ (and a similar result holds for nonstrict inequality). This gives an easy, alternate proof to the result in [27] that μ, α, b, and i are all (strictly) maximized on $T^{K-n}(B_K)$ among matroids of the same rank and cardinality. We list some relevant results below.

<u>Proposition 6.16</u> Let M_1 be strictly freer than M_2. Then,

1. $i(M_1) > i(M_2)$ and $b(M_1) > b(M_2)$.

2. $\alpha(M_1) \geq \alpha(M_2)$ and $\mu(M_1) \geq \mu(M_2)$ with strict inequality if M_1 has no loops.

3. $w_r(M_1) \geq w_r(M_2)$, $\hat{w}_r(M_1) \geq \hat{w}_r(M_2)$, $I_r(M_1) \geq I_r(M_2)$, $b_{i0}(M_1) \geq b_{i0}(M_2)$, and $b_{0j}(M_1) \geq b_{0j}(M_2)$.

4. $\beta(M_1) \geq \beta(M_2)$ with strict inequality if M_1 is connected.

<u>Proof.</u> Formulas (6.16.1) - (6.16.3) are easily proved by the above remarks (see [97]). We prove (6.16.4). This inequality holds

trivially if $K \leq 2$, and we also note that if M is connected, then $\beta(M) > 0 = \beta(B^{n,K-n})$. Now, let M_1 be a connected matroid with $p \in M_1$.

Case 1. If M_1-p and M_2/p are both connected, we are done by induction.

Case 2. If M_2 is separable, then $\beta(M_1) > \beta(M_2) = 0$.

Case 3. If M_1/p is separable, then M_1 is a parallel connection of connected matroids M_1' and M_1''. Further, M_2/p is also separable. Hence, $M_2 = P(M_2',M_2'')$ with $M_1' \geq_w M_2'$, $M_1'' \geq_w M_2''$, and at least one of the inequalities strict. By (4.8.10) and the induction hypothesis, $\beta(M_1) = \beta(M_1')\beta(M_1'') > \beta(M_2')\beta(M_2'') = \beta(M_2)$.

Case 4. If M_1-p is separable, then M_1^*/p is separable, $M_1^* >_w M_2^*$, $\beta(M_1^*) = \beta(M_1)$, and $\beta(M_2^*) = \beta(M_2)$. Thus, duality reduces this case to the previous one.

We end Part I with a discussion of extremal classes. This concept relates the idea of a T-G recognizable hereditary class and the theory of (parametric) T-G inequalities.

Definition 6.17 1. Recall that a hereditary class of matroids $\mathcal{H}$ is one closed under minors (equivalently, under single-point deletion and contraction). Any hereditary class can be defined by its class of excluded minors $\mathcal{E}$ where $E \in \mathcal{E}$ if $E \notin \mathcal{H}$ but every proper minor of E is in $\mathcal{H}$. Conversely, it is clear that any class $\mathcal{C}$ of matroids which contains no proper minors of any of its members is the class of excluded minors for the hereditary class $\mathcal{H} = \{M : \text{no minor of } M \text{ is in } \mathcal{C}\}$.

Since, when calculating T-G group invariants, we forbid deletion and contraction by loops or isthmuses, we are motivated to define a *T-G hereditary class* $\mathcal{H}'$ as one which is closed under deletion and contraction only by nonfactors. The class $\mathcal{H}'$ is also defined by its class $\mathcal{E}'$ of *T-G excluded minors* where $M \in \mathcal{E}'$ if $M \notin \mathcal{H}'$ but $M-p$ and M/p are in $\mathcal{H}'$ for all nonfactors $p \in M$. Obviously, every hereditary class is a T-G hereditary class whereas, for example, $\{B^2\}$ forms a T-G hereditary class which is not an (ordinary) hereditary class. The next proposition shows how to get the T-G excluded minors for a hereditary class from its class of (ordinary) excluded minors. A geometric T-G hereditary class is defined analogously, where we do not allow deletion or contraction by isthmuses.

2. A hereditary class $\mathcal{C}$ of matroids is said to be *(T-G) recognizable* if $t(M_1) \neq t(M_2)$ whenever $M_1 \in \mathcal{C}$, and $M_2 \notin \mathcal{C}$. Examples of recognizable classes are boolean algebras, truncated boolean algebras, and paving matroids (as we saw in (5.15)).

Since, in (3.11), M' is transversal while M is not the minor of a transversal matroid, and since M is planar graphic (and hence graphic, unimodular, and binary), while M' is not, none of the above classes is recognizable. Further, the matroids in (4.3.2) show that the class of representable matroids is not recognizable.

3. Let $p(M) = (p_0(M), p_1(M), \ldots) \in \mathcal{P}$ be a sequence of integer-valued invariants. We then say that $p(M)$ is a *parametrization* of M, and the class of all matroids $\mathcal{M}$ is partitioned into parametric families.

A class $\mathcal{C}$ of matroids is a *parametric* (T-G) *extremal class* with respect to the parametrization p and a given T-G group invariant $f : \mathcal{M} \to \mathbb{Z}$ if there is a function $g : \mathcal{P} \to \mathbb{Z}$ such that

(6.17.4) $\quad f(M) = g(p(M))$ for all $M \in \mathcal{C}$, and

(6.17.5) $\quad f(M) > g(p(M))$ for all $M \notin \mathcal{C}$.

This situation clearly makes $\mathcal{C}$ a T-G recognizable class, and it gives a sharp lower bound on values of f as well.

Proposition 6.18 Let $\mathcal{H}$ be a hereditary class of matroids, and let $\mathcal{E}$ be its class of excluded minors. Further, assume for all $E \in \mathcal{E}$ and nonfactors $p \in E$, $(E-p) \oplus B^{ij} \in \mathcal{H}$ and $(E/p) \oplus B^{ij} \in \mathcal{H}$. Then $\mathcal{H}$ is also a T-G hereditary class with T-G excluded minors: $\mathcal{E}' = \mathcal{E} \cup \{E \oplus B^{ij} : E \in \mathcal{E}, i + j > 0\}$. In particular, every totally separable matroid B^{ij} is in $\mathcal{H}$ or $\mathcal{E}$.

Similarly, excluded minors for geometric T-G hereditary classes are direct sums of ordinary excluded minors and boolean algebras.

Proof. It is clear that no member of $\mathcal{E}'$ is in $\mathcal{H}$. On the other hand, any T-G contraction or deletion of a member $E \oplus B^{ij}$ of $\mathcal{E}'$ must be of the form $(E-p) \oplus B^{ij}$ or $(E/p) \oplus B^{ij}$ where p is a nonfactor, and these matroids are in $\mathcal{H}$ by definition. Thus, all members of $\mathcal{E}'$ are excluded minors.

Conversely, if $M \notin \mathcal{H}$, then M must have a member of E as an excluded minor. Decomposing M into its connected direct-sum factors, we may assume that $M = M_1 \oplus M_2 \oplus \ldots \oplus M_k$ and $E = E_1 \oplus \ldots \oplus E_{k'}$, where $k \geq k'$, and E_i is a minor of M_i for all $i \leq k'$. For $i \leq k'$, we may apply (4.12) to find a sequence of matroids $M_i^0 = M_i, M_i^1, \ldots, M_i^{m_i} = E_i$ where, for all $j < m_i$, M_i^{j+1} equals $M_i^j - p_j$ or M_i^j/p_j with p_j a nonfactor of M_i^j. Similarly, for $i > k'$, either M_i is a loop or we may find a sequence as above with $M_i^{m_i}$ an isthmus. In any case, M has a member of $\mathcal{E}'$ as a T-G minor.

We now give some examples of hereditary classes which we will later show to be extremal.

Proposition 6.19 1. The class of geometries which are direct sums of a line and a boolean algebra, $\mathcal{BL} = \{B^i\} \cup \{L_m \oplus B^i : m \geq 3, i \geq 0\}$ forms a geometric hereditary class whose (geometric) excluded minors are a four-point circuit, C_4, and the direct sum of two three-point circuits, $C_3 \oplus C_3$.

2. The class $\mathcal{T}$ of truncated boolean algebras forms a hereditary class with the unique excluded minor $B^{1,1}$. Its class of T-G excluded minors is then given by $\mathcal{E}' = \{B^{ij} : i > 0, j > 0\}$.

3. The class $\mathcal{SP}$ of series-parallel networks forms a hereditary class with excluded minors

$$\mathcal{E}' = \{L_4, M(K_4)\},$$

where L_4 is a four-point line, and $M(K_4)$ is the geometry of the complete four-graph (the geometry $\overline{M^*}$ of Example (4.5)).

4. The class $\mathcal{S}$ of separable matroids forms a T-G hereditary class with excluded minors $\{B^{1,0}, B^{0,1}\}$.

If $\mathcal{H}$ is any hereditary class whose excluded minors, $\mathcal{E}$, are all connected, then $\mathcal{H} \cup \mathcal{S}$ is a T-G hereditary class with T-G excluded minors $\mathcal{E}$.

5. The class $\mathcal{L}$ of matroids with loops is a T-G hereditary class with T-G excluded minors

$$\mathcal{E}' = \{B^i : i > 0\}.$$

If $\mathcal{H}$ is any hereditary class whose excluded minors $\mathcal{E}$ are all loopless, then $\mathcal{H} \cup \mathcal{L}$ is a T-G hereditary class with T-G excluded minors

$$\mathcal{E}' = \{E \oplus B^i : E \in \mathcal{E},\ i \geq 0\}.$$

Proof. 1. The reader readily checks that any proper geometric minor of C_4 and $C_3 \oplus C_3$ is in $\mathcal{BL}$. Conversely, if $G \notin \mathcal{BL}$, then G must contain (as a subgeometry) a circuit C_i with $i \geq 4$, or it must contain at least two three-point circuits C_3' and C_3''. In the former case, contracting points of C_i gives C_4, while, in the latter case, let r be the maximal rank of $S' = C_3' \cup C_3''$ over all distinct three-point circuits C_3' and C_3'' of G. If $r = 4$, $S' = C_3' \oplus C_3''$; if $r = 3$, S' contains a four-point circuit; and if $r = 2$, $G \in \mathcal{BL}$.

2. The direct sum of a loop and an isthmus, $B^{1,1}$, is not a truncated boolean algebra, while its two minors $B^{0,1}$ and $B^{1,0}$ both are. If $M \notin \mathcal{T}$, then M has a circuit C and point $p \in M-\bar{C}$. Deleting everything except C and p, and contracting all but one point of C, we obtain $B^{1,1}$ as a minor of M.

3. This is proved in [24].

4. Since we are not allowed to delete or contract isthmuses or loops, if M' is a minor of M, then the number of components of M' is at least as great as M. Thus, $\mathcal{S}$ is a T-G hereditary class. Further, (4.12) or (6.5) shows that any connected matroid is either a loop or has an isthmus as a T-G minor. (Note that an elementary extension of this argument shows that the class $\mathcal{S}^k$ of matroids with at least k connected components is a T-G hereditary class with T-G excluded minors $\{B^{ij} : i + j < k\}$.)

It is clear that the union of two T-G hereditary classes is itself such a class. That $\mathcal{E}$ is the class of excluded minors for $\mathcal{H} \cup \mathcal{S}$ follows directly from (4.12).

5. Deletion or contraction by nonfactors never destroys loops. The reader may supply the rest of the proof by modifying the proof of (6.18).

Two techniques for obtaining parametric extremal classes are contained in the following propositions. The first is for when the T-G invariant is given, and the second allows the class (and function g) to define the invariant.

Proposition 6.20 A T-G hereditary class $\mathcal{C}$ is a parametric extremal class for the parametrizaiton $p : \mathcal{M} \to \mathcal{P}$ and T-G group invariant f if there is a function $g : \mathcal{P} \to \mathbb{Z}$ which satisfies the three properties below:

1. Whenever $M \in \mathcal{C}$, then $f(M) = g(p(M))$.

As an equivalent condition, we have,

1'. If $M \in \mathcal{C}$ is totally separable, then $f(M) = g(p(M))$. If $M \in \mathcal{C}$ is not totally separable, then there exists a nonfactor $q \in M$ such that

$$g(p(M)) = g(p(M-q)) + g(p(M/q)).$$

2. For all $M \in \mathcal{M}$ and nonfactors $q \in M$,

$$g(p(M)) \leq g(p(M-q)) + g(p(M/q)).$$

3. Whenever E is a T-G excluded minor for the class $\mathcal{C}$, then there is some member M of $\mathcal{C}$ with the same parameters as E such that $f(E) > f(M)$.

Proof. Conditions 1 and 1' are equivalent by induction on the number of nonfactors since, by hypothesis, f and $g \circ p$ both obey the recursion T1 on the class $\mathcal{C}$.

Now, assume we have an invariant f which obeys conditions 1, 2, and 3. Condition (6.17.4) is the same as our hypothesis (6.20.1). To verify (6.17.5) for all matroids M' not in $\mathcal{C}$, we use induction on the size of M'. Since $M' \notin \mathcal{C}$, it has a T-G excluded minor E. If $M' = E$, then (6.20.3) guarantees that there is a matroid $M \in \mathcal{C}$ with $p(M) = p(M')$, and with $f(M') > f(M) = g(p(M)) = g(p(M'))$.

If M' is not a T-G excluded minor, then there is a nonfactor $q \in M'$ such that either $M'-q$ or M'/q is not in $\mathcal{C}$. Assume the former (the latter case follows simiiarly). Then,

$f(M') = f(M'-q) + f(M'/q)$. Either M'/q is in $\mathcal{C}$ or not. If it is, then $f(M'/q) = g(p(M'/q))$, and if it is not, then, by induction, $f(M'/q) > g(p(M'/q))$. In any case, $f(M'-q) > g(p(M'-q))$, and

$$\begin{aligned} f(M) &> g(p(M-q)) + g(p(M/q)) \\ &\geq g(p(M)). \end{aligned}$$

Proposition 6.21 Let $\mathcal{C}$ be a T-G hereditary class with $\mathcal{E}$ its class of T-G excluded minors. Further, assume that there is a parametrization $p : \mathcal{M} \to \mathcal{P}$ and a function $g : \mathcal{P} \to \mathbb{Z}$ such that

1. $g(p(M)) \leq g(p(M-q)) + g(p(M/q))$ for all $M \in \mathcal{M}$ and nonfactors $q \in M$.

Then, there exists a T-G group invariant f for which $\mathcal{C}$ is extremal if and only if the following two properties hold.

2. Whenever $M \in \mathcal{C}$ is not totally separable, there exists a nonfactor $q \in M$ such that

$$g(p(M)) = g(p(M-q)) + g(p(M/q)),$$

and

3. Whenever $E \in \mathcal{E}$ is not totally separable, there is a nonfactor $q \in E$ such that

$$g(p(E)) < g(p(E-q)) + g(p(E/q)).$$

Under the above conditions, $f(M) = \sum_{i,j} b_{ij}c_{ij}$ is a T-G group invariant for which $\mathcal{C}$ is extremal if and only if

4. $c_{ij} = g(p(B^{ij}))$, $B^{ij} \in \mathcal{C}$

$c_{ij} > g(p(B^{ij}))$, $B^{ij} \in \mathcal{E}$.

Proof. The function $f : \mathcal{M} \to \mathbb{Z}$ is a T-G group invariant by (3.9), and $f(M) = g(p(M))$ for all $M \in \mathcal{C}$ by (6.21.2) and (6.21.4).

Let E be an excluded minor for $\mathcal{C}$. Under the hypothesis of (6.21.3), there is a nonfactor q such that

$$g(p(E)) < g(p(E-q)) + g(p(E/q)).$$

But $E-q$ and E/q are both in $\mathcal{C}$, so that $g(p(E-q)) = f(E-q)$ and $g(p(E/q) = f(E/q)$. Hence,

$$\begin{aligned} f(E) &= f(E-q) + f(E/q) \\ &= g(p(E-q)) + g(p(E/q)) \\ &> g(p(E)). \end{aligned}$$

Otherwise, $E = B^{ij} \notin \mathcal{C}$ so that by our definition of f, $f(E) = c_{ij} > g(p(E))$.

For a general $M' \notin \mathcal{C}$, M' has a T-G excluded minor E and the proof proceeds as in (6.20). The necessity of (6.21.2) and (6.21.3) for the existence of f and of (6.21.4) for c_{ij} is obvious.

We note that the above propositions can be easily modified to the geometric case, and to the case when the Tutte-Grothendieck invariant is maximized on the extremal class. In this latter case, all inequalities are reversed, and we will refer to the conditions by $(6.20.\hat{2})$, etc.

We now state some of the classical T-G inequalities in terms of parametric extremal classes.

Proposition 6.22 1. Let us parametrize geometries by rank and cardinality:

$$p(G) = (r(G), |G|).$$

Then, $\mu(G) \geq |G| - r(G) + 1$, and $\alpha(G) \geq 2^{r(G)-1}(|G| - r(G) + 2)$, with equality (for either invariant) on the extremal class $\mathcal{BL}$ of direct sums of a line and a boolean algebra (see (6.19.1)).

2. When matroids are parametrized by rank and cardinality, we have

$$\beta(M) \leq \binom{|M|-2}{r(M)-1}$$

$$\mu(M) \leq \binom{|M|-1}{r(M)-1}$$

$$\hat{\alpha}(M) \leq \sum_{i=0}^{r(M)-1} \binom{|M|-1}{i}$$

with equality on the extremal class $\mathcal{T}$ of truncated boolean algebras (see (6.19.2)).

3. When geometries are parametrized by connectedness:

$$p(G) = \begin{cases} 1 & \text{if } G \text{ is connected} \\ 0 & \text{if } G \text{ is separable,} \end{cases}$$

then $\beta(G) \geq p(G)$ with equality on the extremal class $\mathcal{SP} \cup \mathcal{S}$ of geometries which are either separable or are series-parallel networks (see (6.19.3), (6.19.4)).

<u>Proof.</u> The proofs for all these are routine calculations using (6.19) and (6.20). We mention below only a few hints and the original reference for the theorem.

1. This first appeared in [68]. For any geometry G, $\overline{G/q}$ is a geometry of rank $r(G)-1$ and cardinality at least $r(G)-1$. Thus, for example, when q is not an isthmus of G, (6.20.2) follows from the following set of inequalities:

$$\begin{aligned} g_\alpha((n,K)) &= 2^{n-1}(K-n+2) \\ &= 2^{n-1}(K-n+1) + 2^{n-1} \\ &= g_\alpha(n,K-1) + g_\alpha(n-1,n-1) \\ &\le g_\alpha(r(G-q),|G-q|) + g_\alpha(r(\overline{G/q}),|\overline{G/q}|). \end{aligned}$$

Further, in verifying (6.20.3) for α·, we get the following calculations:

$$\alpha(C_4 \oplus B^i) = 14\cdot 2^i > 6\cdot 2^{i+1} = \alpha(L_3 \oplus B^{i+1}),$$

and $$\alpha(C_3 \oplus C_3 \oplus B^i) = 36\cdot 2^i > 8\cdot 2^{i+2} = \alpha(L_4 \oplus B^{i+2}).$$

2. This result,which first appeared in [27],uses standard identities on binomial coefficients to verify (6.20.$\hat{2}$). The exact formula for $\hat{\alpha}$ on $\mathcal{T}$ is given by (6.15.3a). To verify (6.20.$\hat{3}$), note that all of the above invariants are zero on the class of T-G excluded minors, $\mathcal{E}' = \{B^{ij} : i > 0, j > 0\}$, whereas the truncated boolean algebra $T^j(B^{i+j})$ has the same parameters as B^{ij}, and gives a positive value for each invariant.

3. That $\beta(G) = 0$ if and only if G is separable first appeared in [53]. For connected geometries, the fact that $\beta(G) = 1$ if and only if G is a series-parallel network is in [24]. It is obvious that $\beta(G) = p(G) = 0$ for separable matroids,while the fact that $\beta(G) = 1$ for connected series-parallel networks follows from (4.8.10) (along with induction and duality). If G-q is separable for a connected geometry G, G is a series connection and G/q is connected, so

$$p(G) \le p(G-q) + p(G/q),$$

while $$\beta(M(K_4)) = \beta(L_4) = 2 > 1 = \beta(G)$$

for any series-parallel network G with p(G) = 1. $M(K_4)$ and L_4 are the T-G excluded minors for $\mathcal{SP} \cup \mathcal{S}$ by (6.19.3) and (6.19.4).

We now generalize (6.22.2) from truncated boolean algebras to the class $\mathcal{N}$ of all nested matroids where the parametrization is, for all r, by the size of the largest flat of rank r.

Proposition 6.23 For the parametrization

$$p(M) = (n;a_0,a_1,a_2,\dots,a_n)$$

where $n = r(M)$ and, for all r,

$$\sum_{i=0}^{r} a_i = \max(|F| \ : F \text{ is a flat of rank } r),$$

then, $\mu(M) = 0$ if $a_0 > 0$, and, in general,

$$\mu(M) \le g(n;a_0,\dots,a_n) =$$

$$\binom{\bar{a}_n}{n-1} - \binom{\bar{a}_{n-1}}{n-1} - \left(\sum_{r=1}^{n-3} \binom{\bar{a}_{n-r-1}}{n-r-1} \sum_{\substack{i_1 \ge 1 \\ i_1+i_2 \ge 2 \\ \vdots \\ i_1+\dots+i_r=r}} \binom{a_n}{i_1}\binom{a_{n-1}}{i_2}\cdots\binom{a_{n-r+1}}{i_r} \right)$$

where $\bar{a}_i = a_2+a_3+\dots+a_r$. Further, equality holds precisely on the class $\mathcal{N} \cup \mathcal{L}$ of nested matroids and matroids with loops.

Proof. We verify the three conditions of (6.20^).

1. $\mu(M) = 0$ if and only if M has a loop $(a_0 > 0)$, so we may assume that $a_0 = 0$. Further, a_1 does not contribute to the formula

for g and, on the other hand, $\mu(M) = \mu(\bar{M})$, where, for nested matroids, $p(\bar{M}) = (n;0,1,a_2,\ldots,a_n)$. Therefore, we may assume that M is a geometry. We use induction on the size of M. Clearly, if $|M| = 1$, $\mu(M) = 1 = g(1;0,1)$.

For a nested geometry of rank two, $M = L_m$ for some m, while $p(L_m) = (2;0,1,m-1)$. Thus, $\mu(L_m) = m-1 = \binom{a_2}{1} = g(p(M))$.

Assume $\mu(M) = g(p(M))$ for all matroids of size K, and let G have size $K+1$.

If G contains an isthmus p, we note that, whether G is nested or not, $\mu(G-p) = \mu(G)$. Further, if $r(G) = n+1$, then $a_{n+1} = 1$ since $G-p$ is a hyperplane. We must verify that $g_{n+1} = g(n+1;0,1,\ldots,a_n,1) = g(n;0,1,\ldots,a_n) = g_n$:

$$g_{n+1} = \binom{\bar{a}_n+1}{n} - \binom{\bar{a}_n}{n-1} - \sum_{r=1}^{n-2} \binom{\bar{a}_{n-r}}{n-r} \sum_{\substack{i_1 \geq 1 \\ \vdots \\ i_1+\ldots+i_r=r}} \binom{1}{i_1}\binom{a_n}{i_2}\cdots\binom{a_{n-r+2}}{i_r}$$

$$= \binom{\bar{a}_n}{n-1} - \binom{\bar{a}_{n-1}}{n-1}\binom{1}{1} - \sum_{r'=1}^{n-3} \binom{\bar{a}_{n-r'-1}}{n-r'-1} \sum_{\substack{i'_1 \geq 1 \\ \vdots \\ i'_1+\ldots+i'_{r'}=r'}} \binom{1}{1}\binom{a_n}{i'_1}\cdots\binom{a_{n-r'+1}}{i'_{r'}}$$

$$= g_n .$$

If G does not contain an isthmus, then $a_n > 1$ where $n = r(G)$. Let q be a point in free position.

By (6.6.4c) and (6.6.4d),

$$p(G-q) = (n;0,1,\dots,a_{n-1},a_n-1) = p', \quad \text{and}$$

$$p(G/q) = (n-1;0,1,\dots,a_{n-2},a_{n-1}+a_n-1) = p'' .$$

Then, g(p) - g(p') =

$$\binom{\bar{a}_n}{n-1} - \binom{\bar{a}_n-1}{n-1} - \sum_{r=1}^{n-3}\binom{\bar{a}_{n-r-1}}{n-r-1} \sum_{\substack{i_1\geq 1\\ \vdots \\ i_1+\dots+i_r=r}} \left(\binom{a_n}{i_1} - \binom{a_n-1}{i_1}\right)\binom{a_{n-1}}{i_2}\cdots\binom{a_{n-r+1}}{i_r}$$

$$= \binom{\bar{a}_n-1}{n-2} - \sum_{r=1}^{n-3}\binom{\bar{a}_{n-r-1}}{n-r-1}\sum\binom{a_n-1}{i_1-1}\binom{a_{n-1}}{i_2}\cdots\binom{a_{n-r+1}}{i_r}$$

$$= \binom{\bar{a}_n-1}{n-2} - \binom{\bar{a}_{n-2}}{n-2} - \sum_{r=2}^{n-3}\binom{\bar{a}_{n-r-1}}{n-r-1} \sum_{\substack{i_1-1+i_2=i_1'\geq 1\\ i_1'+i_2'\geq 2\\ i_1'+\dots+i_{r-1}'=r-1}} \left(\sum_{i=0}^{i_1'}\binom{a_n-1}{i}\binom{a_{n-1}}{i_1'-i}\right)\binom{a_{n-2}}{i_2'}\cdots\binom{a_{n-r+1}}{i_{r-1}'}$$

$$= g(p'').$$

Note that a similar calculation shows that for all $i \geq 1$,

$$\begin{aligned} g(n;0,1,\dots,a_i,a_{i+1},\dots) &= g(n;0,1,\dots,a_i,a_{i+1}-1,\dots) \\ &\quad + g(n-1;0,1,\dots,a_{i-1},a_i+a_{i+1}-1,a_{i+2},\dots), \end{aligned} \tag{6.23.1}$$

which also follows from the fact that if $g \circ p$ obeys the T-G recursion T1 for some nonfactor, it obeys T1 for every nonfactor, and we may apply the formulas in (6.6.4) for $q \in F_{i+1} = \bar{B}_{i+1} - \bar{B}_i$.

The excluded minor M_i (see (6.6.5)) has parameters $(i;0,1,\dots,1,2,i)$ and is a nontrivial weak-map image of the nested matroid N_i with the same parameters (where the weak map is the identity on the cyclic flat F_{i-1} of N and sends all the points in free position to the complementary flat F'_{i-1} of M_i). Since the T-G excluded minor class of $\mathcal{N} \cup \mathcal{L}$ is $\{M_i = i \geq 2\}$ by (6.6.5) and (6.19.5), we have verified (6.20.$\hat{3}$).

It remains to check (6.20.$\hat{2}$). To prove this, let q be a nonfactor of M. Denote p(M-q) by $(n;a'_0,a'_1,\ldots,a'_n)$, and p(M/q) by $(n-1;a''_0,\ldots,a''_{n-1})$. It is a routine matter to check (6.20.$\hat{2}$) in the case when q is in a multiple point (so that p(M/q) = 0 and $p(M-q) \leq p(M)$). Let f_i, f'_i, and f''_i, respectively, denote the size of the largest closed set of rank i in M, M-q, and M/q, respectively. Then $f'_i = f_i$ or $f_i - 1$, and equals $f_i - 1$ if and only if $q \in \overline{F_i - q}$ for every flat $F_i \in M$ with rank i and size f_i. Similarly, for $i < n$, $f''_i \geq f_i$ since if $q \notin F_i$, then $\overline{F_i \cup q} - q$ is a flat in M/q of rank i and size at least f_i, while if $q \in F_i$, then for any $p \notin F_i$, $\overline{F_i \cup p} - q$ is a flat in M/q of rank i and size $\geq f_i$. An upper bound for f''_i is $f_{i+1} - 1$, and this is achieved whenever $q \in \overline{F_{i+1} - q}$ for some flat $F_{i+1} \in M$ with rank i+1 and size f_{i+1}. Hence, if $f'_i = f_i - 1$, then, in addition, $f''_{i-1} = f_i - 1$. Further, $f'_n = f''_{n-1} = f_n - 1$.

Let $h(n;f_0,f_1,\ldots,f_n)$ equal $g(n;f_0,f_1-f_0,\ldots,f_n-f_{n-1})$, and assume that for $j = 1,3,5,\ldots,2m+1$, $f'_{i_j} = f_{i_j} - 1$, and $f'_{i_j - 1} = f_{i_j - 1}$; while for $j = 2,4,\ldots,2m$, $f'_{i_j} = f_{i_j}$, and $f'_{i_j - 1} = f_{i_j - 1} - 1$. (Thus,

$a'_{i_j} = a_{i_j} - 1 > 0$ for odd j, $a'_{i_j} = a_{i_j} + 1$ for even j, and $a'_i = a_i$ otherwise. Further, $i_1 \geq 2$.)

Multiple applications of (6.23.1) then yield:

(6.23.2)
$$h(n;f_0,f_1,\ldots,f_n) = h(n;f'_0,f'_1,\ldots,f'_n) + h_{2m+1} - h_{2m} + \ldots + (-1)^j h_j + \ldots - h_2 + h_1$$

where, for all j,

(6.23.3) $$h_j = h(n-1;f'_0,f'_1,\ldots,f'_{i_j-2},f_{i_j}-1,f_{i_j+1}-1,\ldots,f_n-1).$$

Let

(6.23.4) $$h_{2m+2} = h(n-1;\hat{f}_0,\hat{f}_1,\ldots,\hat{f}_{n-1})$$

where $\hat{f}_{i-1} = f_i - 1$ for all $i : i_{2k-1} \leq i \leq i_{2k}-1$,

or $i \geq i_{2m+1}$, and

$\hat{f}_{i-1} = f_{i-1}$ otherwise.

It is easy to show that $h_{2m+2} \geq h(n-1;f''_0,f''_1,\ldots,f''_{n-1})$, since $\hat{f}''_{n-1} = \hat{f}_{n-1}$, and $f''_i \geq \hat{f}_i$ for all i.

Therefore, using (6.23.2) and (6.23.4), we get

$$h(n;f_0,f_1,\ldots,f_n) - h(n;f'_0,f'_1,\ldots,f'_n) - h(n-1;f''_0,f''_1,\ldots,f''_{n-1})$$
$$\geq h_1 - h_2 + h_3 - h_4 + \ldots + h_{2m+1} - h_{2m+2},$$

and (6.20.$\hat{2}$) will follow from the nonnegativity of this alternating sum.

This last inequality is left to the reader who may verify it by a term-by-term comparison.

Corollary 6.24. 1. Let M be a loopless matroid of size K and rank n. Further, for all $r > 0$, assume that M has a flat of size at least f_r. Then,

$$\mu(M) \leq g(n;0,f_1,f_2-f_1,\ldots,f_i-f_{i-1},\ldots,K-f_{n-1})$$

with equality if and only if M is the nested matroid $N(0,f_1,\ldots,f_i-f_{i-1},\ldots,K-f_{n-1})$.

2. For matroids parameterized as in (6.23),

$$\beta(M) = 0 \text{ if } a_0 > 0 \text{ or } a_n = 1 \ (n > 1),$$

and otherwise

$$\beta(M) \leq g(n;0,a_1,a_2,\ldots,a_i,\ldots,a_n-1).$$

The extremal class is $N \cup L \cup L^*$ where L^* is the class of all matroids with an isthmus.

3. For matroids parameterized as in (6.23),

$$\hat{\alpha}(M) \leq g_n + \ldots + g_1$$

with equality on the extremal class $N \cup L$ where, for all i, $g_i = g(i;0,a_1,\ldots,a_{i-1},a_i+a_{i+1} + \ldots + a_n)$.

Proof. 1. When n and $K = a_1 + \ldots + a_n = b_1 + \ldots + b_n$ are fixed, then $g(n;0,a_1,\ldots,a_n) > g(n;0,b_1,\ldots,b_n)$ where, for all i, $a_0 + \ldots + a_i \leq b_0 + \ldots + b_i$ with strict inequality for at least one i. (This is a consequence of the fact that for the two respective nested matroids, $N_{\underline{a}}$ and $N_{\underline{b}}$, there is a nontrivial rank-preserving weak map from $N_{\underline{a}}$ to $N_{\underline{b}}$.)

2. A matroid M has an isthmus if and only if, in p(M), $a_n = 1$. For any such matroid (of rank $n > 1$), it is separable and $\beta(M) = 0$. Otherwise, $a_n > 1$, and we use (6.15.3.b) and (6.16) to obtain: $\beta(M) \leq \mu(M-p)$ for any p in M with strict inequality unless p is a point in free position. The rest of the proof follows in a straightforward way, noting that if p is in free position, M is nested with parameters $(a_0,\ldots,a_n)$ if and only if M-p is nested with parameters $(a_0,\ldots,a_n-1)$.

3. This is an easy application of (6.15.3.a).

Exercises 6.25 1. Imitate Corollary (6.24) to get maximal values and extremal classes of matroids for the independence number I_r and the Whitney number w_r.

2. Develop a simpler formula for the upper bound of $\mu(M)$ when, for $i \geq 1$, all $a_i = 1$, except $i = n$ and $i = r$. (By (6.24.1), a bound will then be obtained for all matroids of rank n, cardinality K, and with a flat F_r of rank r and size at least k.)

Research Problems 6.26 1. Find combinatorial proofs (i.e., bijections or injections among two appropriate families of subsets) for the equalities and inequalities of (6.15).

2. Develop an extremal theory for minimizing T-G invariants on connected matroids. In particular, try to extend, in the connected case, the idea of an extremal class to include the matroids on which the bounds of [34] are sharp.

3. The most extensive results thus far obtained for parameterized lower bounds for T-G invariants are found in [15]. In particular, Björner obtains the minimum for $\mu(M)$ when M is parameterized by rank, cardinality, and size of smallest circuit. This result can be thought of as dual to the upper bound to be calculated in (6.25.2). Can (6.23) be dualized in a similar manner to obtain lower bounds for a finer parametrization (e.g., by the minimum size, c_j, of a cycle of nullity j)?

4. In [112], Oxley characterizes the classes of matroids on which β equals two, three, and four respectively. Several parametrizations are implicit in his paper.

For example, parametrize a loopless, connected matroid M by the invariant $p(M)$, the maximum positive integer λ for which $\chi(M;\lambda) \le 0$. Then, for $p(M) \le 5$, $\beta(M) \ge p(M)-1$, and Oxley's results give the extremal matroids for these values as well as a class of matroids $(\{L_{m+2}\})$ for which $\beta(M) = p(M)-1 = m$. Is this inequality true in general? If so, what are the extremal matroids? Similar questions may be asked for a parametrization in terms of connectivity:

What is the sharp lower bound for $\beta(M)$ among all matroids of connectivity n (with at least $2n-2$ points)? Oxley conjectures that $g(n) = \binom{2n-4}{n-2}$ and shows that $g(n) \geq 2^{n-2}$.

Bibliography

1. Arrowsmith, D. K. and Jaeger, F., "On the enumeration of chains in regular chain-groups " (preprint, 1980).

2. Baclawski, K., "Whitney numbers of geometric lattices," Advances in Math. 16 (1975), 125-138.

3. ___________, "The Möbius algebra as a Grothendieck ring," J. of Algebra 57 (1979), 167-179.

4. Barlotti, A., "Some topics in finite geometrical structures," Institute of Statistics Mimeo Series No. 439, Department of Statistics, University of North Carolina, Chapel Hill, N. C., 1965.

5. ___________, "Bounds for k-caps in PG(r,q) useful in the theory of error correcting codes," Institute of Statistics Mimeo Series No. 484.2, Department of Statistics, University of North Carolina, Chapel Hill, N. C., 1966.

6. ___________, "Results and problems in Galois geometry," Colloquium on Combinatorics and its Applications, June, 1978, Colorado State University.

7. Bessinger, J. S., "On external activity and inversion in trees " (preprint).

8. Biggs, N., Algebraic Graph Theory, Cambridge University Press, 1974.

9. ___________, "Resonance and reconstruction," Proc. Seventh British Combinatorial Conference, Cambridge U. Press, 1979, 1-21.

10. Birkhoff, G. D.,"A Determinant formula for the number of ways of coloring a map," Ann. of Math. (2) 14 (1913), 42-46.

11. Birkhoff, G. D. and Lewis, D. C., "Chromatic polynomials," Trans. Amer. Math. Soc. 60 (1946), 355-451.

12. Bixby, R. E., "A omposition for matroids," J. Comb. Th. (B) 18 (1975), 59-73.

13. Björner, A., "On the homology of geometric lattices," (preprint: 1977 No. 9, Matematiska Institutionen Stockholms Universitet, Stockholm, Sweden).

14. ___________, "Homology of matroids " (preprint, to appear Combinatorial Geometries, H. Crapo, G.-C. Rota, N. White eds.).

15. Björner, A., "Some matroid inequalities," Disc. Math. 31 (1980), 101-103.

16. Bland, R. G. and Las Vergnas, M., "Orientability of matroids," J. Comb. Th. (B) 24 (1978), 94-123.

17. Bondy, J. A. and Hemminger, R. L., "Graph reconstruction -- A survey," Research Report CORR 76-49, Dept. of Comb. and Opt., University of Waterloo, Waterloo, Ontario, Canada, 1976.

18. Bondy, J. A. and Murty, U. S. R., Graph Theory with Applications, Macmillan, London; American Elsevier, New York, 1976.

19. Brini, A., "A class of rank-invariants for perfect matroid designs," Europ. J. Comb. 1 (1980), 33-38.

20. Brooks, R. L., "On colouring the nodes of a network," Proc. Cambridge Phil. Soc. 37 (1941), 194-197.

21. Brouwer, A. E. and Schriver, A., "The blocking number of an affine space," J. Comb. Th. (A) 24 (1978), 251-253.

22. Bruen, A. A. and de Resmini, M., "Blocking sets in affine planes" (preprint, 1981).

23. Bruen, A. A. and Thas, J. A., "Blocking sets," Geom. Dedic. 6 (1977), 193-203.

24. Brylawski, T., "A Combinatorial model for series-parallel networks," Transactions of the AMS, 154 (1971), 1-22.

25. __________, "Some properties of basic families of subsets," Disc. Math. 6 (1973), 333-341.

26. __________, "The Tutte-Grothendieck ring," Algebra Universalis 2 (1972), 375-388.

27. __________, "A Decomposition for combinatorial geometries," Transactions of the AMS, 171 (1972), 235-282.

28. __________, "Reconstructing combinatorial geoemetries," Graphs and Combinatorics, Springer-Verlag, Lecture Notes in Mathematics 406 (1974), 226-235.

29. __________, "Modular constructions for combinatorial geometries," Transactions of AMS, 203 (1975), 1-44.

30. __________, "On the nonreconstructibility of combinatorial geometries," Journal of Comb. Theory (B), 19 (1975), 72-76.

31. Brylawski, T., "An Affine representation for transversal geometries," *Studies in Applied Mathematics*, 54 (1975), 143-160.

32. ___________, "A Combinatorial perspective on the Radon convexity theorem," Geometriae Dedicata, 5 (1976), 459-466.

33. ___________, "A Determinantal identity for resistive networks," *SIAM J. Appl. Math.*, 32 (1977), 443-449.

34. ___________, "Connected matroids with smallest Whitney numbers," *Discrete Math.* 18 (1977), 243-252.

35. ___________, "The Broken-circuit complex," *Transactions of AMS*, 234 (1977), 417-433.

36. ___________, "Geometrie combinatorie e Loro applicazioni" (1977).
"Funzioni di Möbius" (1977).
"Teoria dei Codici e matroidi" (1979).
"Matroidi coordinabili" (1981).
University of Rome Lecture Series.

37. ___________, "Intersection theory for embeddings of matroids into uniform geometries," *Studies in Applied Mathematics* 61 (1979), 211-244.

38. ___________, "The Affine dimension of the space of intersection matrices," *Rendiconti di Mathematics* 13 (1980), 59-68.

39. ___________, "Intersection theory for graphs," *J. Comb. Th. (B)* 30 (1981), 233-246.

40. ___________, "Hyperplane reconstruction of the Tutte polynomial of a geometric lattice," *Discrete Math.* 35 (1981), 25-38.

41. Brylawski, T. and Kelly, D., "Matroids and combinatorial geometries," *Studies in Combinatorics*, G.-C. Rota, ed., Math. Association of America, 1978.

42. ___________, *Matroids and Combinatorial Geometries*, Carolina Lecture Series Volumn 8, Chapel Hill, N. C., 1980.

43. Brylawski, T., Lo Re, P. M., Mazzocca, F., and Olanda, D., "Alcune applicazioni della Teoria dell' intersezione alle geometrie di Galois," *Ricerche di Matematica* 29 (1980), 65-84.

44. Brylawski, T. and Lucas, T. D., "Uniquely representable combinatorial geometries," Proceedings of the *Colloquio Internazionale sul tema Teorie Combinatorie*, Rome, 1973, *Atti Dei Convegni Lincei* 17, Tomo I (1976), 83-104.

45. Brylawski, T. and Oxley, J., "The Broken-circuit complex: its structure and factorizations," *European J. Combinatorics* 2 (1981), 107-121.

46. ___________, "Several identities for the characteristic polynomial of a combinatorial geometry," *Discrete Math.* 31 (1980), 161-170.

47. Cardy, S., "The Proof of and generalisations to a conjecture by Baker and Essam," *Discrete Math.* 4 (1973), 101-122.

48. Cordovil, R., "Contributions à la théorie des géométries combinatories," Thesis, l'Université Pierre et Marie Curie, Paris, France.

49. ___________, "Sur l'evaluation t(M;2,0) du polynome de Tutte d'un matroïde et une conjecture de B. Grünbaum relative aux arrangements de droites du plan " (preprint, 1980).

50. Cordovil, R., Las Vergnas, M., and Mandel, A., "Euler's relation, Möbius functions, and matroid identities " (preprint, 1980).

51. Cossu, A., "Su alcune propretà dei {k,n}-archi di un piano proiettivo sopra un corpo finito," *Rend. di Mat.* (5), 20 (1961), 271-277.

52. Crapo, H. H., "The Möbius function of a lattice," *J. Comb. Th.* 1 (1966), 126-131.

53. ___________, "A Higher invariant for matroids," *J. Comb. Th.* 2 (1967), 406-417.

54. ___________, "Möbius inversion in lattices," *Archiv. der Math.* 19 (1968), 595-607.

55. ___________, "The Joining of exchange geometries," *J. Math. Mech.* 17 (1968), 837-852.

56. ___________, "The Tutte polynomial," *Aequationes Math.* 3 (1969), 211-229.

57. ___________, "Chromatic polynomials for a join of graphs," Colloquia Mathematica Societatis János Bolyai, *Combinatorial Theory and its Applications*, Balatonfüred (Hungary), 1969, 239-245.

58. ___________, "Erecting geometries," *Proceedings of 2nd Chapel Hill Conference on Combinatorial Math.* (1970), 74-99.

59. ___________, "Constructions in combinatorial geometries," (N.S.F. Advanced Science Seminar in Combinatorial Theory) (*Notes*, Bowdoin College), 1971).

60. Crapo, H. H. and Rota, G.-C., "On the Foundations of Combinatorial Theory: Combinatorial Geometries (preliminary edition), M.I.T. Press, 1970.

61. d'Antona, O. and Kung, J. P. S., "Coherent orientations and series-parallel networks," Disc. Math. 32 (1980), 95-98.

62. Deza, M., "On perfect matroid designs," Proc. Kyoto Conference, 1977, 98-108.

63. Deza, M. and Singi, N. M., "Some properties of perfect matroid designs," Ann. Disc. Math. 6 (1980).

64. Dirac, G. A., "A roperty of 4-chromatic graphs and some remarks on critical graphs," J. London Math. Soc. 27 (1952), 85-92.

65. Dowling, T. A., "Codes, packings and the critical problem," Atti del Convegno di Geometria Combinatoria e sue Applicazioni (Perugia , 1971), 210-224.

66. ____________, "A Class of geometric lattices based on finite groups," J. Comb. Th. 13, (1973), 61-87.

67. ____________, "A q-analog of the partition lattice," A Survey of Combinatorial Theory, North Holland (1973), 101-115.

68. Dowling, T. A. and Wilson, R. M., "The Slimmest geometric lattices," Trans. Amer. Math. Soc. 196 (1974), 203-215.

69. Edmonds, J. and Fulkerson, D. R., "Transversals and matroid partition," J. Res. Nat. Búr. Stand. 69B (1965), 147-153.

70. Edmonds, J., Murty, U. S. R., and Young, P., "Equicardinal matroids and matroid designs," Combinatorial Mathematics and its Applications, Chapel Hill, N. C., (1970), 498-582.

71. Essam, J. W., "Graph theory and statistical physics," Discrete Math. 1 (1971), 83-112.

72. Goldman, J. and Rota, G.-C., "The Number of subspaces of a vector space," Recent Progress in Combinatorics, Academic Press, New York, 1969, 75-83.

73. Greene, C., "An Inequality for the Möbius function of a geometric lattice," Proc. Conf. on Möbius Algebras (Waterloo), 1971; also: Studies in Appl. Math. 54 (1975), 71-74.

74. ____________, "On the Möbius algebra of a partially ordered set," Advances in Math. 10 (1973), 177-187.

75. ____________, "Weight enumeration and the geometry of linear codes," Studies in Appl. Math. 55 (1976), 119-128.

76. ____________, "Acyclic orientations," (Notes), Higher Combinatorics, M. Aigner, ed., D. Reidel, Dordrecht (1977), 65-68.

77. Greene, C. and Zaslavsky, T., "On the interpretation of Whitney numbers through arrangements of hyperplanes, zonotopes, non-Radon partitions, and acyclic orientations of graphs " (preprint, 1980).

78. Greenwell, D. L. and Hemminger, R. L., "Reconstructing graphs," The Many Facets of Graph Theory, Springer-Verlag, Berlin, 1969, 91-114.

79. Hardy, G. H., Littlewood, J. E., and Pólya, G., Inequalities, Cambridge U. Press, 1934.

80. Heron, A. P., "Matroid polynomials," Combinatorics (Institute of Math. & Appl.) D. J. A. Welsh and D. R. Woodall, eds., 164-203.

81. Hsieh, W. N. and Kleitman, D. J., "Normalized matching in direct products of partial orders," Studies in Applied Math. 52 (1973), 285-289.

82. ____________, "Flows and generalized coloring theorems in graphs," J. Comb. Th. (B) 26 (1979), 205-216.

83. ____________, "A Constructive approach to the critical problem " (to appear: Europ. J. Combinatorics, 1981).

84. Kahn, J. and Kung, J. P. S., "Varieties and universal models in the theory of combinatorial geometries," Bulletin of the AMS 3 (1980), 857-858.

85. Kelly, D. G. and Rota, G.-C., "Some problems in combinatorial geometry," A Survey of Combinatorial Theory, North Holland, 1973, 309-313.

86. Knuth, D. E., "The Asymptotic number of geometries," J. Comb. Th. (A) 17 (1974), 398-401.

87. Las Vergnas, M., "Matroids orientables," C. R. Acad. Sci. (Paris), 280A (1975), 61-64.

88. ____________, "Extensions normales d'un matroide, polynôme de Tutte d'un morphisme," C. R. Acad. Sci. (Paris), 280 (1975), 1479-1482.

89. ____________, "Acyclic and totally cyclic orientations of combinatorial geometries," Disc. Math., 20 (1977), 51-61.

90. ____________, "Sur les activités des orientations d'une geometrie combinatoire," Colloque Mathématiques Discrètes: Codes et Hypergraphes, Bruxelles, 1978, 293-300.

91. ____________, "Eulerian circuits of 4-valent graphs imbedded in surfaces," Colloquia Mathematica Societatis János Bolyai 25, Algebraic Methods in Graph Theory, Szeged (Hungary), 1978, 451-477.

92. Las Vergnas, M., "On Eulerian partitions of graphs," Graph Theory and Combinatorics, R. J. Wilson (ed.), Research Notes in Math. 34, Pitman Advanced Publishing Program, 1979.

93. ___________, "On the Tutte polynomial of a morphism of matroids'," Proc. Joint Canada-France Combinatorial Colloquium, Montréal 1979, Annals Discrete Math. 8 (1980), 7-20.

94. Lindner, C. C. and Rosa, A., "Steiner quadruple systems -- a survey," Discrete Math. 22:147-181 (1978).

95. Lindström, B., "On the chromatic number of regular matroids," J. Comb. Theory (B) 24 (1978), 367-369.

96. Lucas, T. D., "Properties of rank preserving weak maps," A.M.S. Bull. 80 (1974), 127-131.

97. ___________, "Weak maps of combinatorial geometries," Trans. Am. Math. Soc. 206 (1975), 247-279.

98. Macwilliams, F. J., "A Theorem on the distribution of weights in a systematic code," Bell System Tech. J. 42 (1963), 79-94.

99. Martin, P., "Enumérations eulériennes dans les multigraphes et invariants de Tutte-Grothendieck," Thesis, Grenoble, 1977.

100. ___________, "Remarkable valuation of the dichromatic polynomial of planar multigraphs," J. Comb. Th. (B) 24 (1978), 318-324.

101. Mason, J., "Matroids: unimodal conjectures and Motzkin's theorem," Combinatorics (Institute of Math. & Appl.) (D. J. A. Welsh and D. R. Woodall, eds., 1972), 207-221.

102. ___________, "Matroids as the study of geometrical configurations," Higher Combinatorics, M. Aigner, ed., D. Reidel, Dordrecht, Holland, 1977, 133-176.

103. Minty, G. J., "On the axiomatic foundations of the theories of directed linear graphs, electrical networks and network programming," Journ. Math. Mech. 15 (1966), 485-520.

104. Mullin, R. C. and Stanton, R. G., "A Covering problem in binary spaces of finite dimension," Graph Theory and Related Topics (J. A. Bondy and U.S.R. Murty, eds.) Academic Press, New York, 1979.

105 Murty, U.S.R., "Equicardinal matroids," J. Comb. Th. 11 (1971), 120-126.

106. Nash-Williams, C. St. J.A., "An Application of matroids to graph theory," Theory of Graphs International Symposium (Rome), Dunod (Paris) (1966), 263-265.

107. Oxley, J. G., "Colouring, packing and the critical problem," Quart. J. Math. Oxford, (2), 29, 11-22.

108. ____________, "Cocircuit coverings and packings for binary matroids," Math. Proc. Cambridge Philos. Soc. 83 (1978), 347-351.

109. ____________, "On cographic regular matroids," Discrete Math. 25 (1979), 89-90.

110. ____________, "A Generalization of a covering problem of Mullin and Stanton for matroids," Combinatorial Mathematics VI. Edited by A. F. Horadam and W. D. Wallis, Lecture Notes in Mathematics Vol. 748, Springer-Verlag, Berlin, Heidelberg, New York, 1979, 92-97.

111. ____________, "On a covering problem of Mullin and Stanton for binary matroids," Aequationes Math. 19 (1979), 118, and 20 (1980), 104-112.

112. ____________, "On Crapo's beta invariant for matroids," Studies in Appl. Math. (to appear).

113. ____________, "On a matroid identity " (preprint, 1981).

114. Oxley, J. G., Prendergast, K. and Row, D. H., "Matroids whose ground sets are domains of functions " (to appear, J. Austral. Math. Soc. (A).)

115. Oxley, J. G. and Welsh, D. J. A., "On some percolation results of J. M. Hammersley," J. Appl. Probability 16 (1979), 526-540.

116. ____________, and ____________, "The Tutte polynomial and percolation," Graph Theory and Related Topics. Edited by J. A. Bondy and U.S.R. Murty, Academic Press, New York, San Francisco, London, 1979, 329-339.

117. Read, R. C., "An Introduction to chromatic polynomials," J. Comb. Th., 4 (1968), 52-71.

118. Rota, G.-C., "On the foundations of combinatorial theory I," Z. Wahrsch, 2 (1964), 340-368.

119. ____________, "Combinatorial analysis as a theory," Hedrick Lectures, Math. Assoc. of Amer., Summer Meeting, Toronto, 1967.

120. ____________, "Combinatorial theory, old and new," Int. Cong. Math. (Nice) (1970) 3, 229-233.

121. Scafati Tallini, M., "{k,n}-archi di un piano grafico finito, con particolare riguardo a quelli con due caratteri, Nota I, II," *Rend. Acc. Naz. Lincei* 40 (8) (1966), 812-818, 1020-1025.

122. ___________, "Calotte di tipo (m,n) in uno spazio di Galois $S_{r,q}$," *Rend. Acc. Naz. Lincei* 53(8) (1973), 71-81.

123. Segre, B., *Lectures on Modern Geometry*, Edizioni Creomonese, Roma, 1961.

124. Seymour, P. D., "On Tutte's extension of the four-colour problem " (preprint, 1979).

125. ___________, "Decomposition of regular matroids," *J. Comb. Th. (B)* 28 (1980), 305-359.

126. ___________, "Nowhere-zero 6-flows," *J. Comb. Th. (B)* 30 (1981), 130-135.

127. Seymour, P. D. and Welsh, D. J. A., "Combinatorial applications of an inequality from statistical mechanics," *Math. Proc. Cambridge Phil. Soc.* 77 (1975), 485-497.

128. Shepherd, G. C., "Combinatorial properties of associated zonotopes," *Can. J. Math.* 26 (1974), 302-321.

129. Smith, C. A. B., "Electric currents in regular matroids," *Combinatorics* (Institute of Math. & Appl.) (D. J. A. Welsh & D. R. Woodall, eds., 1972), 262-285.

130. ___________, "Patroids," *J. Comb. Th.* 16 (1974), 64-76.

131. Stanley, R., "Modular elements of geometric lattices," *Algebra Universalis*, 1 (1971), 214-217.

132. ___________, "Supersolvable semimodular lattices," *Proc. Conference on Möbius Algebras*, University of Waterloo, 1971, pp. 80-142.

133. ___________, "Supersolvable lattices," *Alg. Universalis* 2 (1972), 197-217.

134. ___________, "Acyclic orientations of graphs," *Disc. Math.* 5 (1974), 171-178.

135. Szekeres, G. and Wilf, H., "An Inequality for the chromatic number of a graph," *J. Comb. Th.* 4 (1968), 1-3.

136. Tallini, G., "Problemi e risultati sulle geometrie di Galois," Rel. N. 30, lst. di Mat. dell' Univ. di Napoli (1973).

137. Tutte, W. T., "A Ring in graph theory," Proc. Cambridge Phil. Soc. 43 (1947), 26-40.

138. ____________, "A Contribution to the theory of chromatic polynomials," Canad. J. Math. 6 (1954), 80-91.

139. ____________, "A Class of Abelian groups," Canad. J. Math. 8 (1956), 13-28.

140. ____________, "Matroids and graphs," Trans. Amer. Math. Soc. 90 (1959), 527-552.

141. ____________, "Lectures on matroids," J. Res. Nat. Bur. Stand. 69B (1965), 1-48.

142. ____________, "On the algebraic theory of graph coloring," J. Comb. Th. 1 (1966), 15-50.

143. ____________, "On dichromatic polynomials," J. Comb. Th. 2 (1967), 301-320.

144. ____________, "Projective geometry and the 4-color problem," Recent Progress in Combinatorics (W. T. Tutte, ed.) Academic Press 1969, 199-207.

145. ____________, "Codichromatic graphs," J. Comb. Th. 16 (1974), 168-175.

146. ____________, "All the king's men (a guide to reconstruction)," Graph Theory and Related Topics, Academic Press, 1979, 15-33.

147. Van Lint, J. H., Coding Theory, Springer Lecture Notes, 201, (1971).

148. Walton, P. N. and Welsh, D. J. A., "On the chromatic number of binary matroids," Mathematika 27 (1980), 1-9.

149. Welsh, D. J. A., "Euler and bipartite matroids," J. Comb. Th. 6 (1969), 375-377.

150. ____________, "Combinatorial problems in matroid theory," Combinatorial Mathematics and its Applications, Academic Press, (1971), 291-307.

151. ____________, Matroid Theory, Academic Press, London, 1976.

152. ____________, "Percolation and related topoics," Science Progress 64 (1977).

153. ____________, "Colouring problems and matroids," Proc. Seventh British Combinatorial Conference, Cambridge U. Press (1979), 229-257.

154. Welsh, D. J. A., "Colourings, flows and projective geometry," Nieuw Archief voor Wiskunde (3), 28 (1980), 159-176.

155. White, N., "The Critical problem and coding theory," Research Paper, SPS-66 Vol. III, Section 331, Jet Propulsion Laboratory, Pasadena, CA. (1972).

156. Whitney, H., "A Logical expansion in mathematics," _Bull. Amer. Math. Soc._ 38 (1932), 572-579.

157. ___________, "The Coloring of graphs," _Annals of Math._ 33 (1932), 688-718.

158. ___________, "2-isomorphic graphs," _Amer. J. Math._ 55 (1933), 245-254.

159. ___________, "On the abstract properties of linear dependence," _Amer. J. Math. 57_ (1935), 509-533.

160. Wilf, H. S., "Which polynomials are chromatic?" _Atti dei Convegni_ Lincei 17, Tomo 1 (1976), 247-256.

161. Winder, R. O., "Partitions of n-space by hyperplanes," _SIAM J. Appl. Math._ 14 (1966), 811-818.

162. Young, P. and Edmonds, J., "Matroid designs," _J. Res. Nat. Bur. Stan._ 72B (1972), 15-44.

163. Zaslavsky, T., "Facing up to arrangements: face count formulas for partitions of space by hyperplanes," _Memoirs Amer. Math. Soc._ 154 (1975).

164. ___________, "Counting faces of cut-up spaces," _Bull. Amer. Math. Soc._ 81 (1975), 916-918.

165. ___________, "Maximal dissections of a simplex," _J. Comb. Th. (A)_ 20 (1976), 244-257.

166. ___________, "The Möbius function and the characteristic polynomial" (preprint: chapter for _Combinatorial Geometries_, H. Crapo, G.-C. Rota, and N. White eds.).

167. ___________, "Arrangements of hyperplanes; matroids and graphs," _Proc. Tenth S.E. Conf. on Combinatorics, Graph Theory and Computing (Boca Raton, 1979)_, Vol. II, 895-911, Utilitas Math. Publ. Co., Winnipeg, Man., 1979.

168. ___________, "The Geometry of root systems and signed graphs," _Amer. Math. Monthly_, 88 (1981), 88-105.

169. Zaslavsky, T., "Signed graphs " (preprint, 1980).

170. ____________, "Orientation of signed graphs " (preprint, 1980).

171. ____________, "Signed graph coloring " (preprint, 1980).

172. ____________, "Chromatic invariants of signed graphs " (preprint, 1980).

173. ____________, "Bicircular geometry and the lattice of forest of a graph " (preprint, 1980).

174. ____________, "The slimmest arrangements of hyperplanes: I. Geometric lattices and projective arrangements " (preprint, 1980).

175. ____________, "The slimmest arrangements of hyperplanes: II. Basepointed geometric lattices and Euclidean arrangements (preprint, 1980).

CENTRO INTERNAZIONALE MATEMATICO ESTIVO

(C.I.M.E.)

ON 3-CONNECTED MATROIDS AND GRAPHS

JAMES G. OXLEY

ON 3-CONNECTED MATROIDS AND GRAPHS

James G. Oxley
University of North Carolina, Chapel Hill, USA
and
Australian National University, Canberra, Australia

Introduction

This expository paper will be concerned with Tutte's notion of n-connectedness for matroids. In particular, we shall show how various results for 3-connected graphs can be extended to matroids.

The terminology used here for matroids and graphs will in general follow Welsh [19] and Bondy and Murty [1] respectively. In particular, if T is a subset of a matroid M, then rkT will denote the rank of T, while $M\backslash T$ and M/T will denote respectively the deletion and contraction of T from M. The uniform matroid of rank r on a set of k elements will be denoted $U_{r,k}$. If G is a graph and n is a positive integer, G will be called n-*connected* if one needs to delete at least n vertices from G in order to obtain a disconnected or single-vertex graph. Motivated by this graph-theoretic concept, Tutte [17,18] introduced the following definition of n-connectedness for matroids. If M is a matroid having ground set $E(M)$ and k is a positive integer, M is said to be k-*separated* if there is a subset T of $E(M)$ such that $|T| \geq k$, $|E(M)\backslash T| \geq k$ and

$$\mathrm{rk}\,T + \mathrm{rk}(E(M)\backslash T) - \mathrm{rk}\,M = k - 1 \;.$$

If n is a positive integer, the matroid M is n-*connected* provided there is no k less than n for which M is k-separated.

The notions of n-connectedness of a graph G and n-connectedness of the corresponding cycle matroid $M(G)$ do not, in general, coincide. However,it is straightforward to check that

(1) *for* $n = 2$ *and* $n = 3$, *if* G *is a simple graph having at least four vertices, then* G *is* n-*connected if and only if* $M(G)$ *is* n-*connected.*

For larger values of n, the precise relationship between the graph and matroid-theoretic notions of n-connectedness is discussed in [3] and [12].

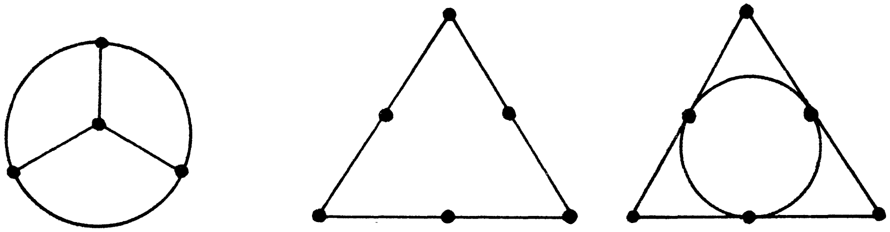
The matroid concept of n-connectedness generalizes the well-known idea of non-separability or connectivity for matroids. In fact, a matroid is 2-connected if and only if it is non-separable. A further appealing property of this concept is that

(2) *a matroid is* n-*connected if and only if its dual is* n-*connected.*

In [15], Seymour has characterized 3-connected matroids in terms of a decomposition operation which is closely related to Brylawski's operation of parallel connection of matroids [2]. For $i = 1,2$, let M_i be a matroid on a set S_i where $|S_i| \geq 3$ and suppose that $S_1 \cap S_2 = \{p\}$ where p is neither a loop nor a coloop of M_1 or M_2. Then the 2-*sum* of M_1 and M_2 is the matroid on the set $S_1 \cup S_2$ having as its collection of circuits all circuits of M_1 not containing p, all circuits of M_2 not containing p and all sets of the form $(C_1\backslash p) \cup (C_2\backslash p)$ where C_i is a circuit of M_i containing p.

(3) **PROPOSITION** [15, (2.10)(b)]. *A matroid is* 3-*connected if and only if it is non-separable and cannot be obtained as a* 2-*sum of two matroids.*

One very important class of 3-connected matroids is the class of cycle matroids of wheels. Suppose that $m \geq 3$. The *wheel* $\mathcal{W}_m$ *of order* m is a graph having $m + 1$ vertices, m of which lie on a cycle (the *rim*); the remaining vertex is joined by a single edge (a *spoke*) to each of the vertices of the rim. Evidently $\mathcal{W}_m$ is simple and 3-connected. Hence, by (1), $M(\mathcal{W}_m)$ is a 3-connected matroid. However, whenever an edge is deleted from $\mathcal{W}_m$ the resulting graph has a vertex of degree two and so is not 3-connected. It follows on applying (1) again that $M(\mathcal{W}_m)$ is a *minimally* 3-*connected matroid*. That is, $M(\mathcal{W}_m)$ is a 3-connected matroid for which no single-element deletion is also 3-connected. Now it is easy to check that $M(\mathcal{W}_m)$ is isomorphic to its dual. Therefore, as $M(\mathcal{W}_m)$ is minimally 3-connected, it follows from (2) that no single-element contraction of $M(\mathcal{W}_m)$ is 3-connected. Another class of minimally 3-connected matroids whose members share this property with the cycle matroids of wheels is the class of whirls. The *whirl* $\mathcal{W}^m$ is the matroid on $E(\mathcal{W}_m)$ having as its collection of circuits, all those circuits of $M(\mathcal{W}_m)$ other than the rim, together with all sets of edges formed by adding a single spoke to the set of edges of the rim. In Figure 1, the wheel $\mathcal{W}_3$ is shown along with a Euclidean representation for the whirl $\mathcal{W}^3$. For comparison, a Euclidean representation for $M(\mathcal{W}_3)$ is also shown. We note that $\mathcal{W}_3$ is just the complete graph K_4.



W_3 W^3 $M(W_3)$

Figure 1

The following theorem underlies most of the results in the remainder of this paper. It is a matroid generalization of an earlier graph-theoretic theorem [16, (4.1)] and, as such, typifies many of the results in this area of research.

(4) THEOREM (Tutte [17, 8.3]). *Let* M *be a minimally* 3-*connected matroid for which no single-element contraction is* 3-*connected. Then* M *is isomorphic to a whirl or the cycle matroid of a wheel.*

From this theorem one can deduce a recursive construction for all 3-connected matroids of rank at least three. A *non-trivial extension* of a matroid M is an extension N of M by a single element e such that e is neither a loop nor a coloop of N and e is not in parallel with any element of M. On the other hand, N is a *non-trivial lift* of M if N^* is a non-trivial extension of M^*. Thus N is a non-trivial lift of M if there is an element e of N such that N/e = M where e is neither a loop nor a coloop of N and e is not in series with any element of M.

(5) THEOREM [10, Theorem 4.1]. *A matroid of rank at least three is* 3-*connected if and only if it is a whirl, the cycle matroid of a wheel, or* $U_{3,5}$, *or is obtainable from such a matroid by a sequence of the following*

operations:

(i) *non-trivial extensions; and*

(ii) *non-trivial lifts* .

The remainder of this paper will concentrate on minimally 3-connected matroids. In particular, we shall show that a number of results of Halin for minimally 3-connected graphs have matroid generalizations or analogues. Many of Halin's results have been extended in another direction by Mader who has generalized them to minimally n-connected graphs for arbitrary n (see, for example, [7] and the survey paper [8]).

(6) THEOREM (Halin [4, Satz 7.6]). *Let* G *be a minimally* 3*-connected graph having* m *vertices. Then*

$$|E(G)| \leq \begin{cases} 2m - 2, & \text{if } m \leq 6 ; \\ 3m - 9, & \text{if } m \geq 7 . \end{cases}$$

Moreover, the following are the only graphs attaining equality in these bounds:

$$\mathcal{W}_{m-1} \quad \text{for} \quad 4 \leq m \leq 6 ;$$

$$\mathcal{W}_6 \text{ and } K_{3,4} \quad \text{for} \quad m = 7; \quad \text{and}$$

$$K_{3,m-3} \quad \text{for} \quad m \geq 8 .$$

In the case of arbitrary minimally 3-connected matroids, precisely the same bounds hold as in the graph case.

(7) THEOREM [9, Theorem 4.7]. *Let* M *be a minimally* 3*-connected matroid of rank at least three. Then*

$$|E(M)| \leq \begin{cases} 2\,\mathrm{rk}\,M , & \text{if } \mathrm{rk}\,M \leq 5 ; \\ 3\,\mathrm{rk}\,M - 6, & \text{if } \mathrm{rk}\,M \geq 6 . \end{cases}$$

From Theorem 6, we know that the bounds in the preceding result are best-possible. Moreover, those matroids attaining equality in Theorem 7 have been characterized [9, Theorem 5.2 and Corollary 5.11]. However, this result is rather cumbersome and, instead of stating it, we merely note that if M is binary and minimally 3-connected, and M attains the relevant bound in the preceding theorem, then M is graphic [9, Theorem 5.12]. Thus M is isomorphic to the cycle matroid of a wheel or a complete bipartite graph $K_{3,m-3}$.

A lower bound on the number of elements in a minimally n-connected matroid of given rank is considerably easier to obtain than Theorem 7. Moreover, whereas no analogue of Theorem 7 is known for $n > 3$, the following lower bound holds for all $n \geq 2$.

(8) THEOREM [9, Theorem 3.2]. *Let* M *be a minimally* n*-connected matroid of rank* r *where* $r,n \geq 2$. *Then*

$$|E(M)| \geq \begin{cases} r + n - 1, & \textit{if} \quad r \geq n ; \\ 2r - 1, & \textit{if} \quad r < n . \end{cases}$$

Moreover, only $U_{r,r+n-1}$ *and* $U_{r,2r-1}$ *attain equality here.*

We now turn to another property of minimally 3-connected graphs and the corresponding property of minimally 3-connected matroids.

(9) THEOREM (Halin [5, Satz 6]). *If* G *is a minimally* 3*-connected graph, then* G *has at least* $\frac{2|V(G)|+6}{5}$ *vertices of degree three.*

It is well-known that in a 2-connected loopless graph G, the set of edges meeting at a vertex forms a cocircuit in $M(G)$. Thus one possible matroid analogue of a vertex of degree three is a 3-element cocircuit. Theorem 9 now prompts the question as to what one can say about the number of 3-element cocircuits in an arbitrary minimally 3-connected matroid. The following lemma extends a result of Seymour [14, (2.3)] for minimally 2-connected matroids.

(10) **LEMMA** [9, Theorem 2.5]. *If* C *is a circuit of a minimally* 3-*connected matroid* M *and* $|E(M)| \geq 4$, *then* M *has at least two distinct* 3-*element cocircuits meeting* C.

This lemma, which is proved by induction on the cardinality of C, contains the core of the proof of the following result.

(11) **THEOREM** [11, §2]. *Let* M *be a minimally* 3-*connected matroid having at least four elements. Then* M *has at least* $1/2(|E(M)| - \text{rk} M) + 1$ 3-*element cocircuits.*

It is straightforward to check that for all $k \geq 4$, the matroid $M(K_{3,k})$ is minimally 3-connected and attains the bound in the preceding result. We now sketch the main idea of the proof of Theorem 11.

Proof outline. Let X be the set of elements of M which are contained in some 3-element cocircuit. By the lemma, X meets every circuit of M, hence X contains a cobasis B^* of M. But B^* contains at most two elements of any 3-element cocircuit of M. Hence, the number of such cocircuits is at least $1/2|B^*| = 1/2(|E(M)| - \text{rk} M)$. If one uses the full force of Lemma 10, then it is not difficult to improve this bound by one and thereby obtain the theorem. The details may be found in the proof of Proposition 2.20 of [11].

On applying Theorem 11 to graphs, one obtains that

(12) *a minimally* 3-*connected graph* G *has at least*
$1/2(|E(G)| - |V(G)| + 1) + 1$ *minimal cutsets of size three.*

Now, in a minimally 3-connected graph, one is more interested in vertices of degree three than in arbitrary minimal cutsets of size three. This leads one to ask whether one can strengthen (12) by replacing "minimal cutsets of size three" by "vertices of degree three." The next theorem answers this question.

(13) THEOREM [11, Proposition 2.20]. *A minimally* 3-*connected graph has at least* $1/2(|E(G)| - |V(G)| + 3)$ *vertices of degree three.*

The proof of this result is similar to the proof of Theorem 11 and uses instead of Lemma 10 its graph-theoretic analogue (see Halin [5, Satz 5]).

Both Theorems 9 and 13 give lower bounds on the number of vertices of degree three in a minimally 3-connected graph G. For certain values of $|E(G)|$, the bound in Theorem 9 is the sharper, while for other values of $|E(G)|$, Theorem 13 gives the sharper bound. The following result is obtained by combining the two theorems and for each value of $|E(G)|$ choosing the better of the two bounds. A small amount of additional argument enables Halin's bound to be sharpened within the given range. We observe that for a minimally 3-connected graph G, one can easily check that $|E(G)| \geq 3/2|V(G)|$. Moreover, by Theorem 6, $|E(G)| \leq 3|V(G)| - 9$. The number of vertices of degree three in G will be denoted by $\nu_3(G)$.

(14) THEOREM [11, Proposition 2.20]. *Let* G *be a minimally* 3-*connected graph. Then*

$$\nu_3(G) \geq \begin{cases} \dfrac{2|V(G)|+7}{5} & \textit{for } \dfrac{3|V(G)|}{2} \leq |E(G)| < \dfrac{9|V(G)|-3}{5} \ ; \\ \dfrac{|E(G)|-|V(G)|+3}{2} & \textit{for } \dfrac{9|V(G)|-3}{5} \leq |E(G)| \leq 3|V(G)| - 9. \end{cases}$$

As another application of Theorem 13 one can characterize all minimally 3-connected graphs attaining equality in Halin's bound [13, Theorem 4.5].

We close by briefly considering minimally n-connected matroids and graphs for $n \geq 4$. The proofs of most of the results stated above rely on Tutte's characterization, in the case $n = 3$, of those minimally n-connected matroids for which no single-element contraction remains n-connected (Theorem 4). The characterization of such matroids when $n \geq 4$ is an open problem. Mader [7, Satz 1] has shown that every circuit in a minimally n-connected graph meets a vertex of degree n and, from this, using the proof method of Theorem 11, one can deduce a new lower bound on the number of vertices of degree n in a minimally n-connected graph [11, Proposition 2.19].

The links between graph theory and matroid theory have always been close (see, for example, [20, 6]). The results above show that in the study of n-connectedness these links can be successfully exploited in both directions to obtain not only new matroid results but also new graph results.

Acknowledgement. The author gratefully acknowledges that this paper was written with the partial support of a Fulbright Postdoctoral Fellowship while he was visiting UNC on leave from ANU.

References

1. J. A. Bondy and U.S.R. Murty, *Graph Theory with Applications* (Macmillan, London; American Elsevier, New York, 1976).
2. T. H. Brylawski, A combinatorial model for series-parallel networks, *Trans. Amer. Math. Soc.* 154 (1971), 1-22.
3. W. H. Cunningham, On matroid connectivity, *J. Combin. Theory Ser. B* (to appear).
4. R. Halin, Zur Theorie der n-fach zusammenhängenden Graphen, *Abh. Math. Sem. Univ. Hamburg* 33 (1969), 133-164.
5. R. Halin, Untersuchungen über minimale n-fach zusammenhängende Graphen, *Math. Ann.* 182 (1969), 175-188.
6. F. Harary and D. Welsh, Matroids versus graphs, *The Many Facets of Graph Theory* (Lecture Notes in Mathematics Vol. 110, Springer-Verlag, Berlin, Heidelberg, New York, 1969) pp. 155-170.
7. W. Mader, Ecken vom Grad n in minimalen n-fach zusammenhängenden Graphen, *Arch. Math. (Basel)* 23 (1972), 219-224.

8. W. Mader, Connectivity and edge-connectivity in finite graphs, *Surveys in Combinatorics,* Ed. B. Bollobás (London Math. Soc. Lecture Notes No. 38, Cambridge University Press, 1979) pp. 66-95.

9. J. G. Oxley, On matroid connectivity, *Quart. J. Math. Oxford* (2) (to appear).

10. J. G. Oxley, On 3-connected matroids, *Canad. J. Math.* (to appear).

11. J. G. Oxley, On connectivity in matroids and graphs, *Trans. Amer. Math. Soc.* (to appear).

12. J. G. Oxley, On a matroid generalization of graph connectivity (submitted).

13. J. G. Oxley, On some extremal connectivity results for graphs and matroids (submitted).

14. P. D. Seymour, Packing and covering with matroid circuits, *J. Combin. Theory Ser. B* 28 (1980), 237-242.

15. P. D. Seymour, Decomposition of regular matroids, *J. Combin. Theory Ser. B* 28 (1980), 305-359.

16. W. T. Tutte, A theory of 3-connected graphs, *Nederl. Akad. Wetensch. Proc. Ser. A* 64 (1961), 441-455.

17. W. T. Tutte, Connectivity in matroids, *Canad. J. Math.* 18 (1966), 1301-1324.

18. W. T. Tutte, Connectivity in matroids, *Graph Theory and its Appplications,* Ed. B. Harris (Academic Press, New York, 1970) pp. 113-119.

19. D.J.A. Welsh, *Matroid Theory* (London Math. Soc. Monographs No. 8, Academic Press, London, 1976).

20. H. Whitney, On the abstract properties of linear dependence, *Amer. J. Math.* 57 (1935), 509-533.

CENTRO INTERNAZIONALE MATEMATICO ESTIVO

(C.I.M.E.)

THE POSET OF SUBPARTITIONS AND CAYLEY'S FORMULA FOR THE COMPLEXITY OF A COMPLETE GRAPH

RHODES PEELE

THE POSET OF SUBPARTITIONS AND CAYLEY'S FORMULA FOR THE COMPLEXITY OF A COMPLETE GRAPH

by

Rhodes Peele
Pembroke State University
Pembroke NC 28372 USA

I. Introduction.

A very well known theorem of Cayley asserts that there are n^{n-2} distinct trees with vertex set $\{1,2, \ldots , n\}$. We can express this result in the language of matroid theory by saying, "The complexity of the complete graph on n vertices is n^{n-2}."

Below we offer a proof of Cayley's Theorem that is based on Möbius Inversion in the generalized sense of Rota [2]. Proofs of Cayley's Theorem are legion, but the present one has the unusual feature that the inversion takes place over a poset that is not a lattice. The poset is an interesting combinatorial object that probably has other applications.

II. The Poset of Subpartitions. Define a poset P_n as follows :

α is an element of P_n iff α is a subset of some (possibly improper) subset of $\{1,2, \ldots , n\} = \underline{n}$.

The elements of P_n are ordered by containment (not refinement). Thus, $\alpha \le \beta$ iff $B \in \alpha$ (read "B is a block of α") implies that $B \in \beta$.

Further notation :

$U(\alpha)$ denotes the union of the constituent blocks of α ;

$|\alpha|$ denotes the number of blocks of α ;

ϕ denotes the minimum element of P_n (note that $|\phi| = 0$ and $U(\phi) = \phi$) ;

ν denotes the element of P_n whose only block is the singleton $\{n\}$;

a dot below a letter in a summation formula indicates the summation variable.

Observe that if $n > 1$ (which we henceforth assume), then the finite poset P_n has no maximum element and is the^r^efore not a lattice. But if α and β are comparable elements of P_n (say, $\alpha \le \beta$), then $[\alpha,\beta]$ is a Boolean algebra, and consequently,

$$\mu(\alpha,\beta) = (-1)^{|\beta| - |\alpha|}$$

where μ is the Mobius function of P_n .

The Hasse diagram of $[\nu,\infty)$ for P_4 is shown in Figure 1. Note that $[\nu,\infty)$ and P_{n-1} are isomorphic.

II. The Subpartition of a Function. Given a function $f : \underline{n} \to \underline{n}$, those $j \in \underline{n}$ for which there exists a $k > 0$ such that $f^k(j) = j$ are called recurrent. The relation iRj iff $f^k(i) = j$ for some $k > 0$ is transitive on $\underline{n}$ and becomes reflexive and symmetric when restricted to the set of recurrent elements of f. The induced subpartition of $\underline{n}$ is denoted by P(f).

Now let T be a labeled tree with vertex set $\underline{n}$. Then there is one and only one function $f : \underline{n} \to \underline{n}$ such that $f(n) = n$ and for $j > n$, $f(j) = k$ iff an edge of T joins j and k. This is intuitively clear since after we add a directed loop to T at vertex n, there is only one way to properly orient the edges of T in order to obtain a "functional digraph". For this f, we have $P(f) = \nu$, and conversely, any f that satisfies $P(f) = \nu$ comes from some tree T via the above construction (view f as a functional digraph, and erase the loop and arrows).

We may therefore identify the collection Tree(n) of labeled trees with vertex set $\underline{n}$ with the set of functions for which $P(f) = \nu$. (This identification is the starting point of an already published proof of Cayley's Theorem due to Katz (see [1]), but now the proofs diverge).

III. Cayley's Formula for Tree(n) . Denote the collection of all functions $f : \underline{n} \to \underline{n}$ by $\underline{n}^{\underline{n}}$. For $\alpha \in P_n$, define

$$g(\alpha) = | \{ f : f \in \underline{n}^{\underline{n}} \text{ and } P(f) = \alpha \} |$$

and

$$h(\alpha) = | \{ f : f \in \underline{n}^{\underline{n}} \text{ and } P(f) \geq \alpha \} | .$$

Example. Let $n = 4$ and let the blocks of α be precisely the singletons {1} and {4}. Present any $f \in \underline{4}^{\underline{4}}$ as a vector (f(1),f(2),f(3),f(4)). Then $g(\alpha) = 8$ since only these functions satisfy $P(f) = \alpha$:

(1,1,1,4) , (1,1,4,4) , (1,4,1,4) , (1,4,4,4) ,

(1,1,2,4) , (1,3,1,4) , (1,3,4,4) , (1,4,2,4) .

Further, $h(\alpha) = 16$ since only these additional functions satisfy $P(f) > \alpha$:

$$(1,2,3,4)\ ,\ (1,3,2,4)\ ,\ (1,2,2,4)\ ,\ (1,3,3,4)\ ,$$
$$(1,1,3,4)\ ,\ (1,4,3,4)\ ,\ (1,2,1,4)\ ,\ (1,2,4,4).$$

Figure 1 exhibits the values of g and h on the interval $[\nu,\infty)$.

Lemma. If α is a nonempty subpartition of $\underline{n}$, then $h(\alpha) = t(\alpha)n^{n - |U(\alpha)|}$ where $t(\alpha)$ is the number of permutations of $U(\alpha)$ whose cycles are precisely the blocks of $U(\alpha)$.

Proof. If a function f is counted by $h(\alpha)$, then every block B of α must be cyclically permuted by f. Conversely, any function f that meets this requirement, is counted by $h(\alpha)$. There are clearly $t(\alpha)n^{n - |U(\alpha)|}$ such functions, since the elements of $\underline{n}$ that do not belong to $U(\alpha)$ may be assigned arbitrary values. □

(An explicit formula for $t(\alpha)$ is easy to write down, but it will not be needed.)

Theorem (Cayley). Let $n > 1$. Then $|\mathrm{Tree}(n)| = n^{n-2}$.

Proof. For all $\alpha \in P_n$ we have

$$h(\alpha) = \sum_{\beta \geq \alpha} g(\beta)$$

and so by Möbius inversion,

$$g(\alpha) = \sum_{\beta \geq \alpha} \mu(\alpha,\beta)h(\alpha).$$

Taking $\alpha = \nu$ we get

$$|\mathrm{Tree}(n)| = g(\nu) = \sum_{\beta \geq \nu} (-1)^{|\beta|-1} h(\beta) =$$

$$\sum_{n \in S \subseteq n} \; \sum_{\substack{U(\beta) = S \\ \nu \leq \beta}} \mu(\nu,\beta)h(\beta).$$

We now fix an arbitrary subset $S \subseteq \underline{n}$ such that $n \in S$ and evaluate the inner sum. There are three cases, and all are quite simple if Figure 1 is kept in mind :

Case 1 : $|S| = 1$. There is only one term, and it contributes $\mu(\nu,\nu)h(\nu) = (-1)^{1-1} t(\nu)n^{n-1} = n^{n-1}$ to the outer sum.

Case 2 : $|S| = 2$. Again there is only one term, and it has the form $\mu(\nu,\beta)h(\beta)$ where β has only the two blocks $\{n\}$ and $\{j\}$, for some $j \neq n$. Such a term contributes $(-1)^{2-1} t(\beta)n^{n-2} = -n^{n-2}$ to the outer sum. Note however that the set S can be selected in $n-1$ ways since $j < n$.

Case 3 : $|S| > 2$. Here,

$$\sum_{\substack{U(\beta) = S \\ \nu \leq \beta}} \mu(\nu,\beta)h(\beta) =$$

$$\sum_{\substack{U(\beta) = S \\ \nu \leq \beta}} (-1)^{|\beta| - 1} t(\beta)n^{n - |S|} =$$

$$n^{n-|S|}\left\{\sum_{|\beta|\ \text{odd}} t(\beta) - \sum_{|\beta|\ \text{even}} t(\beta)\right\} .$$

The bracketed factor vanishes, since exactly half of the permutations of $S\backslash\{n\}$ have an even number of cycles.

We are now ready to perform the outer sum :

$$|\mathrm{Tree}(n)| = n^{n-1} - (n-1)n^{n-2} + 0 = n^{n-2} . \qquad \square$$

REFERENCES

[1] Moon, J. Various proofs of Cayley's Formula for counting trees. Chapter 11 in A Seminar on Graph Theory, F. Harary, ed.

[2] Rota, G.-C. On the foundations of combinatorial theory I : Theory of Möbius finctions. Z. Wahrscheinlichkeitstheorie und Verw. Gebiete 2 (1964) 340 - 368.

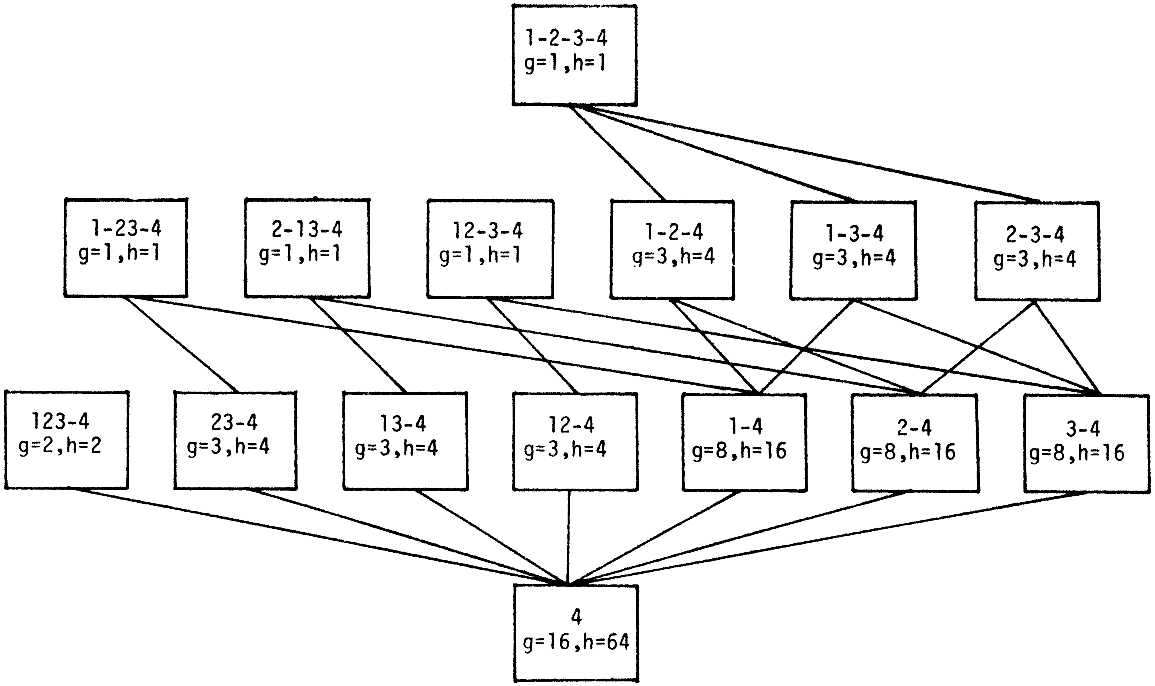


Figure 1

Hasse Diagram of $[\nu,\infty)$ for P_4

CENTRO INTERNAZIONALE MATEMATICO ESTIVO

(C.I.M.E.)

ENGINEERING APPLICATIONS OF MATROIDS - A SURVEY

ANDRAS RECSKI

ENGINEERING APPLICATIONS OF MATROIDS - A SURVEY

ANDRÁS RECSKI
RESEARCH INSTITUTE FOR TELECOMMUNICATION, 1026 BUDAPEST, HUNGARY

INTRODUCTION

The aim of the present contribution is twofold. First, we sketch some engineering problems where matroids can be applied to obtain nontrivial results. Next, one application in electric network theory is described in some details. Effort was made to give a more or less complete list of references. The paper is intended for mathematicians — no previous knowledge in engineering is required.

I. VARIOUS PROBLEMS

1. For the problem of rigid bodies we refer to [3,4,7,12,13, 36,40,42,58,65,66]. See also [64] in the present volume. For example, if the planar systems of rigid braces, like on Fig. 1,

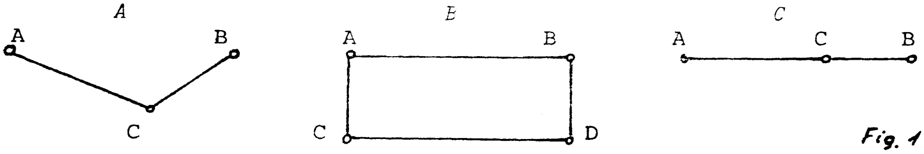


Fig. 1

are considered and fixed to the plane at points A and B then system *A* is rigid while system *B* is not rigid (the points C and D can simultaneously move around A and B respectively) and a further "pin" at C or D or a further brace between, say, A and D is required. System *C* is rigid with respect to mechanical motions but not to "infinitesimal" ones, attacking vertically at point C. Hence a further "pin" is required at C. All what we wish to emphasize here is that there are essentially two types of questions considered:

Question 1A Is the given system rigid?

Question 1B If not, determine the minimal number of extra braces or pins to make the given system rigid (and give such a system).

Some of the quoted sources treat more general problems. Not only "pinned braces" but "slides", "rotors" etc. are considered, and in higher dimensions as well.

2. Strongly related is the activity of [60,61] concerning the man-machine communication via a graphical display. If the designer draws the 2-dimensional image of a 3-dimensional body, the computer must "recognize" the original body. If the recognition of vertices, edges and faces (and the incidence relations among them) is solved, still uncertainities, caused by "wrong" or "misunderstandable" drawings can arise. For example, if the second drawing of Fig. 2 is the input, the computer should probably "ask" the user whether the "nonexistence of the point P" was intentional. Again, two types of questions can be quite natural:

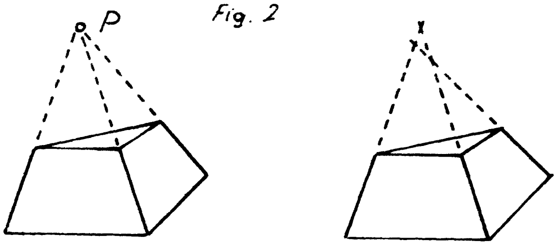


Fig. 2

Question 2A Is the given input understandable for the computer?

Question 2B If not, determine the minimal number of further questions to be answered (and give such a system of questions).

3. Consider the fundamental problem of network analysis. Details will be given in Chapter III, so only the questions are formulated now:

Question 3A Is the given network uniquely solvable?

Question 3B If yes, determine the "degree of freedom" or "complexity" of the network (and give a system of as many independent state variables).

II. VARIOUS REMARKS

1. The list of problems in Chapter I is by no means complete. We are not considering here the applications of matroids in information theory [21-24,32] or in control theory [31]. Matroidal concepts and results are also widely applied to operations research, linear programming etc., see e.g. [6,19,37]. Even such seemingly esoteric fields as behaviourial linguistics have already applied nontrivial matroidal tools [59,62].

2. Questions iA above, for i=1,2,3, can be answered by "yes" or "no" while Questions iB by a non-negative number and a subset of a suitable set. The common feature of all these problems is that *qualitative* questions are posed, so discrete mathematical tools are hopefully applicable. Questions iA will turn out to be, in a sense, special cases of the corresponding Questions iB. This will be made somewhat more precise in Chapter IX.

3. At the first glance all these questions (at least those of form iA) seem to be routine tasks of linear algebra. In practical applications this is not the case, for the following reason. A necessary and sufficient condition to these problems in terms of linear algebra would be the nonsingularity of a usually large matrix with real entries. Checking this nonsingularity by numerical methods can lead to qualitatively wrong answers, due, for example, to roundoff errors in arithmetical operations among real numbers (which are represented by decimals of a finite length in a computer). We shall return to this and related questions in Chapter VII.

4. Speaking quite generally, if an arbitrary phenomenon should be described by a possibly simple mathematical model then

finiteness and linearity of the model are perhaps the most frequent assumptions in many fields of science and technology. Hence tools of discrete mathematics and linear algebra are widely applied. Matroid theory, being a branch of combinatorics, still containing linear algebra as a special case, can therefore serve as a unifying tool. (If a reader find this remark somewhat too general and of little practical value, he/she is requested to return to this point after having finished Chapter V. Both matroids *G* and *A* contained many important information, reflecting properties by graphs and by matrices respectively. However, only their union *G*∨*A* gave the answer to Question 3A.)

III. Formulation of the network analysis problem

A network is an interconnection of devices. The devices are given by their physical properties, in form of linear equations among voltages and currents, see Remark 3 below, while the interconnection is described by a graph.

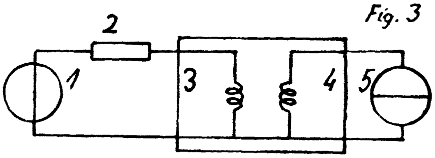
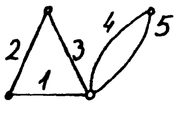


Fig. 3

Example 1. Consider the network of Fig. 3. The devices are as follows: A *voltage source(1)* is defined by $u_1=u(t)$, i.e. a given function of time, while its current i_1 is arbitrary; a *current source(5)* is defined by $i_5=i(t)$ while its voltage u_5 is arbitrary; a *resistor(2)* is defined by $u_2=Ri_2$ and an *ideal transformer(3,4)* by $u_3=ku_4$ and $i_4=-ki_3$. The interconnection of these devices is represented by the *network graph* of Fig. 4, where edges correspond either to 2-terminal devices (sources and resistors) or to individual ports of the multiports (see below); and two edges are incident to the same vertex if the devices or ports are joined to the same node.



The problem (cf. Remark 3 below) of network analysis is: determine all the voltages and currents of every device (as unique functions of the voltages of the voltage sources and currents of the current sources). For example, in the above network $i_2=k^{-1}i_5$ or $u_3=u_1-rk^{-1}i_5$ etc.

As a common generalization of the concepts of resistors (one linear equation relating a voltage and a current) and that of the ideal transformer (two linear equations relating two voltages and two currents) let us define[5] the concept of n-*port* as a system of n linear, homogeneous algebraic equations relating n voltages and n currents. Each port of such an abstract device has one voltage and one current; and every such port is represented by an edge of the network graph. The expression *multiport* will also be used, if the number of ports need not be emphasized.

Remark 1. The class of networks defined above is usually called linear, memoryless and time-invariant. The second condition will be dropped in Chapter IX, see also the next remark. The first (meaning that the multiport equations are linear) and the third (meaning that the structure of the network graph does not change - e.g. by switches) are essential in what follows. However, the concept of multiports is so general that even this class of networks contains a great variety of practically important ones.

Remark 2. Linear devices "with memory", like capacitors and inductors, are excluded in Chapters III-VIII. Hence, if the answer to Question 3A is positive, the system of network equations is algebraic and Question 3B does not arise before Chapter IX.

Remark 3. Some devices may be defined in a more convenient way in terms of other physical quantities, e.g. as in Example 5 in Chapter X below, rather than by voltages and currents. Hence the definition of a multiport and the problem of network analysis can be formulated in a more general way.

The voltages and currents in the network must satisfy not only the defining equations of the devices but also the Kirchhoff Voltage Laws and Current Laws (KVL and KCL respectively), posed by the structure of the interconnection. KVL states that the sum of the voltages along any circuit of the network graph must be zero. KCL states that the sum of the currents along any cut set (i.e. minimal set of edges whose removal disconnects the graph) must be zero. E.g. $u_1+u_3+u_4=0$ and $i_2+i_5=0$ are examples for KVL and KCL respectively, in the network of Example 1. (The question of reference directions is of no particular importance and will be neglected here.)

Hence Question 3A sounds like that: Is the system of equations for the voltages and currents of the network (obtained from the device equations, from KVL's and KCL's) uniquely solvable?

IV. The classical result

If the network graph contains a circuit so that every edge of the circuit corresponds to a voltage source then the currents of these edges cannot be uniquely determined. Similarly, a cut set formed by current sources leads to uncertainity of voltages. Hence *the subgraph* G_u *of the network graph, formed by the edges of the voltage sources, must not contain any circuit, and*

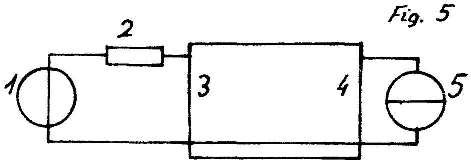
(C1) *the subgraph* G_i*, formed by the current sources, must not contain any cut set (i.e. the complement of* G_i *must be connected).*

This *necessary* condition can be proved to be *sufficient* if the network contains voltage and current sources and resistors ($u=Ri$, $R>0$) only. The proof of the sufficiency (essentially [33], see also [44,8] and some recent textbooks on circuit theory, like [57]) is by no means trivial.

If the network contains arbitrary multiports, too, then (C1) is not sufficient any more.

Example 2. If the equations of the 2-port on Fig. 5 are $u_3=ku_4$, $i_4=0$ then the network will have no unique solution. (No solution at all, if $i_5\neq 0$ while infinitely many if $i_5=0$ since then u_4 and u_5 may be arbitrary.)

Fig. 5



However, observe that the network *graph* of Example 2 is the same as that of Example 1. Hence we can also conclude that *a necessary and sufficient condition of unique solvability, in terms of the network graph only, cannot be given at all.*

V. A stronger necessary condition

Let the network graph contain k edges and let u_ν and i_ν denote the voltage and current of the νth edge, respectively. If we formally generate all the network equations, the system to be solved is $Nx=0$ where $x=(u_1,u_2,\dots,u_k,i_1,i_2,\dots,i_k)^*$. N can be decomposed like $\begin{bmatrix} B & | & 0 \\ 0 & | & Q \\ & A & \end{bmatrix}$, where A is the collection of the matrices of the multiport-equations, 0 denote the zero matrices and B and Q are the edge-circuit and the edge-cutset matrices, respectively.

The edges 1,2,...,k can be labelled in such a way that 1,2, ...,α correspond to the voltage sources and $\beta,\beta+1,\dots,k$ correspond to the current sources (see the remark below). Let $u_0=(u_1,u_2,\dots,u_\alpha)^*$ and $i_0=(i_\beta,i_{\beta+1},\dots,i_k)^*$. Then $Nx=0$ can also be written as $[N'|N_0|N'']\begin{bmatrix} u_0 \\ x_0 \\ i_0 \end{bmatrix}=0$. Hence the network is uniquely solvable if and only if N_0 is nonsingular, or if and only if det $N_0\neq 0$, and then, of course, $x_0=-N_0^{-1}(N'u_0+N''i_0)$.

Generally speaking, if M is a square matrix of the form $\begin{bmatrix} M_1 \\ M_2 \end{bmatrix}$ then, by the Laplace expansion, det M arises in form $\Sigma \pm$det P_1 det P_2 where P_1 is formed by the rows of M_1 and by some columns of M, P_2 is formed by the rows of M_2 and by the rest of the columns of M, and the summation is performed over every choice of the columns. Hence a necessary condition of det $M\neq 0$ is that there must exist at least one decomposition of the column set of M so that both det P_1 and det P_2, belonging to this decomposition, should be nonzero.

Let the column space matroids of the matrices A,B etc be denoted by the corresponding script letters $\mathcal{A},\mathcal{B}$ etc respectively. Then det $M\neq 0$ means that the full column set T of M is independent in $\mathcal{M}$ and, by the above reasoning, this implies that there exists a decomposition $T=T_1\cup T_2$ so that T_i is independent in $\mathcal{M}_i$. But it exactly means that T is independent in $\mathcal{M}_1 \vee \mathcal{M}_2$ where v denotes matroid union.

Let $S=\{u_1,u_2,\dots,u_k,i_1,i_2,\dots,i_k\}$denote the full column set of N, let furthermore $U=\{u_1,u_2,\dots,u_\alpha\}$ and $I=\{i_\beta,i_{\beta+1},\dots,i_k\}$ denote those of N' and N'' respectively (see the remark below).

<u>Remark:</u> Certainly $\alpha<\beta$. We allow the cases $\alpha=0$ or $\beta=k+1$ which means $U=\emptyset$ or $I=\emptyset$ respectively. Then the above decomposition of N is simpler. Even the case $U=I=\emptyset$ causes no problem, only the system of equations to be solved becomes homogeneous. In fact many authors start investigations by "contracting the edges which cor-

respond to voltage sources and deleting the edges which correspond to current sources" if only solvability is concerned. This makes everything simpler since solvability does not change if the corresponding homogeneous system is considered only.

If we denote the matrix $\begin{bmatrix} B & 0 \\ 0 & Q \end{bmatrix}$ by G, we could finally formulate the following necessary condition for unique solvability:

(C2) S-(UUI) *is a base in* GvA .

Before presenting some examples we recollect that if $K=\begin{bmatrix} K_1 & 0 \\ 0 & K_2 \end{bmatrix}$ then $K=K_1+K_2$ where + denotes direct sum. (Here the matrices need not be squares.) Also recollect that if B and Q are the circuit and the cut set matrices of a graph H respectively then $B=M^*(H)$ and $Q=M(H)$ where $M(H)$ denotes the cycle matroid of H.

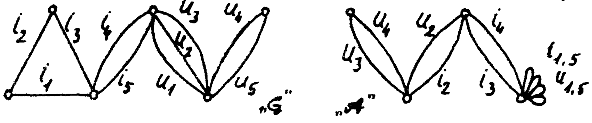


Fig. 6

In order to visualize the above concepts, let us return to Example 1. Both matroids G and A happen to be graphic - they are illustrated as the cycle matroids of the graphs on Fig. 6. The drawing for G is obvious by the above remarks, while to check the drawing for A let us explicitly describe the matrix A:

$$\begin{array}{cccccccccc} u_1 & u_2 & u_3 & u_4 & u_5 & i_1 & i_2 & i_3 & i_4 & i_5 \\ \hline 0 & -1 & 0 & 0 & 0 & 0 & R & 0 & 0 & 0 \\ 0 & 0 & -1 & k & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & k & 1 & 0 \end{array}$$

The matroid GvA also happens to be graphic in this example and can be illustrated as the cycle matroid of the graph of Fig. 7. The set S-$\{u_1,i_5\}$ is clearly a base of this matroid, hence (C2) is met.

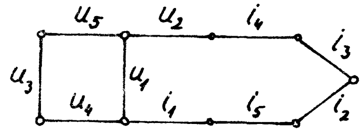


Fig. 7

On the other hand, the matroid A of the second example can be drawn as the cycle matroid of the graph of Fig. 8 and then the result GvA will be illustrated by the graph of Fig. 9. The set S-$\{u_1,i_5\}$ will not be a base now, hence (C2) is violated.

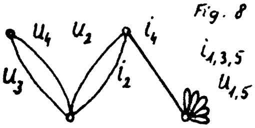


Fig. 8

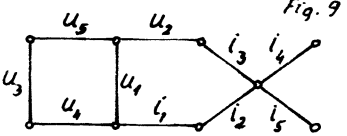


Fig. 9

VI. How can one check conditions (C1) and (C2) ?

Checking condition (C1) in a graph is certainly an easy task. The reader is suggested to prepare an algorithm or is referred to [25, pp.41-42]. On the other hand, (C2) poses some questions.

A large number of algorithms have been published in the last 12 years to decide whether a given set is a base in the union of the matroids $M_1, M_2, \dots, M_n$, see e.g. [2,15,17,18,20,34,35,37,38]. These have polynomial complexity provided we have an "independence oracle" for each M_ν (see [64] in this volume). Roughly speaking, we can obtain an algorithm, polynomial in the size m of the common underlying set S of the M_ν's and in their number n, if the information "whether the given subset of S is independent in M_ν or not" can be obtained in a time polynomial in m.

An independence test in G is essentially as easy as checking (C1). For testing independence in A observe that A always arises as a direct sum, with the summands corresponding to the individual devices. Hence a subset of S is independent in A if and only if, for every μ, the intersection of this subset with the set of voltages and currents of a multiport device N_μ is independent in the summand A_μ.

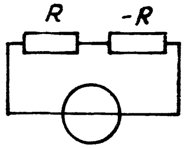
Still, we have to check whether a subset is independent in A_μ, which is given as the column set matroid of a matrix with real entries. However, the difficulty described in Remark 3 of Chapter II does not exist any more, for the following reason.

In the practical realizations of a computer program for network analysis the user has to specify only the devices to be interconnected - and, of course, the way of the interconnection. The models of the devices are stored in the data bank of the computer, as subnetworks, matrices etc. Once a new device becomes available at the market, its model should be prepared and filled into the data bank. At this stage the corresponding matroid A_μ can also be prepared and stored in a suitable way. Even if this task is "difficult" (requires long time or high precision in numerical calculations), this should be done only once, when establishing the model to be stored in the data bank. Then this information is stored for ever and each time when the device is required in an actual analysis (which can be the case many times), we use only the result of these "difficult" calculations.

VII. Is (C2) sufficient?

The proof of the necessity of Condition (C2) clearly indicates that it cannot be sufficient in the mathematical sense. It only implies that we have a nonzero term in the Laplace expansion but it can easily be cancelled out by other nonzero terms, leading to det M= 0.

Example 3. Consider the trivial example on Fig. 10 where the sum of the two resistances is zero. The network is clearly singular but (C2) is met.



However, one can argue that situations like that of Example 3 are artificial and can be disregarded. After all, one can never buy such two resistors R_1 and R_2 in the shop that the *a priori* given relation $R_1+R_2=0$ is exactly met, since the physical parameters of the devices are subject to technological constraints etc.

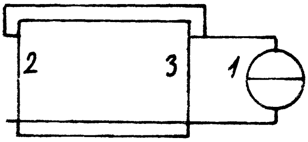
Putting it slightly more exact, if we suppose that the numerical values of the device parameters are, say, algebraically independent transcendentals over the field from which the entries of B and Q are chosen, then (C2) turns out to be sufficient, too.

This additional assumption is usually called "generality" [30] and also arises in some form in many other mathematical and engineering considerations, see e.g. [16,42]. However, there are nontrivial problems of its correct definition. The interested reader is referred to [55].

Although we are not going into details of the rigidity problems, let us return now to Fig. 1 for a moment. The reason of the differences between A and C is that the distance between the pins A and B is equal to the sum of the distances of the braces AC and BC in case of system C. Roughly speaking, if such "algebraic relations" are forbidden, then the rigidity problems become purely combinatorial, e.g. the answers to Questions 1A, 1B will depend on the "graph" of the braces only, and the only "infinitesimal" motions of the system will be the velocities of the mechanical ones [3].

VIII. Should we always accept "generality" ?

The above argument (about the technological uncertainities) is acceptable only as long as *a priori* given relations among parameters of *different* devices are concerned. But if such relations are given among different parameters of the *same* device, one should be more careful. E.g. the two k's in the defining equations of an ideal transformer (see Example 1) are equal, and this equality is not a coincidence but it reflects the physical feature of the device. Such "internal relations" might cause difficulties, as shown by the following example:



Example 4. Let the 2-port of the network of Fig. 11 (the *gyrator*) be defined by $u_2=Ri_3$, $u_3=-Ri_2$. It is not difficult to verify that the network is singular but (C2) is met.

This phenomenon as well as some other similar ones have been well known by network theorists since long time. [1,45-49,57] are typical examples for avoiding such difficulties by describing that the independent subsets from G and A (to meet (C2)) must satisfy certain additional conditions. E.g. if $\{x,y\}$ is the edge set of a 2-port N then only those trees T of the network graph are accepted for which $|\{x,y\}\cap T|=1$ if N is an ideal transformer and $|\{x,y\}\cap T|\neq 1$ if N is a gyrator.

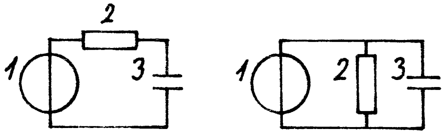
This approach was in a sense generalized for arbitrary 2-ports in [53] where we proved that, among the theoretically possible *infinite* variety of algebraic relations among the 2-port parameters, only *five* relations can really cause such problems. The essence of this result is that these 5 critical relations are independent of the way how the 2-port is embedded into the network, hence they can be checked in stage of establishing the model of the 2-port for the data bank (c.f. the end of Chapter VI).

The above examples indicate that the additional conditions to be checked are at least as hard as the matroid 2-parity problem for represented matroids. Anyhow, this is still a polynomial problem[39-41]. The reader is also referred to [64] in this volume but should observe that generalizing the above questions to k-ports (k>2) will generalize the matroid 2-parity problem in a different way. For this latter we refer to [56] and mention only one interesting question: Let $S_1, S_2, \ldots, S_t$ be disjoint k-element subsets of S and let M be a represented matroid over S. Decide whether there exists a subset X with cardinality at least q so that $|S_i \cap X| \neq 1$ for every $i=1,2,\ldots,t$ (observe that this reduces to the 2-parity problem for k=2), and X is independent in M.

IX. Some remarks on Question 3B

Only memoryless n-ports were considered till now. However, essentially the same approach works in case of devices "with memory" as well. This concept means that the device can store energy. For example, the *capacitor* or the *inductor* with the defining equations $i=C\frac{du}{dt}$ and $u=L\frac{di}{dt}$ respectively, can store (electric resp. magnetic) energy. In fact we may suppose without loss of generality that only these two kinds of new devices are introduced (i.e. a linear n-port with memory can always be substituted by a subnetwork, containing, for a suitable k, a linear memoryless (n+k)-port and k capacitors and inductors.)

The order σ of the system of differential equations to be solved is clearly bounded from above by the number n_C of capacitors plus the number n_L of inductors. However, the case $\sigma<n_C+n_L$ is also possible. For example, the current i_3 of the capacitor in the first network on Fig. 12 is given by the differential equation $RC\frac{d}{dt}i_3 + i_3 = C\frac{d}{dt}u_1$, subject to an initial condition $u_3(t_0)=u_0$, while in the second network one simply obtains $i_3= C\frac{d}{dt}u_1$, without solving any differential equations.



Suppose for a moment that the network contains voltage and current sources, capacitors, inductors and positive resistors only. Then (C1) is still necessary *and sufficient* for the unique solvability, as it can be proved by a rather tedious way, see e.g. [57]. Observe that (C1) is equivalent to the following: there exists a tree T in the network graph, containing all the voltage source edges and none of the current source edges.

Among all the trees, satisfying the above two conditions, find the one which contains the maximal number k_C of capacitors and the one which contains the minimal number k_L of inductors. (It is not difficult to prove that both values k_C and k_L can be reached by the same tree as well.) Then $\sigma=k_C+k_L$.

Observe that to determine k_C and k_L (for answering Question 3B) we need Kruskal's algorithm with gradually decreasing weights for voltage sources, capacitors, resistors, inductors and current sources, while to check (C1) itself, for answering Question 3A only, we need simple independence tests only.

We refer to [30,50-52] for determining σ in networks containing voltage and current sources, capacitors, inductors and linear memoryless n-ports, but wish to emphasize that the algorithms require weighted matroid partition algorithms, unlike in case of memoryless networks, where cardinality matroid partition algorithms could already do.

Generally speaking, Questions iB seem to require weighted versions of those algorithms which were used to answer Questions iA (for i=1,2,3).

X. APPLICATIONS TO NETWORK SYNTHESIS

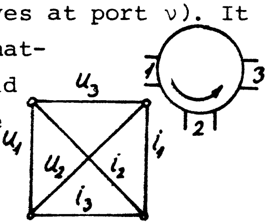
Until now we considered the problem of network analysis, i.e. given the network, determine its properties. In this last chapter we give some remarks on the inverse problem (the real engineering problem: given some specifications, design a network which meets them).

Whether such a problem is solvable depends on the set of devices we are allowed to use as building blocks for our realization process. Negative results like "a particular specification cannot be realized from a given set of building blocks" are usually considered as parts of "realizability theory" while "synthesis" in the narrow sense means rather realization processes, canonical configurations etc. Here we intend to show how matroids can help to obtain new realizability criteria. For more detailed results the reader is referred to [28,54].

Suppose we wish to interconnect the multiports $N_1,N_2,\ldots,N_k$ to form a new multiport N_0. Their matroids $A_1,A_2,\ldots,A_k$ and A_0, respectively, are defined in the same way as in Chapter V - simply the column set matroids of their describing matrices. The way how they are interconnected is described by the network graph H again —edges correspond to ports— and $G=M^{*}(H)+M(H)$, as before.

If the edge set E of the graph H is of the form $E_0 \cup (E-E_0)$ where E_0 is the set of ports of N_0 then [54] A_0 can be obtained from $A_1, A_2, \ldots, A_k$ and G by forming $G \vee (A_1+A_2+\ldots+A_k)$ and then contracting the elements, corresponding to voltages or currents of $E-E_0$.

Example 5. Consider the 3-port *circulator* defined by $x_1=y_2$, $x_2=y_3$ and $x_3=y_1$, where $x_\nu=u_\nu+i_\nu$ and $y_\nu=u_\nu-i_\nu$ (the physical meaning of x_ν and y_ν are incident and reflected waves at port ν). It is not difficult to verify[28,52,54] that the matroid of the circulator is just the cycle matroid of the graph on Fig, 13. If we interconnect the circulator with a resistor in the way shown on Fig. 14a, the network graph will look like Fig. 14b, and a not quite obvious calculation shows that the matroid of the resulting 2-port will be the cycle matroid of the graph of Fig. 14c.



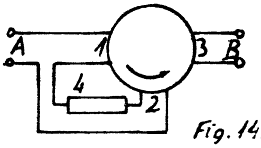
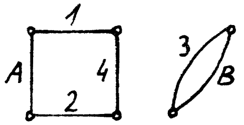


Fig. 14a



14b

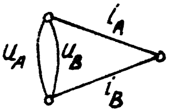


Fig 14c

Of course, a condition, like "generality" in Chapter VII, is required again: we usually call it *qualitative reliability (QR)* in this context[54]. Roughly speaking it means that the realization of a multiport N_0 from the N_ν's is QR if and only if small quantitative changes in the N_ν's cannot lead to a qualitative change of N_0, hence, after the interconnection of the N_ν's, no "mutual tuning" of these components is required any more for meeting the qualitative specifications of N_0. (Somewhat similar ideas have already been presented in [9-11], too.)

The following theorem will be a typical example to show how this approach can be applied:

Theorem: The 3-port circulator cannot be QR-synthesized from 1- and 2-ports, using series-parallel topology (i.e. if the network graph is series-parallel[14]).

Sketch of the proof: It requires a straightforward verification that the matroids of all the 1- and 2-ports are *gammoids*[43]. The matroid G is a gammoid iff the network graph is series-parallel. Finally, the gammoid property is preserved by direct sum, union and contraction, but the matroid of the circulator is not a gammoid, hence the assertion follows.

In addition to the more or less well known matroidal classes (like gammoids, base orderable matroids, representable matroids), which are closed with respect to union and contraction, one can construct new matroidal classes, too, which also lead to new realizability criteria. Some of them have interesting meaning in network theory as well. See [28,54] for further details.

ACKNOWLEDGEMENTS:

The author's contributions to these topics could not be obtained without the highly stimulating discussions in the last ten years with many friends and colleagues, most notably with Á. Csurgay, A. Frank, M. Iri, L. Lovász, T. Roska and V. T. Sós.

REFERENCES

Items [1]-[66] were explicitly mentioned in the present paper. The further 76 items are other papers, related to the applications of matroids to network theory. Special thanks are due to Mr. Masataka Nakamura, University of Tokyo, who has compiled most of them. Further papers, related to the rigidity problems, can be found among the references of [58,65,66]. A substantial part of the research of Japanese scholars is devoted to a structural theory of systems, which may be formulated in matroidal terms and solved by a technique usually called "principal partition". See [26] for a review of these activities.

1. K.Abdullah, A necessary condition for complete solvability of RLCT networks, *IEEE Trans. Circ. Theory,* CT-19 /1972/ 492-3.
2. M.Aigner-T.A.Dowling, Matching theory for combinatorial geometries, *Trans. Amer. Math. Soc.* 158 /1971/ 231-245.
3. L.Asimow-B.Roth, The rigidity of graphs, *Trans. Amer. Math. Soc.* 245 /1978/ 279-289.
4. L.Asimow-B.Roth, The rigidity of graphs II, *J. Math. Anal. & Appl.* 68 /1979/ 171-190.
5. V. Belevitch, *Classical network theory,*Holden-Day, San Francisco, 1968.

6. R.G.Bland, A combinatorial abstraction of linear programming, *J. Combinatorial Theory Ser. B.*23 /1977/ 33-57.

7. E. Bolker-H.Crapo, How to brace a one-story building? *Environment and Planning,* B 4 /1977/ 125-152.

8. P.R.Bryant, The order of complexity of electrical networks, *Proc. IEE (GB)* 106 /1959/ 174-188.

9. H.J.Carlin, General n-port synthesis with negative resistors, *Proc. IRE* 48 /1960/ 1174-75.

10.H.J.Carlin, Singular network elements, *IEEE Trans. Circ. Theory* CT-11 /1964/ 67-72.

11. H.J.Carlin-D.C.Youla, Network synthesis with negative resistors, *Proc. IRE* 49 /1961/ 907-920.

12. H.Crapo, Structural rigidity, *Structural topology* 1 /1979/ 26-45.

13. H.Crapo, More on the bracing of one story buildings, *Environment and Planning,* B

14. R.J.Duffin, Topology of series-parallel networks, *J. Math. Anal. & Appl.* 10 /1965/ 303-318.

15. J.Edmonds, Minimum partition of a matroid into independent sets, *J. Res. Nat. Bureau Stand.*69B /1965/ 67-72.

16. J.Edmonds, Systems of distinct representatives and linear algebra, *J. Res. Nat. Bureau Stand.* 71B /1967/ 241-245.

17. J.Edmonds, Matroid partition, in: Math of the Decision Sciences, Part I. *Lectures in Appl. Math.* 11 /1968/ 335-345.

18. J.Edmonds, Submodular functions, matroids and certain polyhedra, *Combin. Structures and Their Appl.* Gordon and Breach, New York etc. 1970. pp. 69-87.

19. J.Edmonds, Matroids and the greedy algorithm, *Math. Programming* 1 /1971/ 127-136.

20. J.Edmonds, Matroid intersection, *Annals of Discrete Math.*4 /1979/ 39-49.

21. S.Fujishige, Polymatroidal dependence structure of a set of random variables, *Information and Control,* 39 /1978/ 55-72.

22. T.-S.Han, The capacity region of general multi-access channel with certain correlated sources, *Information and Control,* 39.

23. T.-S.Han, Deterministic broadcast channels with a common message, Research Memorandum RMI 79-4, University of Tokyo, 1979.

24. T.-S.Han, Slepian-Wolf-Cover theorem for networks of channels

25. M.Iri, *Network flow, transportation and scheduling: Theory and algorithms,* Academic Press, New York etc. 1969.

26. M.Iri, A review of recent work in Japan in principal partitions of matroids and their applications, *Annals New York Acad. Sci.* 319 /1979/ 306-319.

27. M.Iri, Survey of recent trends in applications of matroids, *Proc. IEEE Intern. Symp. Circuits and Systems,*Tokyo,1979,987.

28. M.Iri-A.Recski, Reflections on the concepts of dual, inverse and adjoint networks, Parts I-II, Technical Research Reports of the IECEJ, September 1979 and January 1980 respectively.

29. M.Iri-A.Recski, What does duality really mean? *Circuit Theory and Appl.*8 /1980/ 317-324.

30. M.Iri-N.Tomizawa, A unifying approach to fundamental problems in network theory by means of matroids, *Trans. IECEJ* 58-A /1975/ 33-40.

31. M.Iri-N.Tomizawa-S.Fujishige, On the controlability and observability of a linear system with combinatorial constraints *Trans.Soc. Instrument & Control Engs.* 13 /1977/ 225-242.

32. P.M.Jensen, Matroids and error-correcting codes, thesis, Dan-

marks Tekniske Høјskole, Lyngby, 1977.

33. G.Kirchhoff,Über die Auflösung der Gleichungen, auf welche man bei der Untersuchungen der linearen Verteilung galvanischer Ströme geführt wird, *Poggendorff Ann. Phys.* 72 /1847/ 497-508.

34. D.E.Knuth, Matroid partitioning, Report Stan-CS-73-342, Stanford University,1973.

35. S.Krogdahl, A combinatorial base for some optimal matroid intersection algorithms, Report Stan-CS-74-468, Stanford Univ.

36. G.Laman, On graphs and rigidity of plane skeletal structures, *J. Engineering Math,* 4 /1970/ 331-340.

37. E.L.Lawler, Matroid intersection algorithms, *Math. Programming* 9 /1975/ 31-56.

38. E.L.Lawler, *Combinatorial optimization: Networks and matroids* Holt, Rinehart and Winston, New York, 1976.

39. L.Lovász, The matroid matching problem, *Coll. Math. Soc. János Bolyai, Algebraic methods in graph theory, Szeged, 1978.*

40 L.Lovász, Matroid matching and some applications, *J. Combinatorial Theory Ser. B,* 28./1980/ 208-236.

41. L.Lovász, Selecting independent lines from a family of lines in a space, *Acta Sci. Math. Szeged* 42 /1980/ 121-131.

42. L.Lovász-Y.Yemini, On generic rigidity in the plane

43. J.H.Mason, On a class of matroids arising from paths in graphs, *Proc. London Math. Soc.(3)* 25 /1972/ 55-74.

44.J.C.Maxwell, *Electricity and magnetism* Clarendon Press, Oxford, 1892.

45. M.M.Milić, The state-variable characterization of a class of linear time-varying nonreciprocal networks, *Proc. Intern.Symp. Network Theory,* Belgrade, 1968. pp. 31-40.

46. M.M.Milić, Explicit formulation of the state equations for a class of degenerate linear networks, *Proc. IEE (GB)* 118 /1971/ 742-745.

47. M.M.Milić, Some topologico-dynamical properties of linear passive reciprocal networks, *Circuit Theory & Appl.* 5 /1977/ 417.

48. T.Nitta-A.Kishima, Solvability and state equations of RCG networks, *Trans. IECEJ* E-60 /1977/ 410.

49. T.Nitta-A.Kara-T.Okada, An algorithm of a proper tree in an RCG network, *Trans. IECEJ* E-62 /1979/ 492.

50. B.Petersen, Investigating solvability and complexity of linear active networks by means of matroids, *IEEE Trans. Circuits & Systems,* CAS-26 /1979/ 330-342.

51. A.Recski, Contributions to the n-port interconnection problem by means of matroids, *Coll. Math. Soc. János Bolyai,18.Combinatorics, Keszthely, 1976.* North-Holland, Amsterdam, 877-892.

52. A.Recski, Unique solvability and order of complexity of linear networks containing memoryless n-ports, *Circuit Theory & Appl.* 7 /1979/ 31-42.

53. A.Recski, Sufficient conditions for the unique solvability of linear networks containing memoryless 2-ports, *Circuit Theory & Appl.* 8 /1980/ 95-103.

54. A.Recski, Matroids and network synthesis, *Proc. 1980 European Conf. on Circuit Theory & Design,* Warsaw, 1980. 192-197.

55. A.Recski-M.Iri, Network theory and transversal matroids, *Discrete Applied Math.*

56. A.Recski-J.Takács, On the combinatorial sufficient conditions for linear network solvability, *Circuit Theory & Appl.*

57. R.A.Rohrer, *Circuit theory: An introduction to the state variable approach.* McGraw-Hill, New York, 1970.

58. I.G.Rosenberg, Structural rigidity I, Foundations and rigidity criteria, Université de Montréal, Preprint CRMA 908, 1979.

59. K.Sugihara, Non-metrical approach to determining the structure of concepts,Univ.of Tokyo, Preprint RMI 78-01, 1978.

60. K.Sugihara, A step toward man-machine communication by means of line drawings of polyhedra, *Bull. Electrotechn. Lab. of Japan,* 42 /1978/ 20-43.

61. K.Sugihara, Studies on mathematical structures of line drawings of polyhedra and their applications to scene analysis, Electrotechn. Lab. of Japan, Preprint No. 800, 1979.

62. K.Sugihara-M.Iri, A mathematical approach to the determination of the structure of concepts, *The Matrix & Tensor Quart.* 30 /1980/ 62-75.

63. D.J.A.Welsh, *Matroid theory,*Academic Press, London etc. 1976.

64. D.J.A.Welsh, *this volume.*

65. W.Whiteley, Introduction to structural geometry I-II,preprint.

66. R.E.Bixby, A composition for matroids, *J. Combinatorial Theory Ser. B.*18. /1975/ 59-72.

67. J.Bruno-L.Weinberg, A constructive graph-theoretic solution of the Shannon switching game, *IEEE Trans. Circuit Theory,* CT-17 /1970/ 74-81.

68. J.Bruno-L.Weinberg, Principal partition and principal minors of a matroid, with applications, *Annals New York Acad. Sci.* 175 /1970/ 49-65.

69. J.Bruno-L.Weinberg, The principal minors of a matroid, *Linear Algebra & Its Appl.* 4 /1971/ 19-59.

70. J.Bruno-L.Weinberg, Generalized networks: Networks, embedded on a matroid I-II, *Networks,* 6 /1976/ 53-94 and 231-272.

71. T.Brylawski, A combinatorial model for series-parallel networks, *Trans. Amer. Math. Soc.*154 /1971/ 1-22.

72. J.Clausen, thesis, University of Copenhagen, 1978.

73. Á.Csurgay-Z.Kovács-A.Recski, On the transient analysis of lumped-distributed nonlinear networks, Proc. 5th Internat. Coll. Microwave Commun. Budapest, 1974.

74. R.J.Duffin-T.D.Morley, Wang algebra and matroids, *IEEE Trans. Circuits & Systems,* CAS-25 /1978/ 755-762.

75. C.A.Holzmann, Realization of netoids, Proc.20th Midwest Symp. Circuits and Systems, Lubbock, Texas, 1977. pp. 394-398.

76. C.A.Holzmann, Binary netoids, Proc. IEEE Intern. Symp. Circuits and Systems, Tokyo, 1979. pp. 1000-1003.

77. M.Iri, Combinatorial canonical form of a matrix with applications to the principal partition of a graph, *Electronics & Communication in Japan,* 54 /1971/ 30-37.

78. M.Iri, The maximum-rank minimum-term-rank theorem for the pivotal transforms of a matrix, *Linear Algebra & Its Appl.*2 /1969/ 427-446.

79. M.Iri, Practical algorithms for transformations of matroids, and their applications to the problems of networks and control, Proc. 12th Intern. Meeting of TIMS, Kyoto, 1975. SI7.2

80. M.Iri, A practical algorithm for the Menger-type generalization of the independent assignement problem, *Math. Programming Study,* 8 /1978/ 88-105.

81. M.Iri-S.Fujishige, Use of matroid theory in operations research, circuits and systems theory, *Intern.J.Systems Science*

82. M.Iri-N.Tomizawa, A practical criterion for the existence of the unique solution in a linear electrical network with mutu-

al couplings, *Trans. IECEJ.* 57-A /1974/ 35-41.

83. M.Iri-N.Tomizawa, An algorithm for finding an optimal "independent assignment",*J.Oper.Res.Soc.Jap.*19 /1976/ 32-57.

84. G.Kishi-Y.Kajitani, On maximally distinct trees, Proc. 5th Annual Allerton Conf.Circuits and Systems, 1967. 635-643.

85. G.Kishi-Y.Kajitani, Maximally distinct trees in a linear graph, *Trans. IECEJ.* 51-A /1968/ 196-203.

86. G.Kishi-Y.Kajitani, Topological considerations on minimal sets of variables describing an LCR network, *IEEE Trans. Circuit Theory*, CT-20 /1973/ 335-340.

87. S.B.Maurer, A maximum-rank minimum-term-rank theorem for matroids, *Linear Algebra & Its Appl.* 10 /1975/ 129-137.

88. G.Minty, On the axiomatic foundations for the theories of directed linear graphs, electrical networks and network programming, *J.Math.& Mechanics*, 15 /1966/ 485-520.

89. M.Nakamura, thesis, University of Tokyo, 1979.

90. M.Nakamura-M.Iri, Fine structures of matroid intersections and their applications, Proc. IEEE Intern Symp. Circuits and Systems, Tokyo, 1979. pp. 996-999.

91. M.Nakamura-M.Iri, On the structure of directed spanning trees: An application of principal partition, Technical Research Rept. of the IECEJ, 1979.

92. M.Nakamura-M.Iri, A structural theory for matroid and polymatroid intersection,

93. H.Narayanan, thesis, Indian Inst.Techn. Bombay, 1974.

94. H.Narayanan, A theorem on graphs and its application to network analysis, Proc. IEEE Intern. Symp. Circuits and Systems, Tokyo, 1979. pp. 1008-1011.

95. T.Nitta, thesis, Kyoto University, 1977.

96. T.Nitta-A.Kishima, State equation of linear networks with dependent sources, based on network topology, *Trans.IECEJ.* 60 /1977/ 1046-1053.

97. T.Ohtsuki-Y.Ishizeki-H.Watanabe, Network analysis and topological degrees of freedom, *Trans.IECEJ.* 51 /1968/ 238-245.

98. T.Ohtsuki-T.Tsuchiya-Y.Ishizeki-H.Watanabe-Y.Kajitani-G.Kishi, Topological degrees of freedom of electrical networks, Proc. 5th Annu. Allerton Conf.Circuits and Systems,1967. 643-653.

99. T.Ohtsuki-H.Watanabe, State variable analysis of RLC networks containing nonlinear coupling elements, *Trans. IEEE Circuit Theory* CT-16 /1969/ 26-38.

100. T.Ozawa, On the minimal graphs of a certain class of graphs, *IEEE Trans. Circuit Theory*, CT-18 /1971/ 387.

101. T.Ozawa, A procedure of graph partitioning for the mixed analysis of electrical networks, *Mem.Fac.Eng.Kyoto Univ.*33/1971/

102. T.Ozawa, Order of complexity of linear active networks and a common tree in the 2-graph method, *Electr.Letters* 8/1972/542.

103. T.Ozawa, On the degrees of interferences and certain trees of a multicoloured-branch graph,*Trans.IECEJ.*55/1972/ 642-643.

104. T.Ozawa, On the existence of a common tree in the 2-graph method, *Trans. IECEJ.* 56 /1973/ 371-372.

105. T.Ozawa, Common trees and partition of two-graphs, *Trans. IECEJ.* 57 /1974/ 383-390.

106. T.Ozawa, Solvability of linear electric networks, *Mem.Fac. Eng.Kyoto Univ.* 37 /1975/ 299-315.

107. T.Ozawa, Topological conditions for the solvability of active linear networks, *Circuit Th.& Appl.* 4 /1976/ 125-136.

108. T.Ozawa,Structure of 2-graphs,*Trans. IECEJ.*,9-A /1976/ 262-263.

109. T.Ozawa-Y.Kajitani, Diagnosability of linear active networks, Proc.IEEE Intern.Symp.Circuits and Systems,Tokyo,1979.866-9.

110. T.Ozawa-T.Nitta,Some considerations on the state equations of linear active networks and network topology, *Mem.Fac.Eng. Kyoto University*, 34 /1972/ 413-424.

111. Pásztor Z., thesis, University of Budapest, 1977.

112. Petersen,B., thesis, Danmarks Tekniske Hφjskole,Lyngby,1976.

113. B.Petersen, Investigating solvability and complexity of linear active networks, Proc.1978.European Conf. Circuit Th. and Design, Lausanne, 1978. pp. 508-512.

114. B.Petersen, The qualitative appearance of linear active network transfer functions by means of matroids, Proc. IEEE Intern.Symp. Circuits and Systems, Tokyo, 1979. 992-995.

115. B.Petersen, Algorithms for topological investigation of linear active networks, Proc. IEEE Intern. Symp. Circuits and Systems, New York, 1980. 354-358.

116. B.Petersen, Circuits in the union of matroids: An algorithmic approach.

117. A.Recski, On partitional matroids with applications, *Coll. Math.Soc.J.Bolyai* 10. North-Holland, 1974. II. 1169-1179.

118. A.Recski, Matroids and state variables, Proc.1976 Europ.Conf. Circuit Theory and Design,Genova, 1976. I. 44-51.

119. A.Recski, On the sum of matroids II, Proc. 5th British Combinatorial Conf, Aberdeen, 1975. 515-520.

120. A.Recski, Applications of graph theory to network analysis— a survey, *Beiträge zur Graphentheorie und deren Anwendungen* Proc.Conf. Oberhof /G.D.R./ 1977. pp. 193-200.

121. A.Recski, Matroidal structure of n-ports, *Coll.Math.Soc.J. Bolyai* 18. North-Holland, 1978. II. 893-909.

122. A.Recski, Matroids in network theory, Proc.6th Intern.Symp. on Microwave Communication, Budapest, 1978.

123. A.Recski, Sufficient conditions for the unique solvability of networks containing linear memoryless 2-ports, Proc. 1978. Europ.Conf.Circuit Theory and Design,Lausanne,1978. 93-97.

124. A.Recski, Terminal solvability and the n-port interconnection problem, Proc. IEEE Intern. Symp. Circuits and Systems, Tokyo, 1979. pp. 988-991.

125. M.Saito-T.Asano-T.Nishizeki, On the 3-terminal matroids, Techn.Research Report of the IECEJ, 1979.

126. M.Sengoku-T.Matsumoto, On maximal circuit-free and cutset-free subgraphs and hybrid trees in a linear graph, Proc.IEEE Intern Symp. Circuits and Systems, 1975. pp. 104-107.

127. S.Shinoda-H.Sakuma-T.Yasuda, Semimatroids, Proc.IEEE Intern. Symp. Circuits and Systems, 1979. Tokyo, pp. 1004-1007.

128. C.A.B.Smith, Electric currents in regular matroids, Proc.4th British Combinatorial Conference, 1973.

129. C.A.B.Smith, Patroids,*J.Combinatorial Th.Ser.B.*16 /1974/ 64.

130. J.Takács,thesis,University of Budapest, 1978.

131. N.Tomizawa, A practical criterion for the existence of a linkage pair of bases in a muoid and an algorithm for determining the maximally distant linkage pair of bases, *Trans. IECEJ*. 59-A /1976/ 280-286.

132. N.Tomizawa, Strongly irreducible matroids and principal partition of a matroid into strongly irreducible minors, *Trans. IECEJ*. 59-E /1976/ 14-15.

133. N.Tomizawa-M.Iri, An algorithm for solving the "independent assignment problem" with application to the problem of de-

termining the order of complexity of a network, *Trans.IECEJ.* 57-A /1974/ 627-629.

134. N.Tomizawa-M.Iri, An algorithm for determining the rank of a triple matrix product AXB with application to the problem of discerning the existence of the unique solution in a network, *Trans. IECEJ.* 57-A /1974/ 50-57.

135. V.Torma, thesis, University of Budapest, 1977.

136. Z.Ünver, thesis, Middle East Technical Univ.,Ankara, 1978.

137. Z.Ünver-Y.Ceyhun, On a graphical representation for matroids

138. L.Weinberg, Matroids, generalized networks and electric network synthesis, *J. Combinatorial Theory Ser. B.*23 /1977/ 106-126.

139. L.Weinberg, Duality in networks: Roses, bouquets and cut sets; Trees, forests and polygons, *Networks,* 5 /1975/ 179.

Dr. András Recski

Research Institute for Telecommunication

H-1026 Budapest,
Gábor Á. u. 65.
Hungary

CENTRO INTERNAZIONALE MATEMATICO ESTIVO

(C.I.M.E.)

MATROIDS AND COMBINATORIAL OPTIMISATION

D.J.A. WELSH

Merton College, University of Oxford

Lectures given at the Centro Internazionale Matematico Estivo, Villa Monastero, Varenna, from August 24 - September 2, 1980

Matroids and Combinatorial Optimisation

4. Lovász's Attack on the Parity Problem

   1. The parity problem
   2. 2-polymatroids
   3. The Gallai-Lovász identity
   4. A minimax theorem for linear 2-polymatroids
   5. On a polynomial algorithm for the 2-parity problem
   6. Pinning planar structures

5. Oracle Bounds on Algorithms

   1. The concept of an oracle
   2. Examples and further results
   3. The 2-parity problem is exponential

6. Seymour's Characterisation of Regular Matroids

   1. Binary and regular matroids
   2. Splitters
   3. The decomposition theorem
   4. A polynomial algorithm to decide whether a matrix is totally unimodular

7. Colouring, Flows and Blocking Problems

   1. The blocking problem
   2. Colouring graphs
   3. Flows taking values in an abelian group
   4. Tangential blocks
   5. Further problems

8. Flows in Matroids

   1. The max flow min cut theorem
   2. Multicommodity flows
   3. Multicommodity flows in matroids
   4. Summary of results

1. Computational Complexity

§1. Introduction

Although the study of the computational complexity of solvable decision problems has been to a large extent motivated by considerations of their practical computability it has also led to a re-examination of the nature and relationship of classical problems in fields as diverse as number theory, combinatorial optimisation and recursive function theory.

Indeed, one of the outstanding open problems in contemporary mathematics is the conjecture (discussed in §3 below) that the class P of languages recognisable in polynomial time by a deterministic Turing machine is not equal to the class NP of languages recognisable in polynomial time by a non-deterministic Turing machine.

In this first lecture I briefly review relevant concepts of complexity theory, in subsequent lectures I concentrate on the interplay between complexity theory and recent results about matroids.

§2. Low level complexity

Consider the problem of multiplying two $n \times n$ matrices. The standard algorithm demands n^3 multiplications and $n^3 - n^2$ additions. One of the more striking early results in complexity theory was the theorem of Strassen (1969) who proved that a pair of $n \times n$ matrices can be multiplied in $\leq c\, n^{\log 7}$ arithmetic operations, where c is some constant.

For large n, since $\log_2 7 \simeq 2.81$, this represents a considerable saving over the standard algorithm, and it naturally raised the question: by how much could the index log 7 be reduced? This question is still unresolved.

Even though arguments which reduce the upper bound in the above problem are complicated and ingenious, it is a much more difficult problem to obtain a non trivial lower bound to such a computational problem. A moment's reflection suggests that an obvious lower bound on the complexity of the above problem is $O(n^2)$ - all the data has to be examined. (Prove this!)

Similar arguments apply to combinatorial problems. Consider the problem of finding the smallest circuit in a graph on n-vertices. Such a graph would be presented to the computer as a $n \times n$ matrix and it is not difficult to show that in order to decide the size of the largest circuit we must examine each entry in the adjacency matrix, giving us a lower bound of $O(n^2)$ and that there does exist an algorithm for solving the problem which takes at most $O(n^4)$ arithmetic operations.

Loosely speaking, therefore, the problem is tractable and the only interest is in deciding the exact value of the exponent. Problems such as these, although of practical interest will not be our main concern here. (For a discussion of such problems we refer to Bollobas [78], Milner and Welsh [76], and Borodin and Munro [75].) We will be more concerned with the gap between polynomial and exponential complexity.

§3. The class NP

Let π be a computational problem, that is a collection of computational tasks each of which is called an instance of π. For example the problem of prime testing is to determine for any given number n whether it is prime and a typical instance is a specific integer.

When studying the complexity of a problem π we associate with each instance I a size $|I|$. The choice of the particular measure used to define size is not unique but generally speaking we take the size $|I|$ to be correlated to the minimum amount of memory space required to specify I. Thus the size $|n|$ of an integer n is defined as the number of digits in the binary representation of n, thus $|n| = \log_2 n$. The size of an instance corresponding to a graph G on n vertices is the number of vertices plus the number of edges, however for most problems it is standard to use n, the number of vertices to specify the size of the input.

As far as these lectures are concerned, since we are only concerned with the gap between polynomial and exponential complexity there is no loss in precision in making this our standard interpretation of size when dealing with graph problems.

Complexity theory is based on a Turing machine model of computation (with which we assume familiarity). Most modifications of such a model do not affect the complexity notions considered below, though of course some care has to be exercised, (particularly in problems involving large integers) - see Aho Hopcroft and Ullman [74] for a discussion of the relationship between complexity measures with respect to different models.

For any function t, a Turing machine M runs in time t if on each input of size n the machine halts within t(n) steps. M runs in polynomial time if M runs in time p for some polynomial p.

If Σ is the input alphabet of the Turing machine M in question and π is a decision problem i.e. a partition of Σ^* (the set of all finite sequences from Σ) into two sets L and $\Sigma^* \backslash L$ corresponding to the output

ACCEPT or NON ACCEPT, then we say L belongs to the class P is there exists a Turing machine M such that for each string $I \in \Sigma^*$, I is accepted by M if and only if $I \in L$ and moreover M runs in polynomial time. The class P is thus the class of sets whose membership is decided by some Turing machine which runs in polynomial time.

Formally, the class NP is the collection of languages which are accepted by a non-deterministic Turing machine in polynomial time. A rigorous and formal definition of a non-deterministic Turing machine and the class NP is given by Garey and Johnson [79] or Hopcroft and Ullman [79].

For our purposes it is probably more instructive to proceed as follows. A language $L \subseteq \Sigma^*$ is in the class NP if for each member $\sigma \in L$ there is an algorithm for demonstrating that $\sigma \in L$ which runs in polynomial time on a deterministic machine.

Because of this existential quantification in the notion of acceptance by a non-deterministic Turing machine (NDTM) there is no obvious reason why the complement of a set in NP should also be in NP. This is best illustrated by example.

Example. Let Σ^* be the collection of inputs corresponding to all graphs, let L be the subset of Σ^* corresponding to graphs which have Hamiltonian circuits (i.e. circuits which visit each vertex once and only once). Given a typical member of L we can demonstrate its membership of L in polynomial time by exhibiting any one of its Hamiltonian circuits.

However given a member of $\Sigma^* \backslash L$ there is no known way of demonstrating that is doesn't have a Hamiltonian circuit in polynomial time!

Accordingly we define co-NP to be the class of languages L such that $\Sigma^*\backslash L$ is in NP.

Clearly if a language $L \in P$, then $\Sigma^*\backslash L \in P$ and hence we have

$$P \subseteq NP \cap \text{co-NP}.$$

§4. NP-complete problems

A major tool in complexity classification is computational reducibility. In studying NP, the most useful notion has been deterministic polynomial reducibility. For any problems $\pi_1, \pi_2 \in \Sigma^*$ we write $\pi_1 \propto \pi_2$ and say π_1 is reducible to π_2 if there exists a Turing machine which runs in polynomial time and which, given an instance of π_1 will convert it into an instance of π_2 such that the 'answer' to an instance of π_1 is 'yes' if and only if the answer to the instance of π_2 is "yes". If L_1 is reducible to L_2 and L_2 has a polynomial time algorithm then so does L_1.

Formally there exists a polynomial transformation of a language $L_1 \subseteq \Sigma_1^*$ to a language $L_2 \subseteq \Sigma_2^*$ if there is a function $f: \Sigma_1^* \to \Sigma_2^*$ such that:

(1) There is a polynomial time Turing machine which computes f.

(2) For all $x \in \Sigma_1^*$, $x \in L_1$ if and only if $f(x) \in L_2$.

In this case we write $L_1 \propto L_2$.
A language L is called NP-complete if:
(3) $L \in NP$.

(4) For any other $L' \in NP$, $L' \propto L$.

Cook in 1971 proved what is probably the most important theory so far in complexity theory:

Theorem 1. There exist NP-complete languages.

Cook's proof was essentially constructive. He exhibited an NP-complete language derived from a decision problem in Boolean logic, which is usually referred to as SATISFIABILITY. We describe it as follows.

The SATISFIABILITY problem is the problem of propositional calculus of determining whether a given logical formula is true for at least one assignment of the values 'true' and 'false' to the variables. The associated NP-complete language is then the collection of logical formulae which are satisfiable.

By a slight (but very common) loss of precision we shall speak of a decision problem π being NP-complete if the accepting lan uage (corresponding to those instances of π for which the answer is YES) is an NP-complete language.

In other words a problem is NP-complete if it is at least as hard (algorithmically) as any other problem in the class NP.

Once one knows a single NP-complete problem π one can prove another problem π' is NP-complete by a) showing that $\pi' \in$ NP and b) showing that π is reducible to π' in polynomial time. Karp (1972) used this technique to exhibit a number of natural NP-complete problems and this process has been contiued almost 'ad nauseam' so that now the number of known NP-complete problems must be in the thousands.

§5. Some Examples

We illustrate the above concepts with some examples of well-known problems.

(1) GRAPH COLOURABILITY

INSTANCE: Graph $G = (V, E)$, integer $k > 2$.

QUESTION: Is G k-colourable in the sense that we can assign colours to V(G) from the set $\{1,\ldots,k\}$ such that two vertices which are joined by an edge have the same colour?

This is NP-complete even when $k = 3$ and the graphs are restricted to being planar. For $k = 2$ it is just the problem of recognizing when G is bipartite and clearly belongs to P.

(2) CLIQUE

INSTANCE: Graph $G=(V,E)$, positive integer k.

QUESTION: Does G contain a set V' of vertices such that $|V'| \geq k$ and each pair of vertices is joined by an edge?

For any fixed k this is in P since the exhaustive search is of complexity $O(|V|^k)$. However for general k the problem is NP-complete.

(3) LINEAR PROGRAMMING

INSTANCE: Integer valued n-vectors $(v_i : 1 \leq i \leq m)$, integers $d_1,\ldots,d_m$, $c_1,\ldots,c_n$, b

QUESTION: Is there a vector $x = (x_1,\ldots,x_n)$ of rationals such that for $1 \leq i \leq m$, $v_i.X \leq d$ and $c.x \geq b$?

In Garey-Johnson [79, (p. 288)] the exact status of this problem is stated as uncertain. It was not known to be NP-complete nor was it known to be in P. However standard linear programming duality arguments showed that it is also in co-NP and this suggested that it was unlikely to be NP-complete. The problem was settled in (1979) by L.G. Khachian who, in one of the most important thoerems of the last decade, has shown that LINEAR PROGRAMMING is in P.

(4) TOTAL UNIMODULARITY

INSTANCE: An $m \times n$ matrix A with entries from the set $\{0, 1, -1\}$.

QUESTION: Is A not totally unimodular, that is, is there a square submatrix of A whose determinant is not in the set $\{0, 1, -1\}$?

Again in Garey-Johnson [79, p. 288] the status of this problem is open. One of the most important applications of matroid theory is Seymour's theorem which settles this problem by showing its membership of P. We devote Lecture 6 to this problem.

Another problem which is open in Garey-Johnson and which has now been settled by the matroid arguments of Lovasz is the SPANNING TREE PARITY problem, see Lecture 4 below.

Of the open problems in complexity theory at the moment, one of the most intriguing is:

(5) GRAPH ISOMORPHISM

INSTANCE: Two graphs $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$.

QUESTION: Are G_1 and G_2 isomorphic?

This is a problem known to be in NP but not known to be NP-complete or to be in P or in co-NP.

§6. P-space

We close this brief introduction to the theory of P and NP by mentioning some problems which appear to be significantly harder though still solvable.

A decision problem π can be computed in polynomial space if there exists a Turing machine which decides π and which for any input x never visits more than $p(|x|)$ squares of working tape, where p is some polynomial.

It is obvious that if π is computable in polynomial time it is computable in polynomial space. Thus $P \subseteq$ P-space. It is not much more difficult to prove

$$NP \cup \text{co } NP \subseteq \text{P-space}.$$

For example consider our prototype problem of deciding whether or not a graph has a hamiltonian circuit. If we are uninterested in the time of the computation but only in its space requirements we can just exhaustively test all n! possible sequences of possible edge sets - this will be enormously time consuming but of low polynomial space complexity.

In 1973 Meyer and Stockmeyer identified a P-space complete problem which bears the same relationship to P-space as SATISFIABILITY does to the class NP. This problem is known as QUANTIFIED BOOLEAN FORMULAS (QBF) and is defined as follows:

QBF

INSTANCE: A well formed quantified Boolean formula

$$F = (Q_1\ x_1)(Q_2\ x_2)\ldots(Q_n\ x_n)E$$

where E is a Boolean expression in the variables $x_1,\ldots,x_n$ and each Q_i is either "$\exists$" or "$\forall$".

QUESTION: Is F true?

Note that SATISFIABILITY is the case where each Q_i is "$\exists$".

Since the appearance of QBF many other P-space complete problems have been discovered by the usual technique of exhibiting membership of P-space and then finding some way of showing reducibility to QBF. Many of these examples have been of the following type involving games on graphs:-

VERTEX HEX

INSTANCE: Graph G = (V, E) and two specified vertices s,t.

QUESTION: Does the player have a winning strategy in the following game on G. Players 1 and 2 alternately choose a vertex from V\{s,t}, with those chosen by player 1 being coloured "white", the other being coloured "black". Play continues until all such vertices have been coloured and player 1 wins the game iff there is a path in G from s to t which uses only white vertices.

Even and Tarjan [76] have proved that this is a problem which is complete in P-space. For other examples of P-space complete problems and an excellent accout of the theory briefly reviewed above we refer to Garey and Johnson [79].

2. Matroid Theory

§1. Definitions

First some basic notation. V(r,q) will denote the vector space of rank r (hence dimension r - 1) over the field GF(q): PG(r - 1,q) (AG(r - 1,q)) will denote the corresponding projective (affine) space. We will move freely between vector spaces and the corresponding projective space. Thus our terminology will vary from say a "subspace" to the corresponding "flat" for essentially the same set of points depending on circumstances. Much of the time we shall be working with the field of 2 elements where the difference between the geometry and corresponding vector space is minimal.

Our graph terminology is standard, G will denote throughout a graph with vertex set V and edge set E. An edge which joins a vertex to itself is called a loop, two edges which have a common pair of endpoints will be called parallel and a graph with no loops or parallel elements is called simple. The simple graph on n vertices in which each pair of vertices is joined is the complete graph K_n. A cycle of G is a set of edges $e_1,\ldots,e_t$ such that e_i and e_{i+1} are incident $1 \leq i \leq t$ and e_i is not incident with e_j, $j \neq i + 1$ or $i - 1$ except that e_t is incident with e_1. In other words a cycle is the set of edges of a simple closed path. The deletion of an edge e from a graph G gives a graph G_e' on the same vertex set. The contraction of e from G gives a graph G_e'' which is obtained from G by deleting e and then identifying its two endpoints.

If G and H are two graphs, G is said to be *contractible* to H or to have H as a *subcontraction* if we can obtain H from G by an appropriate sequence of deletions and contractions of edges. A *cutset* of G is a set of edges whose removal increases the number of connected components of G. A *cocycle* is a minimal cutset.

A *bridge* or *isthmus* is a cutset of size 1. We usually write $X \cup e$ for $X \cup \{e\}$ and $X\backslash e$ to denote $X\backslash\{e\}$. The cardinality of a set X will be denoted by $|X|$. Any other graph terminology used can be found for example in Bondy & Murty [76].

A *matroid* is a pair consisting of a finite set S and a collection $\mathcal{J}$ of subsets of S which are called *independent sets* and satisfy the following axioms:

(I1) $\phi \in \mathcal{J}$;

(I2) If X is independent and $Y \subseteq X$ then Y is independent;

(I3) If $A \subseteq S$ all maximal independent subsets of A have the same cardinality which is called the *rank* of A and is denoted by r(A).

We usually write M to denote the matroid, its *rank* is the rank of S, r(S). A set is *dependent* if it is not independent and is a *base* if it is a maximal independent subset of S.

Matroids $M_1 = (S_1, \mathcal{J}_1)$ and $M_2 = (S_2, \mathcal{J}_2)$ are *isomorphic* if there is a 1-1 map $\Psi : S_1 \to S_2$ such that X is independent in $M_1 \Leftrightarrow \Psi X$ is independent in M_2.

A subset F of S is a *flat* or a *closed set* or a *subspace* if for each element $y \in S\backslash F$, $\rho(F \cup Y) > \rho(F)$. A *hyperplane* is a maximal proper flat, that is if a matroid has rank r a hyperplane is any flat of rank

$r - 1$, a line is any flat of rank 2.

From analogy with graphs (see Example 3 below) we call an element x of S a loop of M on S if $r(\{x\}) = 0$ and a set C is a circuit if it is minimal dependent. Two elements are parallel if their union is a circuit.

The flats of a matroid, ordered by inclusion, forma geometric lattice. Every geometric lattice can be obtained from a matroid in this way and there is a natural one-one correspondence between matroids and geometric lattices, in which the loops of the matroid are identified with the zero element of the lattice and sets of mutually parallel elements are identified with the atoms (elements of rank one in the lattice) in exactly the same way as projective spaces are obtained from vector spaces by identifying elements which are mutually linearly dependent.

Duality and Minors

Two crucial ideas in matroid theory are those of duality and of taking minors.

The first, duality, corresponds to orthogonality in vector space theory but is really much simpler. If M is a matroid on S its dual matroid is the matroid on S which has as its bases those subsets of S of the form S\B, whre B is a base of M. It is denoted by M* and clearly (M*)* = M*.

If $e \in S$ we let M'_e denote the matroid on S\e whose independent sets are those independent sets of M which are contained in S\e. We call this operation the deletion of e from S, it corresponds exactly to removing an edge from a graph.

The dual operation, contracting e from S, gives a matroid M''_e on S\e whose independent sets are all sets X of S\e with the property that

$X \cup e$ is independent in M, except in the trivial case when e is a loop of M in which case M_e'' is the same as M_e'.

Contracting is the matroid operation corresponding exactly to contracting an edge from a graph and equivalently to projection in a vector space.

The key facts about these operations are:

(1) The contraction and deletion of elements are commutative matroid operations.

(2) Contraction and deletion are dual operations in the sense that $(M_e')^* = (M^*)_e''$, $(M^*)_e' = M_e''$.

Finally because of (1) we can define a minor of M to be any matroid obtainable from M by a series of contractions and deletions, and write $M > N$ to denote that N is a minor of M.

For proofs of all these statements and more on the theory of matroids we refer to the books by Bryant and Perfect [80], Brylawski and Kelly [80], Crapo and Rota [70], Lawler [76], Tutte [70] or Welsh [76].

§2. Classes of matroids

In this section we briefly describe some different class of matroids which commonly arise in combinatorial applications.

Representable matroids

Let V be a vector space over GF(q), let S be any subset of vectors in V and let $X \subseteq S$ be a member of $\mathcal{J}$ iff X is a linearly independent set of vectors. Any matroid obtained in this way is called representable.

Not all matroids are representable, for example the following 9-element matroid is not representable over any field.

Example. Let $S = \{1,2,\ldots,9\}$ and let $\mathcal{J}$ consist of all subsets of cardinality ≤ 3 except those which are collinear in Figure 1. Those familiar with projective geometry will recognise Figure 1 as the Pappus configuration with one line missing. Since Pappus' theorem must hold in any geometrical configuration coordinatised over a field, this matroid cannot be embedded in a vector space over any field.

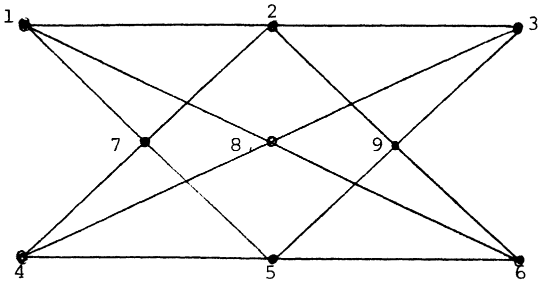


Figure 1

Graphic matroids

Let G be a graph. Call a subset X of edges of G independent if X contains no cycle. This gives a matroid on E(G) called the cycle or polygon matroid of G, and is denoted by M(G), and any matroid obtainable this way is called graphic.

All such matroids are representable over any field. As an example we show in Figure 2 the equivalence and hence coordinisation of the cycle matroid $M(K_4)$ (Figure 2a) with a configuration of points and lines in 2 dimensional space, Figure 2b.

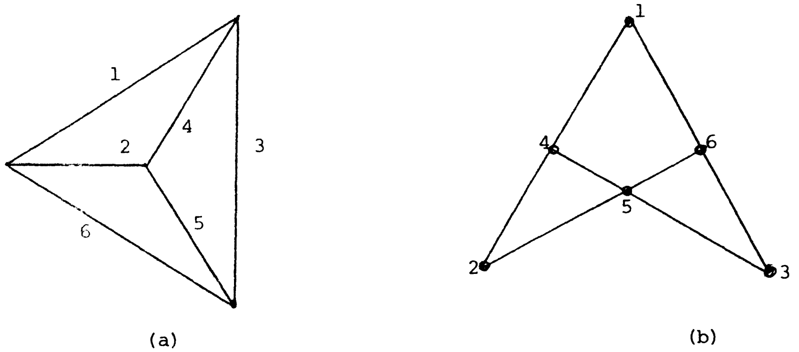


Figure 2

Cographic Matroids

An important class of dual matroids is that obtained from the class of cycle matroids of graphs. Whitney proved:

Theorem 1. If M(G) is the cycle matroid of a graph G then M*(G) is the matroid on E(G) whose circuits are the minimal cutsets of G. Moreover G is a planar graph iff M*(G) is also the cycle matroid of some graph.

Any matroid obtainable in this way is called cographic.

Since it is straightforward to prove that the dual of a representable matroid is also representable (indeed over the same field) then we know:

(1) Cographic matroids are representable over any field.

Transversal Matroids

One of the major applications of matroid theory has been in obtaining new results in transversal theory. For a comprehensive survey of this area we refer to Mirsky [71]. We give the bare outlines here.

Let S be a finite set and let $\mathcal{A} = (A_i : i \in I)$ be a finite collection of subsets of S. A partial transversal of $\mathcal{A}$ is a set X such that there is an injection $\phi : X \to I$ such that for each $x \in X$,

$$x \in A_{\phi(x)} ,$$

and if $i \neq j \Rightarrow \phi(x_i) \neq \phi(x_j)$.

Theorem 2. The collection of partial transversals of a family $\mathcal{A}$ of sets form the independent sets of a matroid $M(\mathcal{A})$.

Any matroid isomorphic to a matroid of the form $M(\mathcal{A})$ for some collection $\mathcal{A}$ is called a *transversal* matroid.

Paving Matroids and Steiner Systems

A matroid is uniquely defined by its collection of hyperplanes, and axioms for a matroid in terms of its hyperplanes are the following.

A collection $\mathcal{H}$ of subsets of S is the set of hyperplanes of a matroid on S if:

(a) No member of $\mathcal{H}$ properly contains another.

(b) If H_1, H_2 are distinct members of $\mathcal{H}$ and $x \in H_1 \cup H_2$ there exists $H_3 \in \mathcal{H}$ such that $H_3 \supseteq (H_1 \cap H_2) \cup x$.

Using these axioms it is easy to prove that if $\mathcal{A} = (A_i : i \in I)$ is a family of subsets of S such that:

(i) $|I| \geq 2$;

(ii) Each member A_i of $\mathcal{A}$ has cardinal at least d;

(iii) Each d-element subset of S is contained in exactly one of the sets A_i;

Then $\mathcal{A}$ forms the set of hyperplanes of a matroid; matroids obtainable in this way are called *paving matroids*.

A particularly interesting paving matroid is the following.

A *Steiner system* S(d, k, n) is a collection of k-subsets called *blocks* of an n-set S such that each d-subset of S is contained in a unique block.

It is easy to see that the blocks of any S(d, k, n) form the hyperplanes of a paving matroid.

§3. Special Matroids

A few matroids will keep on cropping up throughout these lectures.

The simplest type of matroid is the uniform matroid of rank k on n elements. It is defined by the property that it is on a groundset of n elements and every k-subset of the groundset is a base. We denote this matroid by $U_{k,n}$.

A uniform matroid of particular importance is the matroid $U_{2,4}$ often called the 4 point line. It is the smallest matroid which is not binary, that is representable over the field of two elements. Moreover we have the basic theorem of Tutte [65].

Theorem. A matroid is binary if and only if it has no minor isomorphic to $U_{2,4}$.

The smallest binary matroid which is not representable over the reals is the Fano matroid which we denote by F_7. It is the seven point matroid of rank 3 corresponding to the projective plane PG(2,2). It has a binary representation by the columns of the matrix below.

$$F_7 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Its dual matroid F_7^*, sometimes called the heptahedron, has rank 4 and has the matrix representation shown over GF(2).

$$F_7^* = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

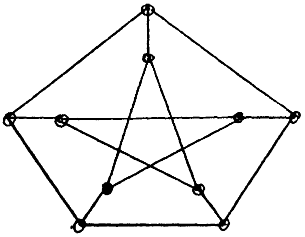
In general we shall write M(G) to denote the cycle or polygon matroid of a graph G and M*(G) to denote the cocycle or bond matroid of G.

However when the graph G is not planar so that there is no possible source of confusion we may write G or G* to denote respectively M(G) or M(G*).

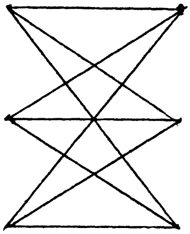
In particular K_5 will be used to denote the graph K_5 and its equivalent geometric form, the three dimensional Desargues' configuration. It is a useful exercise to carry out this identification. An instant corollary is that, the Desargues configuration has automorphism group isomorphic to S_5.

Now take the Desargues configuration and join by a line each pair of points which are not collinear in it. The resulting configuration of 10 points and 15 lines will form the Petersen graph P_{10}. Its cocyle matroid occurs frequently in lectures 7 and 8 and is denoted by P^*_{10} .

The bipartite graph $K_{3,3}$ is another graph whose matroids recur in matroid theory. Again we often write $K^*_{3,3}$ to denote $M^*(K_{3,3})$.



P_{10}

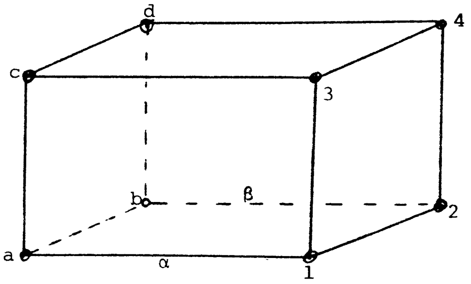


$K_{3,3}$

All the matroids we have described above have been representable over some field, graphic and cographic matroids are in fact representable over every field. An example of a matroid which is representable over no field in the following matroid which is sometimes described as the Vamos matroid, V_8. It has eight elements a,b,c,d, 1,2,3,4 and rank 4 and its bases are all 4-sets of the groundset except the set $\mathcal{L}$ of 'lines' defined as follows: Take

$$\alpha = \{a,1\},\ \beta = \{b,2\},\ \gamma = \{c,3\},\ \delta = \{d,4\}.$$

Then $\mathcal{L}$ is the set $\alpha \cup \beta$, $\alpha \cup \gamma$, $\alpha \cup \delta$, $\beta \cup \gamma$, $\beta \cup \delta$, but not $\gamma \cup \delta$. The reason why it is not representable over any field is easy to see. V_8 can be 'represented' in 3 dimensional Euclidean space as follows.



By postulating $\alpha \cup \beta$ etc. to be members of $\mathcal{L}$ we are demanding that a,b 1,2 etc. are coplanar. However if we have a 'true' embedding of V_8 in Euclidean space we have made so many sets of points coplanar that we would force c,d, 3,4 to be coplanar - however since we demand $\gamma \cup \delta \notin \mathcal{L}$. This is not the case. Hence V_8 is not representable.

§4. Excluded minor theorems

We have already seen one excluded minor condition in §3 where we noted Tutte's theorem characterising binary matroids as those which have no minor isomorphic to $U_{2,4}$. Much of matroid theory is concerned with theorems of this type. The prototype of these theorems is the one quoted above, Tutte's other big theorems are also of this type and more recently we have had other excluded minor type conditions found by Reid [70], Bixby [79] and notably Seymour [77], [79], [80] and [81]. We summarise these results below.

(1) M is binary iff $M \not> U_{2,4}$.

(2) M is representable over GF(3) iff $M \not> U_{2,5}, U_{3,5}, F_7$ or F_7^* .

Following Walton and Welsh [80] we define $Ex(M_1, M_2, \ldots, M_k)$ to be the class of binary matroids with no minor isomorphic to M_i, $1 \leq i \leq k$. Then we have:

(3) M is regular, (i.e.. representable over every field) iff $M \in Ex(F_7, F_7^*)$.

(4) M is graphic iff $M \in Ex(F_7, F_7^*, K_5^*, K_{3,3}^*)$.

For $\mathfrak{F}$ any class of matroids $\mathfrak{F}^*$ is the dual class defined by $M \in \mathfrak{F}^* \Leftrightarrow M \in \mathfrak{F}$. Clearly therefore we can dualise (4) to get

(5) M is cographic iff $M \in Ex(F_7, F_7^*, K_5, K_{3,3})$.

We shall make extensive use of these crucially important theorems below, particularly in lectures 6, 7 and 8.

§5. Matroid polyhedra

Instead of axiomatising a matroid by its independent set axioms we could habe defined it as a pair (S,r) where $r : 2^S \rightarrow Z^+$ satisfies: for all $A, B \subseteq S$;

(1) $r(\phi) = 0$

(2) $A \subseteq B \Rightarrow r(A) \leq r(B)$,

(3) $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$,

(4) $r\{x\} \leq 1 \quad x \in S$.

Here of course r is the rank function. If we drop the constraint (4) and have a function μ satisfying just (1), (2) and (3) we call (S,μ) an integer polymatroid, and if we allow μ to take non-integer values we have just a polymatroid.

μ is called the ground set rank function. It defines a polyhedron P in $\mathbb{R}_S^+$ by the $2^n + n$ inequalities ($n = |S|$) of the form:

$$\underset{\sim}{x} \in P \Leftrightarrow \sum_{i \in A} x_i \leq \mu(A) \quad A \subseteq S, \quad x_i \geq 0,$$

we call P the independence polytope of the polymatroid. The vector rank $r(\underset{\sim}{a})$ of a vector $\underset{\sim}{a} \in \mathbb{R}^S$ is then given by

$$r(\underset{\sim}{a}) = \min_{A \subseteq S}\{a(A) + \rho(S \backslash A)\} .$$

We often write $\mathbb{P} = (S,P,\mu)$ to indicate that $\mathbb{P}$ has ground set rank function μ and independence polytope P.

An alternative definition of a polymatroid is as follows.

Definition 2. A polymatroid is a pair (S,P) where S, the ground set is a non empty finite set and P, the set of independent vectors in $\mathbb{P}$ is a non empty compact subset of $\mathbb{R}_S^+$ in the space $\mathbb{R}_S$ such that

(a) every subvector of an independent vector is independent

(b) for every vector $\underset{\sim}{a}$ in $\mathbb{R}_S^+$, every maximal independent subvector $\underset{\sim}{x}$ of $\underset{\sim}{a}$ has the same modulus, $r(\underset{\sim}{a})$, the vector rank of $\underset{\sim}{a}$ in $\mathbb{P}$.

It is not that difficult to show the equivalence of the two above definitions, details are given in [Welsh 76, Chapter 18].

The two crucial properties of polymatroids are the following results of Edmonds [70].

Theorem 1. If P is the independence polytope of an integer polymatroid all the vertices of P are integer valued.

Proof. (Sketch) Consider any vertex v of P; choose a linear function which achieves its maximum over P only at v. By the greedy algorithm (see §3.1) there is an integral solution which is optimum. Since v is the only solution v must be integral.

Theorem 2. If P_1, P_2 are the independence polytopes of two integer polymatroids then all the vertices of $P_1 \cap P_2$ are integral.

Proof. Much harder: see Lawler [76].

3. Matroids and Algorithms

§1. The greedy algorithm

In 1957 R. Rado realised that a well known and simple minded algorithm for finding a spanning tree of a graph which had a maximum weight over all weighted trees could be generalised to give an algorithm which would find a base of maximum (or minimum) weight in any matroid.

Indeed more can be said: suppose that S is a finite set and $w : S \to \mathbb{R}^+$ is a weight function. Extend $w : 2^S \to \mathbb{R}^+$ by letting

$$w(A) = \sum_{x \in A} w(x) \qquad (A \subseteq S) .$$

Let $\mathcal{J}$ be any collection of subsets of S which satisfies the conditions

(i) $\emptyset \in \mathcal{J}$

(ii) $A \in \mathcal{J} , \ B \subseteq A \Rightarrow B \in \mathcal{J}$.

Define problem $\pi(\mathcal{J},w)$ to be the problem of finding a member of $\mathcal{J}$ of maximum weight.

For a given such $\mathcal{J}$ and w let $X(\mathcal{J},w)$ be the subset of S obtained by the following procedure:

(1) Select element $x \in S$ such that $\{x\} \in \mathcal{J}$ and such that $w\{x\}$ is a maximum over all such x.

(2) Let $X = \{x\}$

(3) Select $y \in S\backslash X$ such that $X \cup \{y\} \in \mathcal{J}$ and such that of all such

y, $w(X \cup y)$ is a maximum. If no such y exists stop.

(4) Let $X = X \cup \{y\}$ and return to (3).

It is not difficult to prove

Theorem 1. If $\mathfrak{F}$ is the collection of independent sets of a matroid then for any non negative w, $X(\mathfrak{F}, w)$ is an optimum set. Conversely if $X(\mathfrak{F}, w)$ is an optimum set for all possible choices of $w \geq 0$, then $\mathfrak{F}$ is the collection of independent sets of a matroid.

Proof. Straightforward see Welsh [76, Chapter 19].

The procedure of getting the set $X(\mathfrak{F}, w)$ above has been aptly christened the greedy algorithm, and an appealing axiomatisation of matroids is "that they are the only structures for which the greedy algorithm works for all choices of non-negative weight function".

§2. The union of matroids

Let $M_i (1 \leq i \leq k)$ be matroids on the sets $S_i (1 \leq i \leq k)$ which may or may not be disjoint.

The union of the M_i, denoted by $M_1 \vee \ldots \vee M_k$ is the matroid on $S = S_1 \cup \ldots \cup S_k$ in which a set X is independent if and only if

$$X = X_1 \cup \ldots \cup X_k$$

where X_i is independent in M_i. If r_i is the rank function of M_i, then $M_1 \vee \ldots \vee M_k$ has rank function, defined for all $A \subseteq S$ by

$$(1) \qquad r(A) = \min_{X \subseteq A} (r_1 X + \ldots + r_k X + |A \backslash X|) \ .$$

This construction in matroid theory has many applications, see for example the article by A. Recski in this volume.

It is also important because it can be proved by perhaps the first example of a 'good' but non-trivial algorithm in matroid theory. More precisely suppose that in the above situation we wish to know whether or not the ground set S can be partitioned into sets $I_1,\ldots,I_k$ such that for $1 \le j \le k$, I_j is independent in M_j. Edmonds [65] has produced an algorithm which does this in polynomial time provided that whether or not a set X is independent in M_j can be decided in polynomial time. This algorithm known as the matroid partitioning algqrithm, produces constructive proofs of the result (1) and has an interesting 'dual algorithm' called the intersection algorithm.

Consider first the following well known theorem, see Welsh [76, Chapter 8].

Theorem 1. If M_1 and M_2 are matroids on S then there exists a set X with $|X| \ge k$ and which is independent in both M_1 and M_2 if and only if for all $A \subseteq S$,

$$r_1(A) + r_2(S\backslash A) \ge k.$$

It is not difficult to deduce this result from (1) by duality theory. Correspondingly, provided there is a fast algorithm for recognising independence in both M_1 and M_2 there is a 'fast', that is polynomial, algorithm for finding a set X of maximum weight w(X) and which is independent in both M_1 and M_2. This algorithm, known as the 'matroid intersection algorithm' is well described in Lawler [76]

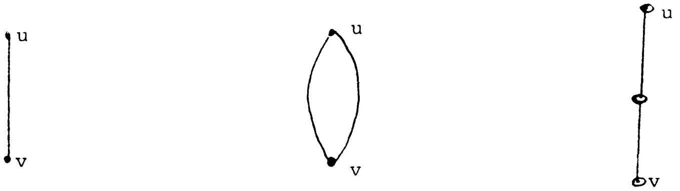
§3. The Shannon switching game

A very nice application of the partitioning algorithm ıs that it gives a polynomial algorithm for the following game, commonly called the Shannon-switching game but which we shall call EDGE - HEX.

In §1.6 we defined the game VERTEX - HEX in which two players alternately colour vertices of a graph in an attempt to join (or cut) two specified vertices.

EDGE - HEX is exactly the same game except that instead of colouring vertices the players alternately colour edges of G.

Call a graph G (and a pair of specified vertices) a join graph if there is a winning strategy for the join player whether or not he goes first. Similarly G is a cut graph if the cut player can win against all possible strategies of the join player, no matter who goes first. Finally G is a neutral graph if the player who goes first can win against all possible strategies of the other player. Mutually exclusive possibilities are illustrated in the example of Figure 1.



(a) neutral graph (b) join graph (c) cut graph

Figure 1

Lehman [64] characterised join graphs in the following theorem:

Theorem 1. The game (G,u,v) is a join game if and only if there exist two edge disjoint trees T_1, T_2 on the same subset of vertices $V(T_1) = V(T_2) \subseteq V(G)$ such that $\{u,v\} \subseteq V(T_i)$.

Similar 'derived' theorems characterise cut and neutral graphs. More importantly, it is reasonably straightforward to apply the partitioning algorithm of the last section to give a polynomial algorithm which decides whether or not a graph G is cut, neutral or join. In other words we have the dichotomy when comparing with §1.6.

(1) Deciding whether the first player can win VERTEX HEX is complete in P-space but the same problem for EDGE HEX can be done in polynomial time.

§4. A polynomial algorithm for k-connectivity

A matroid M on S is connected if there exists no proper subset A of S with

$$r(A) + r(S\backslash A) = r(S) \ .$$

It has been known for some time that there exists polynomial algorithms to test whether a matroid is connected or not (see for example Cunningham [73]).

More recently Cunningham and Edmonds (1979) have announced a polynomial algorithm to test for a given matroid M whether or not it has a k-separation, that is a set $A \subseteq S$, such that

$$r(A) + r(S\backslash A) \leq r(S) + (k-1) \qquad (1)$$

where both $|A|$ and $|S\backslash A|$ are not less than k.

As we shall see in §6.4 in connection with Seymour's decomposition theorem for unimodular matrices we will need to decide whether or not a given matroid has such a separation. The following method shows the existence of such a polynomial algorithm provided independence in the matroid can be checked in polynomial time.

By the matroid intersection theorem, two matroids M_1, M_2 with rank functions r_1, r_2 have a common independent set of size t iff$\forall\, Y \subseteq S$,

(2) $$r_1(Y) + r_2(S\backslash Y) \geq t.$$

For the given matroid M on S consider

$$M_1 = (M\backslash X_1)/X_2 \ ,$$
$$M_2 = (M\backslash X_2)/X_1 \ .$$

Then M_i on $T = S\backslash(X_1 \cup X_2)$ has rank function r_i, for $U \subseteq T$, given by

$$r_1(U) = r(U \cup X_2) - r(X_2)$$
$$r_2(U) = r(U \cup X_1) - r(X_1).$$

Using (2), M_1, M_2 have a common independent set of size t if and only if for all $U \subseteq T$,

$$r((T\backslash U) \cup X_2) + r(U \cup X_1) \geq t + r(X_1) + r(X_2).$$

This proves the validity of the following algorithm:

Algorithm

(1) Select pairs of disjoint k-sets (X_1, X_2) in turn.

(2) For each pair (X_1, X_2) use the intersection algorithm to decide if M_1, M_2 above have a common independent set of size t where t is chosen so that

$$t + r(X_1) + r(X_2) = r(S) + (k-1) \ .$$

(3) If no such independent set exists then the corresponding (X_1, X_2) induces a k-separation of M, otherwise M has no k-separation.

Clearly this is polynomial since the intersection algorithm is polynomial and the number of ways of picking the pair (X_1, X_2) is $O(n^{2k})$.

For more on connectivity see §6.2 below and also the article by J.G. Oxley in this volume.

4. Lovász's Attack on the Parity Problem

§1. The parity problem

The classical parity problem seems to have originated with E. Lawler in (1971) when it was defined as follows.

Given a matroid M on S and a partitioning of S (taken to be a set of even cardinality 2n) into blocks of size 2, say

$$\{e_1,\bar{e}_1\},\ \{e_2,\bar{e}_2\},\ \ldots\ ,\ \{e_n,\bar{e}_n\},$$

find an algorithm for deciding whether or not M has an independent set X of cardinal t with the property that $e_i \in X$ if and only if its mate $\bar{e}_i \in X$. Such a set is called an independent parity set.

The above is called the 2-parity problem to distinguish it from the k-parity problem in which we take $|S| = kn$, and we partition S into disjoint blocks E_i, where $|E_i| = k$, $1 \le i \le n$, and we wish to decide whether M has an independent set X, of cardinality t such that if $X \cap E_i \neq \emptyset$ then $X \supseteq E_i$.

We first remark that the 'k-matroid intersection problem' is a special case of the 'k-parity problem'.

Proof. Let M_i, $1 \le i \le k$, be matroids on S. Take $S_1,\ldots,S_k$ to be disjoint copies of S and let M_i' be an isomorphic copy of M_i on the set S_i. Let

$$N = \bigvee_{i=1}^{k} M_i' \ .$$

Define the k-parity sets for $S' = S_1 \cup \ldots \cup S_k$ in the obvious way:- a given block is $\{e_i^1,\ldots,e_i^k\}$ where e_i^j is the copy of $e_i \in S$ in the set S_j. It is easy to see that there is a 1-1 correspondence between k-parity sets of N and intersections of the k matroids $M_1,\ldots,M_k$. □

Hence since the k-matroid intersection problem reduces in a special case to deciding whether k families of sets have a common transversal, and this is NP-complete, we have shown:

(1) For $k \geq 3$, the k-parity problem is NP-hard.

However for $k = 2$ the situation is different.

First note that the 2-parity problem cannot be 'extremely' easy since it certainly includes 2-matroid intersection, which is not trivial. It also includes the problem of finding a maximum matching in a graph.

A <u>matching</u> in a graph $G = (V,E)$ is a subset $F \subseteq E$ such that no two members of F are incident with a common vertex. Finding a maximum matching in a graph is a highly non-trivial problem but it does have a polynomial algorithm (Edmonds (65)).

It is not difficult to prove:

(2) MAXIMUM MATCHING $\propto$ 2-PARITY.

<u>Proof</u>. Replace each edge e_i of G by a pair of edges $f_i, \bar{f}_i$ with a new vertex between them. Let $G' = (V',E')$ be the graph so obtained. If $\mathcal{J}$ is the collection of sets $X \subseteq E'$ such that no two edges of X are incident with the same vertex of G', unless it is one of the new vertices created by subdivision, then it is not difficult to verify that $\mathcal{J}$ is the collection of independent sets of a matroid M on E'. The 2-parity problem for M with f_i and $\bar{f}_i$ as mates solves the maximum matching problem for G. □

§2. 2-polymatroids

We have already met polymatroids in §2.4. Here we concentrate on a special class of polymatroids, called by Lovász [80], 2-polymatroids.

Recall that a polymatroid can be defined as a pair (S,μ) where $\mu : 2^S \to \mathbb{R}^+$ satisfies

(1) $\mu(\phi) = 0$,

(2) $A \subseteq B \Rightarrow \mu(A) \leq \mu(B)$,

(3) $\mu(A) + \mu(B) \geq \mu(A \cup B) + \mu(A \cap B)$.

The pair (S,μ) is a 2-polymatroid if in addition we restrict μ to taking only integer values and to satisfy the constraint

(4) $\mu(\{x\}) = 2$ for all $x \in S$.

Note first that an immediate consequence of (3), (4) is:

(5) For all $X \subseteq S$, $\mu(X) \leq 2|X|$.

First some examples:

Example 1. If M_1 and M_2 on S are matroids with rank functions r_1 and r_2 then (S,r_1+r_2) is a 2-polymatroid.

Example 2. If S is any collection of lines (= flats of rank 2) in a matroid and we define

$$\mu\{\ell_1,\ell_2,\ldots,\ell_k\} = r\{\ell_1 \cup \ldots \cup \ell_k\}$$

where r is the rank function of the matroid then (S,μ) is a 2-polymatroid.

Example 3. If $G = (V,E)$ is a graph with no loops and for $X \subseteq E$ we define $\mu(X)$ to be the number of vertices of G which are incident with X then (E,μ) is a 2-polymatroid.

A set $X \subseteq S$ is a <u>matching</u> in the 2-polymatroid (S,μ) if

$$\mu(X) = 2|X|,$$

and the cardinality of a maximum matching we denote by $\nu(S,\mu)$, or when there is no ambiguity by $\nu(S)$.

Intuitively we may think of $\nu(S,\mu)$ as the 'cardinality of the largest independent set in the polymatroid'.

Thus in the examples above we have:

<u>Example 1</u>. $\nu(S,r_1+r_2)$ is the maximum cardinality of a set independent in both M_1 and M_2.

<u>Example 3</u>. $\nu(E(G),\mu)$ is the (maximum) cardinality of a set of pairwise disjoint edges, often denoted by $\alpha(G)$.

The relationship with the 2-parity problem is a consequence of the following proposition.

<u>Proposition</u>. Finding a maximum 2-parity set in a matroid is no harder than finding a maximum matching in a 2-polymatroid.

<u>Proof</u>. We assume M is simple on $S = S_1 \cup S_2$ where

$$S_1 = \{e_1,\dots,e_n\},\ S_2 = \{\bar{e}_1,\dots,\bar{e}_n\} \quad .$$

are disjoint sets.

Let ℓ_i $(1 \le i \le n)$ be the line of the matroid M which contains the pair $e_i,\bar{e}_i$. Let $L = \{\ell_1,\dots,\ell_n\}$ and let (L,μ) be the 2-polymatroid defined by

$$\mu\{\ell_1,\ell_2,\dots,\ell_k\} = r\{\ell_1 \cup \dots \cup \ell_k\} \quad .$$

where r is the rank function of M. It is easy to verify that this in fact does give a 2-polymatroid. Moreover $\{\ell_1,\ldots,\ell_k\}$ is a matching of size k in (L,μ) if and only if

$$\mu\{\ell_1,\ldots,\ell_k\} = 2k$$

which is the case if and only if $\{e_1,\bar{e}_1,e_k,\ldots,e_k,\bar{e}_k\}$ is an independent parity set of size 2k in M. □

§3. The Gallai-Lovász Identity

Consider Example 3 of the previous sections. A well known identity of graph theory due to Gallai [61] relates $\alpha(G)$, the maximum number of disjoint edges with $\beta(G)$, the minimum number of edges needed to cover all the vertices of G by

(1) $$\alpha(G) + \beta(G) = |V(G)| .$$

Suppose we denote by $\rho(S) = \rho(S,\mu)$ the minimum cardinality of a set $X \subseteq S$ such that $\mu(X) = \mu(S)$. In other words, $\rho(S)$ is 'the minimum cardinality of a spanning set'. Then we can prove the following result of Lovasz [80].

<u>Theorem 1</u>. <u>In any 2-polymatroid</u> (S,μ),

$$\nu(S) + \rho(S) = \mu(S).$$

This obviously gives Gallai's Theorem [61] as a special case.

When μ is the sum of rank functions of two matroids M_1 and M_2, Example 1 above, it relates the maximum size of a common independent in the two matroids with the minimum size of a set spanning in both matroids.

In order to prove Theorem 1 we need the following lemma.

Lemma. Let (S,μ) be a 2-polymatroid and let A be a maximum matching. If $\mu_A : 2^S \to \mathbb{Z}$ is defined by

$$\mu_A(X) = \mu(A \cup X) - \mu(A) \qquad (X \subseteq S)$$

then (S,μ_A) is a matroid.

Proof. $\mu_A(\phi) = 0$.

$$\begin{aligned}\mu_A(X) + \mu_A(Y) &= \mu(A \cup X) + \mu(A \cup Y) - 2\mu(A)\\ &\geq \mu(A \cup X \cup Y) + \mu(A \cup (X \cap Y)) - 2\mu(A)\\ &= \mu_A(X \cup Y) + \mu_A(X \cap Y)\end{aligned}$$

so that μ is submodular, and clearly increasing. Moreover $\mu_A\{x\} = \mu(A \cup \{x\}) - \mu(A)$, so that if $x \in A$, $\mu_A\{x\} = 0$ while since A is a maximum matching $\mu_A\{x\} \leq 1$ when $x \notin A$. □

Proof of Theorem 1. Let (S,μ) be a 2-polymatroid and let T be a subset of S of minimum cardinality such that $\mu(T) = \mu(S)$.

Let A be a maximum matching in T, that is A is a set of maximum cardinality which is contained in T and for which

$$\mu A = \sum_{x \in A} \mu(x) = 2|A| .$$

Let $X = T\backslash A$, so that

$$\begin{aligned}\mu(S) &= \mu(T)\\ &= \mu(A \cup (T\backslash A)) .\end{aligned}$$

Thus using the lemma

$$\begin{aligned}\mu(S) &= \mu_A(T\backslash A) + \mu(A)\\ &\le |T\backslash A| + \mu(A) = |T\backslash A| + 2|A|\\ &\le |T| + |A| .\end{aligned}$$

Hence we have

$$\rho(S) = |T| \ge \mu(S) - |A| = \mu(S) - \nu(S) . \tag{2}$$

On the other hand, suppose that A is a maximum matching in (S,μ) and suppose that X is a basis of the matroid (S,μ_A). Then

$$\begin{aligned}\mu(A \cup X) &= \mu(A) + \mu_A(X)\\ &= \mu(A) + \mu_A(S\backslash A) = \mu(S)\end{aligned}$$

since all the elements of A are loops in (S,μ_A). Hence $\rho(S) \le |A \cup X|$. Thus

$$\begin{aligned}\rho(S) \le |A \cup X| &= |A| + |X| = |A| + \mu_A(X)\\ &= |A| + \mu_A(S\backslash A)\\ &= |A| + \mu(S) - \mu(A)\\ &= |A| + \mu(S) - 2|A|\\ &= \mu(S) - |A|\\ &= \mu(S) - \nu(S)\end{aligned}$$

and this with (2) completes the proof. □

We close this section by remarking that it is easy to find examples to show that Theorem 1 fails when (S,μ) is a polymatroid but not a 2-polymatroid.

§4. A min-max theorem for linear 2-polymatroids

Suppose that $\mathbb{P}$ is a projective space. Let $A_1,\ldots,A_n$ be subsets of $\mathbb{P}$ and let $S = \{A_1,\ldots,A_n\}$. We can define a polymatroid (S,μ) on S by defining

$$\mu(X) = r(\cup\{A_i : A_i \in X\}) \qquad (X \subseteq S),$$

where r is the rank function of the underlying space $\mathbb{P}$. Any polymatroid obtained in this way we call a linear polymatroid, and when the A_i are all lines in $\mathbb{P}$ we have a linear 2-polymatroid.

Lovász [80a] proved the following remarkable result.

Theorem 1. Let (S,μ) be a linear 2-polymatroid formed by subspaces of a projective space $\mathbb{P}$. Then

$$\nu(S) = \min\left(r(A) + \sum_{i=1}^{k} \left\lfloor \frac{\mu(S_i+A) - r(A)}{2} \right\rfloor\right)$$

where A ranges over subspaces of $\mathbb{P}$ and $\{S_1,S_2,\ldots,S_k\}$ ranges over all partitions of S, and where

$$\mu(S_i+A) = r(\{\cup A_j : A_j \in S_i\} \cup A) .$$

The proof of this theorem is difficult, we can do no more than sketch the main idea.

First, however, we describe an equivalent formulation. This was the original geometrical result proved by Lovasz in (1978).

Let $\mathcal{H}$ be a set of subspaces of a projective geometry. A subfamily $\mathcal{F}$ of $\mathcal{H}$ is called independent if no member of $\mathcal{F}$ intersects the flat spanned by the other members.

Theorem 2. Let $\mathcal{H}$ be a set of lines in a projective space $\mathbb{P}$. Then the maximum number $\nu(\mathcal{H})$ of independent lines in $\mathcal{H}$ is equal to the minimum value of

$$r(A) + \sum_{i=1}^{k} \left\lfloor \frac{r(A_i) - r(A)}{2} \right\rfloor$$

where $A, A_1, \ldots, A_k$ are flats of $\mathbb{P}$ such that $A \subseteq A_i$ $(i=1,2,\ldots,k)$ and each line in $\mathcal{H}$ which does not intersect A is contained in some A_i, and r is the rank function of the underlying projective space $\mathbb{P}$.

We leave it as a (not difficult) exercise for the reader to show the equivalence of Theorems 1 and 2.

As part of this we state without proof:

(1) Let $\mathcal{F}$ be a set of lines in $\mathbb{P}$, then $r(\mathcal{F}) \leq 2|\mathcal{F}|$ with equality if and only if $\mathcal{F}$ is an independent set of lines.

Sketch Proof of Lovasz's Theorem 2

First we show that if $\mathcal{F}$ is any set of independent lines and $A, A_1, \ldots, A_k$ are subspaces such that $A \subseteq A_i$ and each line of $\mathcal{F}$ either meets A or is contained in some A_i, then

$$|\mathcal{F}| \leq r(A) + \sum_{i=1}^{k} \left\lfloor \frac{r(A_i) - r(A)}{2} \right\rfloor .$$

Let $\mathcal{F}_i$ and $\mathcal{F}_0$ denote the set of lines of $\mathcal{F}$ which are contained in A_i and which meet A respectively.

Let A_i' be the subspace of $\mathbb{P}$ spanned by $\mathcal{F}_i' = \mathcal{F}_i \setminus \mathcal{F}_0$.

Let A_2' be the subspace spanned by $\mathcal{F}_2 \backslash \mathcal{F}_1 \backslash \mathcal{F}_0$ and in general let A_i' be the subspace spanned by $\mathcal{F}_i' = \mathcal{F}_i \backslash \mathcal{F}_{i-1} \backslash \mathcal{F}_{i-2} \backslash \ldots \backslash \mathcal{F}_1 \backslash \mathcal{F}_0$.

Then

$$r(A_1') = 2|\mathcal{F}_1'|$$

and more generally

$$r(A_i') = 2|\mathcal{F}_i'|$$

and moreover the spaces A_i' are clearly independent and hence so are the spaces $A_i' \cap A$, $0 \le i \le k$. Thus

$$r(A) \ge \sum_{1}^{k} r(A_i' \cap A).$$

But

$$\begin{aligned} r(A_i' \cap A) &= r(A_i') + r(A) - r(A_i' \cup A) \\ &\ge r(A_i') + r(A) - r(A_i). \end{aligned}$$

$$\therefore \quad |\mathcal{F}_i'| = \tfrac{1}{2} r(A_i') \le \frac{r(A_i) - r(A)}{2} + \frac{r(A_i' \cap A)}{2}$$

$$\le \frac{r(A_i) - r(A)}{2} + r(A_i' \cap A),$$

and using integrality.

$$|\mathcal{F}_i'| \le \left\lfloor \frac{r(A_i) - r(A)}{2} \right\rfloor + r(A_i' \cap A).$$

$$\therefore \quad |\mathcal{F}| = \sum_{i=0}^{k} |\mathcal{F}_i'| \le \sum_{i=1}^{k} \left\lfloor \frac{r(A_i) - r(A)}{2} \right\rfloor + r(A_i' \cap A) + r(A_0' \cap A)$$

$$\le r(A) + \sum_{i=1}^{k} \left\lfloor \frac{r(A_i) - r(A)}{2} \right\rfloor$$

which proves one half of the identity.

We now prove the converse by induction on $\nu(\mathfrak{F})$.

Case 1. There exists a point p in the projective space $\mathbb{P}$ such that p is contained in the span of each collection of $\nu(\mathfrak{F})$ independent lines. Project from p onto a hyperplane of $\mathbb{P}$ not going though p, (that is contract p out of the underlying matroid). This gives a collection $\mathfrak{F}_1$ of independent lines. We assert $|\mathfrak{F}_1| \leq \nu(\mathfrak{F}) - 1$ for suppose that

$$|\mathfrak{F}_1| = \nu(\mathfrak{F}).$$

Then the original lines in $\mathfrak{F}$ must have formed a set of $\nu(\mathfrak{F})$ independent lines.

But $p \in \operatorname{span}(f^{-1}(\mathfrak{F}_1))$.

Hencep and the set of lines $\mathfrak{F}_1$ are in a space of rank $2\nu(\mathfrak{F})$. Thus the lines $\mathfrak{F}_1$ are contained in a space of rank $2\nu(\mathfrak{F}) - 1$. But it is impossible to have $\nu(\mathfrak{F})$ independent lines in a subspace of rank $2\nu(\mathfrak{F}) - 1$.

Hence $\nu(\mathfrak{F}_1) \leq \nu(\mathfrak{F}) - 1$.

Hence by the induction hypothesis there exist flats $A', A_1', \ldots, A_k'$ in this hyperplane H such that each line of $\mathfrak{F}_1$ not intersecting A' is contained in some A_i', $A' \subseteq A_i'$, and

$$(*) \qquad \nu(\mathfrak{F}) - 1 \geq r(A') + \sum_{i=1}^{k} \left\lfloor \frac{r(A_i') - r(A')}{2} \right\rfloor .$$

Now take A to be the flat spanned by A' and p and A_i to be the flat spanned by A_i' and p for $1 \leq i \leq k$, and we obtain the required set of flats in $\mathbb{P}$.

For clearly the right hand side of (*) is increased by 1 if we replace A', A_i' by A and A_i respectively. Moreover if a line ℓ does not intersect A its projection ℓ' does not intersect A' and hence ℓ' is contained in some A_i' which implies ℓ is contained in A_i .

Case 2. For each point $p \in \mathbb{P}$ there exists a set of $\nu(\mathfrak{F})$ independent lines in $\mathfrak{F}$ whose span does not include p.

This is the hard part of the proof, and we can only make a few remarks to illustrate the difficulty.

a) Any A achieving the minimum on the right hand side of the equation must be empty for otherwise it can be shown that a p exists for which Case 1 applies.

b) Because of (a) we need to show that there exist pairwise disjoint flats $A_1,\ldots,A_k$ in $\mathbb{P}$ such that each line of $\mathfrak{F}$ is contained in one of these A_i and moreover

$$\nu(\mathfrak{F}) = \nu_1+\ldots+\nu_k$$

where $r(A_i) = 2\nu_i + 1$, $1 \le i \le k$.

This implies that each collection of $\nu(\mathfrak{F})$ independent lines in $\mathfrak{F}$ has ν_i lines which are contained in A_i .

§5. On a polynomial algorithm for the 2-parity problem

Consider now the algorithmic problem.

π_1 : INSTANCE: A 2-polymatroid (S,μ) and an integer t.

QUESTION: Does (S,μ) have a matching of cardinality $\ge$ t?

We are interested in the question whether or not π_1 has a polynomial algorithm subject to the proviso that we can obtain the rank μX of an arbitrary set X in time which is a polynomial function of $|X|$.

By taking the special cases of μ discussed in §2 any such algorithm would be a polynomial algorithm for the graph matching problem and the matroid intersection problem, and hence is unlikely to be trivial. Indeed Garey and Johnson [79, p. 287] pose as an open problem that of deciding whether or not the following problem π_2 is NP-complete.

π_2 : INSTANCE: Graph $G = (V,E)$ and a partition of E into disjoint 2-element sets $E_1,\ldots,E_m$.

QUESTION: Is there a spanning tree $T = (V,E')$ for G such that for each E_i, $1 \le i \le m$, either $E_i \subseteq E'$ or $E_i \cap E' = \phi$?

This is clearly a special case of the matroid parity problem in which the underlying matroid M is graphic.

Now consider Lovász's Theorem 4.1. Provided we are given a 2-linear polymatroid represented in the projective space we can nondeterministically either

"produce a set of k independent lines, that is a matching of size k"

or

"produce a set A and a partition $\{S_1,\ldots,S_k\}$ of S such that

$$r(A) + \sum_{i=1}^{k} \left\lfloor \frac{\mu(S_i+A) - r(A)}{2} \right\rfloor < k \text{ "}$$

and more importantly we can check these assertions in polynomial time.

Thus in the terminology of Chapter 1 we know π_1 is a member of (NP) $\cap$ (co-NP), and hence in view of our earlier remarks it would give some hope that there exists a polynomial algorithm for π_1 .

This Lovász has produced. It is an extremely complicated algorithm, of high polynomial complexity, and of course only works for linear polymatroids which are represented not just representable in some projective space.

There is fairly strong evidence (see 5.3 below) that the matching problem for general 2-polymatroids is not solvable in polynomial time, however it is also clear that there do exist polynomial algorithms for certain classes of 2-polymatroids which are not representable - for example any polymatroid (S,μ) for which μ can be written as the sum of two rank functions. Extending this class is an interesting but almost certainly formidable problem.

§6. Pinning planar structures

As a nice application of Lovász's theory we consider a problem arising in the theory of rigid structures.

Consider a graph G whose vertices are points in the Euclidean plane and whose edges are rigid bars with flexible joints at the vertices. Suppose that some of the bars are pinned down to the plane. An infinitesimal motion is an assignment of a velocity $v(x)$ to each vertex x such that for every edge (x,y) of G,

$$(v(x) - v(y)).(x-y) = 0$$

and

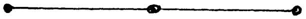
$$v(x) = 0 \quad \text{if } x \text{ is pinned.}$$

A structure is rigid if its only infinitesimal motion is $v(x) = 0 \ \forall \ x \in V(G)$.

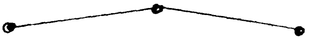
Deciding whether or not a structure is rigid is a straightforward exercise in linear algebra. The pinning number $\pi(G)$ of a structure is the minimum number of vertices which need to be pinned in order to make G rigid.

First note, that although we represent π as a function only of G, in reality it is a function also of its representation in the plane. An easy illustration of this is provided by the following example.

Example. G



G'



G and G' are isomorphic graphs but $\pi(G) = 3$ whereas $\pi(G') = 2$.

Now consider the action of pinning down a vertex; in general such an action will reduce the dimension of the vector space of possible motions by exactly 2. Using this basic idea it is not difficult to see (for a rigorous account see Lovász [80]) that finding the pinning number of a planar structure is exactly the problem of finding a minimum spanning set in a 2-polymatroid.

But by the Lovász-Gallai identity this is equivalent to finding the cardinality of a maximum matching and this can then be done by the 2-parity algorithm.

It is interesting that Mansfield [80] has recently shown that finding the pinning number of a structure in 3 or more dimensions is an NP-complete problem and so there will only be a polynomial algorithm if NP = P.

5. Oracle Bounds on Algorithms

§1. The concept of an oracle

There are f(n) non-isomorphic matroids where

$$2^{2^{n-3/2\log n+O(\log\log n)}} \le f(n) \le 2^{2^{n-\frac{1}{2}\log n+O(\log\log n)}}$$

so as pointed out in Robinson and Welsh [80] there is little hope of doing large-scale computing on matroids; for what ever possible way of representing a matroid is chosen the 'data base' or 'size of input' for a matroid problem on an n-set will be $O(2^n)$.

Accordingly the complexity of matroid computations is often measured in terms of the number of demands made on various possible oracles. For example in Robinson-Welsh an independence oracle ($\mathcal{J}$-oracle) is a function I which for any set S and matroid M on S, and any $A \subseteq S$, tells us whether A is independent or not in the matroid M. Formally

$$I(A) = \begin{cases} \text{YES} & \text{if } A \in \mathcal{J}(M) \\ \text{NO} & \text{if not.} \end{cases}$$

A property P of matroids is any collection of matroids which is closed under isomorphism, i.e. if $M \in P$ and $N \simeq M$, then $N \in P$. If P_n denotes the property P restricted to matroids on n-sets then the complexity of P_n with respect to the $\mathcal{J}$-oracle is defined to be the maximum number of calls on the oracle in a minimum algorithm to decide whether or not a matroid M on an n-set has or has not the property P, where the maximum is taken over all possible matroids M on an n-set. This concept is made rigorous in Robinson and Welsh [80] and can clearly be defined for other matroid oracles such as the following.

(1) A base oracle ($\mathcal{B}$-oracle) which tells us whether or not a given set is a base in the matroid under construction.

(2) A circuit ($\mathcal{C}$-oracle) which tells whether or not a set is a circuit.

(3) A rank ($\mathcal{R}$-oracle) which gives the rank of any set.

Two matroid oracles θ_1, θ_2 are polynomially equivalent if there exist polynomials f , g such that for any property P of matroids,

$$C_{\theta_1}(P_n) \leq f(n)\, C_{\theta_2}(P_n)$$

and

$$C_{\theta_1}(P_n) \leq g(n)\, C_{\theta_2}(P_n) \quad ,$$

for all n, where $C_{\theta}(P_n)$ denotes complexity with respect to the θ-oracle.

Proposition. The $\mathcal{I}$ and $\mathcal{R}$ oracles are polynomially equivalent and are not polynomially equivalent to the $\mathcal{B}$ and $\mathcal{C}$ oracles.

Proof. That $\mathcal{I}$ and $\mathcal{R}$ are polynomially related is not difficult to see. The non-equivalence of the other oracles is achieved by constructing various examples, such as taking P to be the property LOOP of having a loop. Then

$$C_{\mathcal{I}}(\mathrm{LOOP}_n) = C_{\mathcal{C}}(\mathrm{LOOP}_n) = n,$$

whereas for n > 1,

$$C_{\mathcal{B}}(\text{LOOP}_n) \geq n^{-3/2}\,2^{n-\frac{1}{2}} \ .$$

Similarly if FREE is the property of having every set independent,

$$C_{\mathcal{I}}(\text{FREE}_n) = C_{\mathcal{B}}(\text{FREE}_n) = 1$$

$$C_{\mathcal{C}}(\text{FREE}_n) = 2^n - 1 \ . \qquad \square$$

§2. Examples and further results

It is clear that the greedy algorithm discussed in §3.1 gives a very fast algorithm with respect to the $\mathcal{I}$ -oracle. Similarly all the other examples 'which worked' in Chapter 3 such as matroid intersection and having a given connectivity are polynomial algorithms with respect to the $\mathcal{I}$ -oracle.

However, our next theorem shows that these examples tend to be the exception rather than the rule.

We, show that with respect to the above oracles 'most' properties are exponential. More precisely we consider binary oracles, i.e. oracles which accept as input any set and only give YES-NO answers, and prove the following theorem.

Theorem. For any binary oracle $\mathcal{O}$ and any α such that

$$\alpha(n) \leq e^{(n-3/2)\log n}$$

$$\lim_{n\to\infty} |D_\alpha(n)|/M(n) = 0$$

where $D_\alpha(n)$ denotes the set of properties P_n of n-element matroids which have $C_{\mathcal{O}}(P_n) \leq \alpha(n)$, and M(n) denotes the number of different properties of matroids on an n-set.

Proof. See Robinson and Welsh [80].

In other words we know that "almost all" matroid properties are exponential with respect to any binary oracle.

Since the rank oracle, while not binary, is polynomially equivalent to the $\mathcal{J}$ -oracle, a similar result holds for the rank oracle.

Other less natural oracles have been considered by some authors. For example Jensen and Korte [80] consider the GIRTH oracle ($\mathcal{G}$-oracle), defined to give for any matroid M on S and any, $T \subseteq S$, the length of the smallest circuit in the matroid $M|T$.

It is easy to find a polynomial p such that for any property P,

$$C_{\mathcal{G}}(P_n) \leq p(n)\, C_{\mathcal{J}}(P_n)$$

and at the same time to exhibit properties which are exponential with respect to $\mathcal{J}$ but polynomial with respect to $\mathcal{G}$. In other words the $\mathcal{G}$ -oracle is strictly stronger (with respect to these measures of complexity) than the independence oracle.

However the search for the 'best oracle' for matroid problems is in reality a hopeless quest since in practice in order to set up this 'best oracle' we would need to do an exponential amount of work.

§3. The 2-PARITY problem is exponential

As an example of the 'oracle' approach we prove the following proposition of Lovász [80] and Jensen and Korte [80] which is of direct interest to the work of Chapter 4.

Proposition. With respect to the rank oracle the 2-parity problem is exponential.

Proof. Consider the family of polymatroids or more precisely the 2-polymatroids (S,μ) defined by

$$\mu(X) = \begin{cases} 2|X|, & |X| \le t \\ 2t+2, & |X| \ge t+2 \\ \in\{2t+1, \text{ or } 2t+2\} & |X| = t \quad . \end{cases}$$

Then for all possible assignments of the rank μ on t-element sets μ is a polymatroid rank function for $t \ge 1$. Let A be any algorithm based on the rank oracle and apply to the 2-polymatroid (S,μ_0) where

$$\mu_0(X) = \begin{cases} 2|X| & \text{if} \quad |X| \le t \\ 2t+1 & \text{if} \quad |X| = t+1 \\ 2t+2 & \text{if} \quad |X| \ge t+2 \ . \end{cases}$$

We assert that A must ask the oracle for $\mu_0(X)$ for each $X \subseteq S$ which has $|X| = t+1$. For suppose not, then there exists $X_1 \subseteq S$, $|X_1| = t+1$ whose rank $\mu_0(X_1)$ is not probed.

Now consider the 2-polymatroid (S,μ_1) where

$$\mu_1(X) = \begin{cases} 2|X| & \text{if} \quad |X| \le t \\ 2t+1 & \text{if} \quad |X| = t+1,\ X \ne X_1 \\ 2t+2 & \text{if} \quad X = X_1 \text{ or } |X| \ge t+2 \ . \end{cases}$$

Since for all sets X for which the algorithm has asked for $\mu_0(X)$ we have $\mu_0(X) = \mu_1(X)$ the algorithm A must give the same answer to the input polymatroid (S,μ_1) as it does to the input polymatroid (S,μ_0). This is impossible since the maximum size of a matching $\nu(S,\mu_0)$ is t while $\nu(S,\mu_1) = t+1$.

Hence the algorithm must ask for all $\binom{n}{t+1}$ values $\mu_0(X)$, $|X| = t+1$. Thus provided we let

$$\nu = \frac{n-1}{2}$$

we have

$$\binom{n}{\nu+1} > (2-\epsilon)^n$$

for sufficiently large n and this prove the proposition. □

Note: This result contrasts with Lovász's Theorem 4.5.1. However with $|S| = 4$ and $t = 1$, the polymatroid (S,μ_1) above is the Vamos matroid, or more precisely is the set of lines of the Vamos matroid (see §2.3) which is well known not to be representable over any field.

For a more complete treatment of these topics we refer to the recent papers of Robinson and Welsh [80], Jensen and Korte [80] (where very many properties are shown to be exponential) and Hausmann and Korte [80].

6. Seymour's Characterisation of Regular Matroids

§1. Binary and regular matroids

In his fundamental papers, Tutte [58], [59] characterised matroids which are binary, that is representable over the field GF(2) and regular, that is representable over every field by the following theorems.

Theorem 1. A matroid is binary if and only if it has no minor isomorphic to $U_{2,4}$

Theorem 2. A matroid is regular if and only if it has no minor isomorphic to $U_{2,4}$, F_7 or F_7^* .

An easy consequence of Theorem 2 is that M is regular if and only if it is representable over every field. Another characterisation of regular matroids is that they are binary matroids which can also be represented over the reals by the columns of a matrix of the form (I_r,A) where I_r is the unit $r \times r$ matrix and A is an $r \times (n-r)$ totally unimodular matrix (i.e. all its submatrices have determinants in the set $\{0,1,-1\}$).

Well known properties of regular matroids are:

(1) A minor or dual of a regular matroid is regular.

(2) Graphic and cographic matroids are regular.

This last result is especially significant in view of the recent result of P.D. Seymour [80] which characterises regular matroids as those which can be built up by 'sticking together' graphic and cographic matroids and copies of a single matroid on 10 elements (we call it R_{10} and define it later).

Apart from the beauty of Seymour's theorem and the fact that it explains why many theorems about graphs are often extendible to regular matroids, the methods he used to develop this proof, notably splitters are proving to be a major tool in other problems in matroid theory.

§2. Splitters

Before we can properly discuss splitters we need the more familiar notion of a k-separation.

A matroid M(S) has a k-separation for some integer k if there exists $A \subseteq S$, with $|A| \geq k$ and $|S \backslash A| \geq k$ such that

$$r(A) + r(S\backslash A) \leq r(S) + (k-1).$$

Thus a matroid has a 1-separation if and only if it is disconnected or is 1-separable.

If $\mathcal{F}$ is a class of matroids which is closed under the taking of minors we say that $N \in \mathcal{F}$ is a splitter for $\mathcal{F}$ if every $M \in \mathcal{F}$ with a minor isomorphic to N either has a 1 or 2-separation or is isomorphic to N.

The first thing to note is that classes of matroids which have splitters are not easy to find. The existence of a splitter for a class usually seems to mean a fairly significant structure constraint on the class.

For example we can assert:

(1) The class of binary matroids has no splitter.

Proof. Suppose M_0 is a splitter, then there exists a large binary projective space containing M_0 and this is not 2-separable, contradiction.

(2) The class of graphic matroids has no splitter.

Proof. As in (1) with a complete graph taking the place of the projective space.

Probably the first splitter to appear in the literature (though it was not called by this name) is implicit in the proof by Wagner [64] that the truth of Hadwiger's conjecture for the case n = 5 is equivalent to the 4-colour theorem. Let V_8 denote the graph of Figure 1, the Möbius ladder.

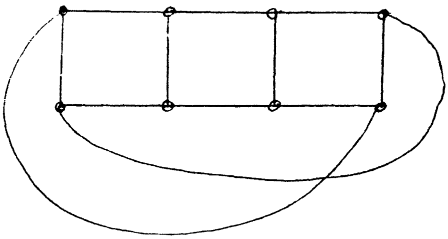


Figure 1

Then

(3) $M(V_8)$ is a splitter for the class of graphic matroids with no minor isomorphic to $M(K_5)$.

Before stating the key proposition in the search for splitters we need one more definition.

If $\mathcal{F}$ is a class of matroids closed under the taking of minors we say $N \in \mathcal{F}$ is compressed in $\mathcal{F}$ if:

(a) N is a geometry, that is, has no loop or parallel elements;

(b) If $M \in \mathcal{F}$ and $M \backslash e = N$ then either e is a loop of M or e is a loop of M* or e is parallel to some other element of M.

In other words a geometry $N \in \mathcal{F}$ is compressed in $\mathcal{F}$ if there is no non-trivial single element extension of N in the class $\mathcal{F}$.

Then we can prove the following proposition which gives us a straightforward method of deciding whether or not N is a splitter for a class of binary matroids.

Theorem 1. Suppose that $\mathcal{F}$ is a class of binary matroids which is closed under the taking of minors and under isomorphism and $N \in \mathcal{F}$. If N is non-null, connected and satisfies:

(i) N is compressed in $\mathcal{F}$,

(ii) N* is compressed in $\mathcal{F}$ *,

(iii) N is not isomorphic to the polygon matroid of the wheel W_n for any $n \geq 3$;

then N is a splitter for $\mathcal{F}$.

The wheel W_n is the graph on n + 1 vertices, n of which form the rim, with the remaining vertex (the centre) joined to each of the rim vertices.

We illustrate the use of Theorem 1 by showing how it gives us a very important splitter.

(4) F_7^* is a splitter for the class of binary matroids which have no minor isomorphic to F_7.

Proof. F_7^* is certainly non-null and connected. It is a geometry, and will therefore be compressed in Ex (F_7) if we can show that if $M \in$ Ex (F_7) and $M \backslash e = F_7^*$ then e is either a loop of M or of M* or e is parallel to some other element of M. But this is proved by brute force checking all possible binary single element extensions of F_7^*. In exactly the same way we can show $(F_7^*)^* = F_7$ is compressed in Ex (F_7^*) and since F_7^* is certainly not a wheel (4) follows from Theorem 1. □

The reader may well puzzle over the significance of the 'wheel condition (iii)' in Theorem 1. The explanation is that without it the proposition fails, for example if $\mathcal{F}$ is the finite class of minors of W_{n+1} then W_n satisfies the conditions (i) and (ii) but W_{n+1} is not 2-separable.

Although most of the applications of splitters to date have been within the class of binary matroids we should note that Theorem 1 can be extended to non-binary matroids as follows.

Theorem 2. If $\mathcal{F}$ is a class of matroids, closed under minors, and under isomorphism and $N \in \mathcal{F}$ is non-null, connected and satisfies in addition to the conditions (i), (ii) and (iii) of Theorem 1 the additional condition:

(iv) N is not isomorphic to the whirl $\mathcal{W}_n$ for $n \geq 3$; then N is a splitter for $\mathcal{F}$.

The whirl $\mathcal{W}_n$ is defined as follows. Consider the wheel W_n, it is a graph on 2n edges. If the edges are labelled in such a way as to make $\{1,2,\ldots,n\}$ the rim (or outer circuit) then $\mathcal{W}_n$ is the non-binary matroid whose independent sets are exactly the independent sets of W_n except that in $\mathcal{W}_n$, $\{1,2,\ldots,n\}$ is not a circuit but an independent set. Wheels and whirls were first studied by Tutte [66] who showed that if M on S is a matroid which is not 2-separable and is not isomorphic to a wheel or a whirl then for some $p \in S$, $M\backslash p$ or M/p is not 2-separable.

§3. The decomposition theorem

A very interesting regular matroid is the following 10-element matroid, which we call R_{10} and which first occurred in the work of Bixby [77].

It is the matroid consisting of the 10 5-vectors over GF(2) each of which have exactly 3 non-zero entries.

The following properties are routine to check.

(1) R_{10} is regular, self-dual but is not graphic or cographic and for any $e \in R_{10}$, $R_{10} \backslash e = K_{3,3}$, $R_{10}/e = K^*_{3,3}$.

More important is the following property

(2) R_{10} is a splitter for the class of regular matroids.

Proof. Tedious checking of one-element extensions of R_{10} and then using Theorem 2.1. □

Now this means that every regular matroid with an R_{10} minor is 2-separable, except R_{10} itself. Hence we may ask, where are highly connected regular matroids to be found? They certainly exist, for example graphic and cographic matroids are regular and can be arbitrarily highly connected. Seymour's main theorem essentially says that these graphic and cographic matroids together with R_{10} are the only 4-connected regular matroids.

Before giving Seymour's result we need one last set of definitions.

If M_1, M_2 are binary matroids on S_1 and S_2 respectively we define $M_1 \Delta M_2$ to be the matroid on the symmetric difference $S_1 \Delta S_2$ which has as its set of cycles all subsets of $S_1 \Delta S_2$ of the form $C_1 \Delta C_2$ where C_i is a cycle of M_i. (A cycle of a matroid is a union of disjoint circuits.)

(3) When $S_1 \cap S_2 = \emptyset$ and $|S_1|, |S_2| < |S_1 \Delta S_2|$, we call $M_1 \Delta M_2$ a 1-sum.

(4) When $S_1 \cap S_2 = \{z\}$ say and z is not a loop or coloop of M_1 or M_2 and $|S_1|, |S_2| < |S_1 \Delta S_2|$, we say $M_1 \Delta M_2$ is a 2-sum of M_1 and M_2.

(5) When $|S_1 \cap S_2| = 3$ and $S_1 \cap S_2 = C$ say where C is a circuit of both M_1 and M_2 and $|S_1|, |S_2| < |S_1 \Delta S_2|$ then we say $M_1 \Delta M_2$ is a 3-sum of M_1 and M_2.

In each case we call M_1 and M_2 the parts of the sum.

Now a 1-sum is just the usual direct sum, the 2-sum and 3-sums are the matroid operations corresponding to 'sticking' two graphs together by an edge or triangle respectively and then deleting the edge or triangle in question. In either case if we have a matroid M which is the 2 or 3 sum of other matroids, then we have a convenient way of breaking it up into these smaller structure.

More precisely, in the language of Brylawski [76] we form the generalised parallel connection of M_1, M_2 and then delete the modular flat 'across which' we are joining M_1 and M_2.

Seymour's decomposition theorem can now be stated:

Theorem 1. *If* M *is a regular matroid it is the* 1,2 *or* 3 *sum of graphic matroids, cographic matroids, and copies of the* 10 *element matroid* R_{10}.

The full proof of this theorem is difficult and long, (94 pages of typescript!) However we attempt to give the main ideas below.

First we introduce yet another very special regular matroid which we call R_{12}. It is the matroid induced by linear independence over GF(2) cn the columns of the following matrix.

$$\begin{bmatrix} 1 & & & & & & 1 & 1 & 1 & 0 & 0 & 0 \\ & 1 & & 0 & & & 1 & 1 & 0 & 1 & 0 & 0 \\ & & 1 & & & & 1 & 0 & 0 & 0 & 1 & 0 \\ & & & 1 & & & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & & & & 1 & & 0 & 0 & 1 & 0 & 1 & 1 \\ & & & & & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

R_{12} is regular, is isomorphic but not equal to R^*_{12}, and does not contain R_{10} as a minor. It can be alternatively defined as the matroid obtained by taking the 3-sum across the edges a,b,c of the cycle matroid of $K_5\backslash e$ of Figure 2

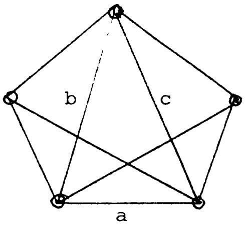


Figure 2

with a copy of $M^*(K_{3,3})$ in which a,b,c are any three elements of $K_{3,3}$ which form a triad of edges having a common end point.

Throughout, great use is made of the following decómposition lemmas, which are surprisingly awkward to prove.

(6) If M is binary the following are equivalent

(a) M is 1, or 2-separable or has a 3-separation (X_1,X_2) with $|X_1|$, $|X_2| \geq 4$

(b) M is expressible as a 1,2 or 3 sum of smaller matroids.

(7) If M is binary and M is the 3-sum of M_1 and M_2 then if M has no 2-separation, M_1 and M_2 are both isomorphic to minors of M.

The key steps in Seymour's proof can now be stated.

(8) Every regular matroid which is 3-connected and which is neither graphic nor cographic has R_{10} or R_{12} as a minor.

(9) If M is regular and $M > R_{12}$ then M has a 3 separation (X_1,X_2) with $|X_i| \geq 6$.

(10) Every regular matroid with a minor isomorphic to R_{12} is expressible as the 1,2 or 3 sum of matroids in the class $Ex(F_7,F_7^*,R_{12})$.

This is really the crux of the whole proof since it essentially says that a regular matroid which has connectivity ≥ 4 cannot have R_{12} as a minor and hence by (8) is either graphic or cographic or has R_{10} as a minor. But now, by the splitter theorem (2) we know that if it has R_{10} as a minor it is 2-separable and we can look at the parts of the 2-separation and use inductive arguments.

§4. A polynomial algorithm to test whether a matrix is totally unimodular

An important and immediate practical consequence of Seymour's decomposition theorem is that it leads to an efficient polynomial algorithm for testing whether or not an matrix A with entries from the set {-1,0,1} is totally unimodular, that is is there a square submatrix of A whose determinant is not in the set {-1,0,1}?

This question was one of the outstanding open problems in computational complexity, see for example Garey and Johnson [79, p. 228]. Its importance lies in the fact that at the heart of many of the integer programming problems which can be solved in polynomial time is a totally unimodular matrix. For example the trivial observation that if in a linear programming problem we have a totally unimodular matrix means in all thc divisions used when using the simplex method we shall be dividing by 1 and hence will not be moving outside the class of integers.

Theorem 1. There exists a polynomial algorithm for deciding whether or not an $m \times n$ matrix with entries from $\{0,1,-1\}$ is totally unimodular.

This follows almost immediately from Seymour's decomposition theorem with a result of Cunningham and Edmonds [80] which gives a fast (that is polynomial) algorithm for deciding whether or not a matroid is k-connected for any fixed integer k. We have described such an algorithm in §3.4.

Roughly speaking the algorithm works as follows:

Given a binary matroid M test if it is 1, 2 or 3 separable. If not then it is regular if and only if either (a) M is graphic or (b) M is cographic or (c) M is R_{10} .

Possibilities (a) and (b) can then be checked by an algorithm of Tutte [60] (in case (b) applied to M*). Possiblity (c) is trivial to check.

When M has a 1, 2 or 3 separation then we examine the parts and recursively apply the above procedure. It is not difficult to see that since the individual subroutines are polynomial the whole programme can be completed in polynomial time.

7. Colouring, Flows and Blocking Problems

§1. The blocking problem

In this lecture we relate the fundamental graph colouring problem with the less well known problem of deciding which graphs support flows taking values in various abelian groups and then relate both (via matroid theory) with a blocking problem in projective spaces which goes back at least as far as Veblen (1912).

As we shall see the splitter·theory developed in the last chapter enables us to reduce this last, apparently intractible geometry problem to a conjecture about graphs which on the surface at least offers much more hope.

Consider the projective space PG(r,q). For any positive integer t, a t-block is a set X of points in this space such that $X \cap F \neq \emptyset$ for each flat F of rank r - t. In particular the 1-blocks are the sets which have non-empty intersection with every hyperplane of PG(r,q). It is therefore obvious that if X is a t-block and $Y \supseteq X$ then Y is a t-block. X is a minimal t-block if it is a t-block but X\p is not a t-block for each $p \in X$.

Standard vector space arguments give:

(1) The projective space PG(t,q) is a minimal t-block over the field GF(q) for each integer $t \geq 2$ and each prime power q.

For example PG(2,2) is a 2-block over GF(2) and is a 1-block over GF(4). More generally we have:

(2) A t-block over GF(p} is a 1-block over GF(p^t) for each positive integer t.

The converse is not always true, there exist 1-blocks over GF(p^t) which when regarded as geometrical configurations are not representable (that is coordinatisable) over GF(p). However we can show:

(3) If a 1-block over GF(p^t) is representable over GF(p) then it is a t-block over GF(p).

Matroids and the Blocking Problem

Suppose that M is a matroid on S with rank function ρ. Its chromatic polynomial P(M;λ) defined by

$$P(M;\lambda) = \sum_{A\subseteq S} (-1)^{|A|} \lambda^{\rho S-\rho A}$$

is a well known Tutte-Grothendieck invariant (see the Lectures in this volume by T.H. Brylawski).

The relationship between blocking and the chromatic polynomial is contained in the following remarkable theorem.

Theorem 1: Suppose that M is a matroid of rank r on S and that M is embeddable in V(r,q), then there exists an r - t subspace F of V(r,q) such that $F \cap S = \emptyset$ if and only if $P(M;q^t) > 0$.

The first point to notice about Theorem 1 is that its conclusion does not depend on the embedding, but says that for any embedding such a subspace exists. In fact, the full version of Theorem 1 proved by Crapo and Rota [70] shows that $P(M;q^t)$ enumerates the collections of hyperplanes whose intersection is a flat of the type required.

The relationship with blocking is now obvious.

(4) A matroid M which is representable over GF(q) is a t-block over GF(q) if and only if $P(M;q^t) = 0$.

The statement (4) illustrates precisely the slight abuse of language in the statement "M is a t-block". What we mean is, any of the various vector representations of M in V(r,q) is a t-block. In other words it is not their coordinatisation in V(r,q) which is important but their geometrical structure.

Example 1: If F_7 is the Fano matroid consisting of the 7 non-zero vectors of V(3,2),

$$P(F_7;\lambda) = (\lambda-1)(\lambda-2)(\lambda-4).$$

Example 2: More generally the projective geometry M = PG(r,q) has chromatic polynomial

$$P(M;\lambda) = \prod_{\tau=0}^{r} (\lambda-q^{\tau}).$$

Example 3: If K_n is the complete graph on n vertices then its cycle matroid $M(K_n)$ has chromatic polynomial

$$(\lambda-1)(\lambda-2)\ldots(\lambda-n+1).$$

Example 4: If $U_{2,n}$ denotes the matroid of rank 2 on n points in which every 2-set is independent, in other words the n point line, then its chromatic polynomial is

$$P(U_{2,n};\lambda) = \lambda^2 - n\lambda + (n-1).$$

Thus by evaluating their respective chromatic polynomials at appropriate values we have

(5) The (q+1)-point line (see Example 4) is a 1-block over the field GF(q).

(6) The Fano matroid F_7 is a 2-block over GF(2).

(7) For any prime power q, the cycle matroid $M(K_{q+1})$ is a 1-block over GF(q), and thus if $q = p^t$ it is also a t-block over GF(p).

§2. Colouring graphs

The relationship between the chromatic polynomial of a matroid and graph colouring is straightforward. If G is a graph its chromatic polynomial $P(G;\lambda)$ is that function of λ which when evaluated at $\lambda = n$ for any non-negative integer n gives the number of proper colourings of the vertices of G using n or fewer colours. A proper colouring of G is a colouring of the vertices in which no two vertices which are adjacent in G have the same colour. For example it is easy to check that

$$P(K_t;\lambda) = \lambda(\lambda-1)\ldots(\lambda-t+1).$$

If G is a connected graph it is shown in Welsh [76, Chapter 16] that

(1) $P(G;\lambda) = \lambda\, P(M(G);\lambda)$

and thus the chromatic number $\chi(G)$ of the graph G, the smallest integer n for which G has an n colouring is given by

$$\chi(G) = \inf_{n \in Z^+} n : P(M(G);n) > 0.$$

Now every graph G has a cycle matroid M(G) which is representable over every field. Hence:

(2) A graph G is such that M(G) is a t-block over GF(q) if and only if it has a chromatic number $\chi(G) > q^t$.

Thus the graphic 1-blocks over GF(2) are the cycle matroids of non-bipartite graphs.

In fact Tutte [66a] proves:

(3) M is a minimal 1-block over GF(2) iff M is the cycle matroid of an odd circuit.

When we come to 2-blocks over GF(2) however, the situation is much more complicated. Since K_5 is a minimal graph which is not 4-colourable we have:

(4) $M(K_5)$ is a minimal 2-block.

However, there are many others, for clearly any graph G which is not 4-colourable but is such that $G \backslash e$ is 4-colourable for every edge e, is going to have a cycle matroid which is a minimal 2-block. Such graphs are called edge-critical and an infinite family of them can easily be constructed see for example Ore [67].

However as we shall see if we consider only those graphs G such that G is not 4-colourable but every sub-contraction of G is 4-colourable then the situation changes.

§3. Flows taking values in an abelian group

If D is a directed graph and H is a finite abelian group, an H-flow on D is a map $\phi : E(G) \to H \backslash \{0\}$ such that for each vertex v of D

$$\sum_{e \in \delta^+(v)} \phi(e) - \sum_{e \in \delta^-(v)} \phi(e) = 0 \bmod H,$$

where $\delta^+(v)$ denotes the set of edges directed out of v and $\delta^-(v)$ denotes the set of edges directed into v. In other words an H-flow on D is a flow in the usual sense, that is satisfying Kirchoff's laws at each vertex, with the two provisos a) that arithmetic is in the group H and b) no edge is allowed to have a zero flow. This is often called a nowhere zero flow in the literature.

If there exists some H-flow on D we say that D supports an H-flow.

W.T. Tutte in 1954 asked the question: what flows can graphs accommodate? As we shall see, there are some surprising and beautiful answers.

First note that if D can support an H-flow and D' is any digraph which is obtainable from D by reorientation of some edges,then D' can support an H-flow. In other words for a given group H, whether or not a digraph D supports an H-flow only depends graphically on the structure of the underlying graph G(D) obtained from D by removing the directions on the edges. Thus, henceforth we speak of an undirected graph G supporting an H-flow to mean that in any orientation of G, an H-flow is possible.

Secondly, and this is a very nice application of Tutte-Grothendieck theory we have the following theorem:

Theorem 1. The number of H-flows on a graph G depends only on the order of the group H and is given by evaluating the chromatic polynomial of the cocycle matroid M*(G) at $\lambda = O(H)$, the order of the group H.

Proof. Straightforward application of contraction-deletion, see the lectures by T.H. Brylawski in this volume.

Example. Consider H-flows on any directed version of K_4. $M^*(K_4)$ has chromatic polynomial $(\lambda-1)(\lambda-2)(\lambda-3)$. Hence the number of $Z_2 \times Z_2$ flows on K_4 is 3.2.1 = 6.

Thus we may sensibly speak of a graph having a k-flow to mean that for any orientation of G and any abelian group H of order k there exists an H-flow on G. Moreover, and this is most crucial, we can decide whether or not a particular graph supports a k-flow by calculating the chromatic polynomial of its cocycle matroid and then evaluating this polynomial at $\lambda = k$.

As a first consequence of Theorem 1 we have the following result:

(2) Any planar graph G without bridges has a 4-flow.

Proof. This statement follows from the Four Colour Theorem of Appel and Haken [76]. To see this, we note that if G is planar and bridgeless there exists a (dual) graph G* which is planar and loop free and M*(G) = M(G*). Hence

$$P(M^*(G);4) = P(M(G^*);4)$$

and by the 4-colour theorem and (6.1) we know

$$P(M(G^*);4) > 0$$

since G* is planar. □

In his fundamental paper in 1954, W.T. Tutte made two conjectures. The first, that there exist some integer n such that any bridgeless graph G has an n-flow, was settled by Jaeger [76] who showed that any bridgeless graph G had an 8-flow. This very nice result has just been improved by Seymour [80] who has proved

Theorem 2. Every bridgeless graph has a 6-flow.

The second conjecture of Tutte [54] is still unsettled, and is known as his 5-flow conjecture; it can be stated as follows:

Tutte's 5-flow Conjecture: Every bridgeless graph has a 5-flow.

To see that this conjecture, if true, is best possible consider the Petersen graph P_{10} shown in Figure 1.

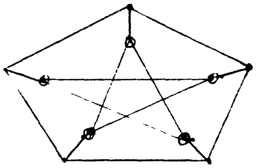


Figure 1 The Petersen graph P_{10}

It is non-trivial to verify that P_{10} has no k-flow for $k \leq 4$ and that it is the smallest graph with this property.

Alternatively, the reader can (with sufficient patience) show that $P(M^*(P_{10});\lambda) = (\lambda-1)(\lambda-2)(\lambda-3)(\lambda-4)(\lambda^2-5\lambda+10)$ and thus P_{10} has no 4-flow.

Now when every vertex v of G has degree 3, that is G is cubic, it is not difficult to see that provided G is bridgeless, G has a 4-flow if and only if the edges of G are colourable in 3-colours so that no two incident edges have the same colour. In other words:

(4) A cubic bridgeless graph G has a 4-flow if and only if it is 3-edge colourable.

Using this, a second conjecture of Tutte [69] can be formulated as:

Tutte's 4-flow Conjecture. A cubic bridgeless graph G has a 4-flow if it has no subgraph contractible to the Petersen graph P_{10}.

A stronger version of this conjecture is implicit in Tutte [66]

Tutte's 4-flow Conjecture - (Strong Version). A bridgeless graph has a 4-flow if it has no subgraph contractible to P_{10}.

It seems surprisingly difficult to show that these two versions of Tutte's 4-flow conjecture are equivalent.

§4. Tangential Blocks

We return now to the original geometrical problem of Tutte [66], namely finding the minimal 2-blocks over GF(2).

Examples of minimal 2-blocks which we have already found are:

(a) the 7 point matroid of rank 3, F_7,

(b) the 10 point matroid of rank 4, K_5,

(c) the 15 point matroid of rank 6, P^*_{10} .

From these it is possible to construct other minimal 2-blocks by "sticking them together" in a non-trivial fashion.

This is because of the observation of Oxley [79] that if M,N are two minimal k-blocks then their series connection is also a minimal k-block. (The series connection is the matroid operation corresponding to the graph operation of Hajös union). Continuing this analogy with graph theory we see that as mentioned earlier, any edge critical 5-chromatic graph has a polygon matroid which forms a minimal 2-block. However each of the matroids of K_5, F_7 and P^*_{10} has the additional property that no minor of them is also a 2-block. A 2-block with this property is called a tangential 2-block. This is not Tutte's original definition but can be seen to be equivalent to it see Welsh [79]. In 1966 Tutte proved that these three matroids were the only tangential 2-blocks of rank ≤6. In 1976, Datta proved by a complicated geometrical argument that there is no tangential 2-block of rank 7.

Tutte's tangential 2-block conjecture, originally made in (1966) and still unsettled, can be stated in the following form:

Tutte's tangential block conjecture: The only tangential 2-blocks are F_7, K_5 and P^*_{10} .

Seymour's theory of splitters is a major step towards proving this conjecture. First consider Hadwiger's conjecture which in its full form asserts

Conjecture. (Hadwiger) If a loopless graph G is not n-colourable it contains K_{n+1} as a subcontraction.

Dirac [52] showed that it was true for n = 3 and Wagner [64] showed that for n = 4 it was equivalent to the 4-colour conjecture. Therefore it holds for n = 4. Thus we know that there can be no new tangential 2-block which is the cycle matroid of a graph. Seymour [80] uses his characterisation of regular matroids to prove the following striking result:

Theorem 1. Any new tangential 2-block must be the cocycle matroid of a graph.

In other words, Seymour's result shows that Tutte's tangential 2-block conjecture is exactly equivalent to the strong form of the 4-flow conjecture. Thus he has reduced this seemingly intractable geometrical problem to the conceptually much simpler problem of characterising those graphs which have no 4-flow. More precisely, there exists a tangential 2-block other than F_7,$M(K_5)$ and $M^*(P_{10})$ if and only if there is a bridgeless graph G not containing a sub-graph contractible to P_{10} which has no 4-flow.

Sketch proof of Theorem 1. First consider a tangential 2-block M which is not K_5, F_7 or P^*_{10} (we use K_5 for $M^*(K_5)$, P^*_{10} for $M^*(P_{10})$. If it were graphic there would exist a graph G which was not contractible to K_5 but which was not 4-colourable. This would contradict Hadwiger's conjecture for the case n = 5, which by Wagner's theorem showing the equivalence of Hadwiger's 5-chromatic conjecture with the 4-colour theorem of Appel and Haken, we know to be true. Hence the only tangential 2-block which is graphic is K_5. Now consider the existence of a non-regular tangential 2-block M_0. Since M_0 is not regular it must contain either F_7 or F^*_7 as a minor. But because F_7 is a tangential 2-block, by minimality, this minor must be F^*_7. Hence since F^*_7 is a splitter for binary matroids with no F_7 minor we know that either $M_0 = F^*_7$ or M_0 has a 2-separation. It is not difficult to show that a tangential 2-block cannot have a 2-separation. Hence, $M_0 = F^*_7$. But $\chi(F^*_7) = 2$ and hence F^*_7 is not a tangential 2-block. So we have shown that there are no non-regular tangential 2-blocks. It remains to show that there exists no tangential block which is regular but neither graphic nor cographic.

Suppose such a matroid M exists. Then by the decomposition theorem it must be possible to express M as a 1,2 or 3 sum of graphic or cographic matroids or copies of R_{10}. An induction argument shows that this is impossible unless M is cographic and hence the only tangential blocks which are not cographic are F_7 and K_5. □

§5. A problem on the Desargues Configuration

The conjectures and problems posed so far seem to be hard, at least in the sense that they have stood the test of time. We close this lecture with new conjectures which may be easier to settle in the negative but which if true would imply or further relate some of the earlier conjectures. The first is a much stronger form of Tutte's 5-flow conjecture -

Conjecture 1. If M is binary and has no minor isomorphic to the 3-dimensional Desargues configuration, then $\chi(M) \leq 5$.

Note: we have presented this conjecture in its geometrical form; the reader will quickly realise that the 3-dimensional Desargues configuration is as a matroid identical with $M(K_5)$.

The motivation for this conjecture is a recent paper by Walton and Welsh [80] in which it is shown that if M satisfies the conditions of the conjecture and also has no minor isomorphic to PG(2,2) then $\chi(M) \leq 6$ and that if Tutte's 5-flow conjecture is true 6 can be replaced by 5.

Other problems of this sort are contained in Welsh [80]. Possibly easier to settle is the weaker form of Conjecture 1.

Conjecture 2. If $M \in Ex(K_5)$ then there exists t, independent of M, such that $\chi(M) \leq t$.

8. Flows in Matroids

§1. The max-flow min-cut theorem

Many problems in discrete optimisation can be formulated in terms of finding maximum flows in capacity constrained networks. A comprehensive account of the theory and its applications is given by Ford and Fulkerson (1962). In this chapter we extend these ideas to matroids and get some intriguing results which could be viewed as bridging a gap between the applied theory of flows and finite geometry.

Consider an undirected graph G and two distinguished vertices u,v, to be called the source and sink respectively; $c_i \geq 0$ is the capacity of the edge e_i and represents the amount of flow which it can support. Finding the maximum feasible flow from u to v in the capacitated graph can be found by a well known polynomial method, known as the 'max flow min cut' algorithm.

In order to consider the problem as a matroid problem we insert an additional distinguished edge e joining the vertices u,v. Let $C_1,\dots,C_p$ be the circuits of the matroid M(G) which contain the edge e. The value of the maximum flow from u to v is the maximum value of $u_1+\dots+u_p$ subject to the conditions that the flow along e_i is not more than c_i and where $u_i \geq 0$ represents the flow or circulation around the circuit C_i.

We can now formulate the maximum flow problem for matroids as follows. Let e be a distinguished element of matroid M on $S = \{e,e_1,\dots,e_n\}$

and let $C_1,\dots,C_p$ be the circuits of M which contain e. Let $c_i \geq 0$ $(1 \leq i \leq n)$ be the capacity of e_i. Let the $n \times p$ matrix $A = (a_{ij})$ be defined as

$$a_{ij} = \begin{cases} 1 & e_i \in C_j , \\ 0 & e_i \notin C_j . \end{cases}$$

A feasible e-flow in M is a vector $\underline{u} = (u_1,\dots,u_p)$ satisfying

$$(1) \quad \sum_{j=1}^{p} a_{ij} u_j \leq c_i \quad (1 \leq i \leq n) , \qquad u_i \geq 0 ,$$

and $\underline{u} = (u_1,\dots,u_p)$ is a maximum e-flow if it maximises $\Sigma\, u_i$ subject to the constraints (1). Σu_i is then called the value of the maximum e-flow.

Now let C* be any cocircuit of M which contains e. We define its capacity, C(C*), by

$$C(C^*) = \Sigma\{c_i : i, e_i \in C^*\} .$$

The matroid M has the max flow min cut (MFMC) property if for any element e which is not a loop and any set of real capacities $c_i \geq 0$, the maximum value of an e-flow equals min C(C*) where the minimum is taken over all cocircuits C* containing e. We call this minimum the min capacity of e. It is easy to prove (see Welsh [76], chapter 19) the following:

(2) In any matroid the maximum value of an e-flow is less than or equal to the min capacity of e.

For general matroids not much more can be said since it is easy to find examples where the maximum e-flow has a value strictly less than the min capacity. For regular matroids however, we can say more.

(3) In any regular matroid the maximum value of an e-flow equals the min capacity of e.

If M is a matroid on $S \cup e$ we say that (M,e) has the integer max flow min cut property (Z^+ - MFMC) property if when the capacities c_i are restricted to being non-negative integers there exists a non-negative integer flow $(u_1, \ldots, u_p)$ which equals the min capacity of e.

A matroid M has the integer max flow min cut property if (M,e) has the (Z^+ - MFMC) property $\forall$ e. It is obvious that

(4) If M has the Z^+ - MFMC property then M has the (MFMC)-property.

Gallai [59] and Minty [66] independently proved:

(5) Regular matroids have the integer max flow min cut property.

However (5) is not best possible since it is easy to check that F_7 also has the Z^+ - MFMC property. Seymour [77] completely wrapped up the problem by proving:

Theorem 1. Let M be a connected matroid. Then M has the integer max flow min cut property if and only if M is binary and has no minor isomorphic to F_7^*.

The original proof of this was very involved, we now show how the theory of splitters simplifies the proof enormously.

Proof. First we let the reader check that the class $\mathfrak{F}$ of matroids with the (Z^+ - MFMC)-property is closed under the taking of minors- this is straightforward.

Secondly it is easy to verify that neither $U_{2,4}$ nor F_7^* have the (Z^+-MFMC)-property. Hence $\mathfrak{F}$ must contain only binary matroids.

Thirdly it is easy to see that $M \in \mathfrak{F}$ if and only if it belongs to the class $\mathfrak{F}_0$ defined by $M \in \mathfrak{F}_0$ if and only if it has the following apparently weaker property.

For $w : S\backslash e \to \mathbb{Z}^+$ and $k \in \mathbb{Z}^+$ suppose that each cocircuit D containing e satisfies

$$w(D\backslash e) = \sum_{a \in D\backslash e} w(a) \geq k \quad .$$

Then there exists k circuits of M, each containing e, but no more than w(p) containing any other element $p \in S$.

We need to prove $Ex(F_7^*) = \mathcal{F}_0$.

(a) Suppose $M \in \mathcal{F}_0$, then $F_7^* \not< M$ for we know every minor of M also belongs to $\mathcal{F}_0$ and $F_7^* \notin \mathcal{F}_0$. Hence $\mathcal{F}_0 \subseteq EX(F_7^*)$.

(b) Suppose $M \in Ex(F_7^*)$ but $M \notin \mathcal{F}_0$. By the Gallai-Minty result we know M cannot be regular. Hence $M > F_7$ or F_7^*. But $M \not> F_7^*$, so $M > F_7$. But F_7 is a splitter for $EX(F_7^*)$, thus either $M = F_7$ or M is 2-separable. But $F_7 \in \mathcal{F}_0$ (simple checking). Thus M is 1 or 2-separable. But now fairly straightforward arguments show that if parts of a 1 or 2 separation both belong to $\mathcal{F}_0$ then the 1 or 2 sum of the parts must also belong to $\mathcal{F}_0$. Hence induction on $|S|$ shows that $M > F_7^*$, and this contradiction completes the proof. □

Note. It is interesting that the above proof uses splitters together with the Gallai-Minty theorem that the result holds for regular matroids. It is somewhat surprising that we cannot get a direct proof by the following argument. The Ford-Fulkerson theorem says that graphic matroids belong to $\mathcal{F}_0$; it is easy to prove that cographic matroids belong to $\mathcal{F}_0$; it is routine to check that $R_{10} \in \mathcal{F}_0$. Hence if we could prove that belonging to $\mathcal{F}_0$ was preserved under 1, 2 and 3-sums we would have a proof that regular matroids also belonged to $\mathcal{F}_0$. However it is not true that membership of $\mathcal{F}_0$ is preserved under 3-sums!

Example. Take the 3-sum of K_4 and F_7. Both have the Z+-MFMC property but their 3-sum is F_7^*!

§2. Multicommodity flows

If instead of just one source and one sink we have k pairs of distinct vertices, (u_1,v_1), $(1 \le i \le k)$, where u_i is a source of commodity i destined for the sink v_i, and c_j the capacity of the edge e_j is an upper bound on the total amount of matroid that the edge e_j can accommodate we have what is known as the multicommodity flow problem. It is an obvious generalisation of the problem: how many edge disjoint paths $u_1 \to v_1, \ldots,$ $u_k \to v_k$ can be drawn in a graph G? The case k = 1 is of course just the max flow problem.

2-commodity flow

Let $\mathbb{P} = \mathbb{P}_k$ be the edge sets of all minimal paths $P_1,\ldots,P_t$ which join u_1 to v_i $(1 \le i \le k)$. Let $\nu(\mathbb{P})$ be the maximum number of edge disjoint member of $\mathbb{P}$ and let $\mathbb{P}^*$ be the blocker of $\mathbb{P}$, that is $\mathbb{P}^* = \{X : X \subseteq E(G),$ $X \cap P_i \ne \phi \;\forall\, i, 1 \le i \le t$, and X is a minimal set with this property$\}$.
It is obvious that

(1) $\nu(\mathbb{P}) \le \min|D| : D \in \mathbb{P}^*$.

The max flow min cut theorem of Ford and Fulkerson says that equality holds in (1) when k = 1.

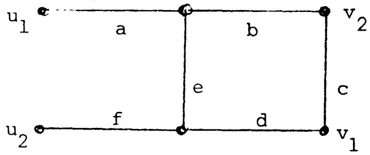
More generally, if $\mathcal{L}$ is any clutter, that is a family of sets $\{X : X,Y \in \mathcal{L} \Rightarrow X \not\subseteq Y\}$, and $\mathcal{L}^*$ is its blocking clutter, $\mathcal{L}$ is said to be Mengerian if

$$\nu(\mathcal{L}) = \min\{|D| : D \in \mathcal{L}^*\} ,$$

and thus the max flow min cut theorem essentially says that when k = 1, $\mathbb{P}_k$ is a Mengerian clutter.

For k = 2, however this is false.

Examplel. Let G be as shown,



$\mathbb{P}_2$ = {a,b,c}, {a,d,e}, {b,e,f}, {c,d,f},

$\nu(\mathbb{P}_2) = 1$,

but the minimum cardinality of a blocker of $\mathbb{P}_2$ is 2.

Nevertheless we do have the following:

Theorem 1. (2-commodity flow theorem). Let G be an undirected graph and let u_1, u_2, v_1, v_2 be vertices of G. Let $c : E \to Q^+$ be a capacity function and let ϕ_i be a flow from u_i to v_i, $1 \le i \le 2$. Then the maximum value of $\phi_1 + \phi_2$ such that

$$\phi_1(e) + \phi_2(e) \le c(e) \qquad (e \in E(G))$$

equals the minimum capacity of a cut which disconnects u_1 from v_1 and u_2 from v_2 .

This results, originally proved by Hu [63] by a very long and involved argument now has a very short elegant proof by Seymour [78].

We illustrate the theorem by considering the graph G_0 of Example 1. Assign capacity c(e) = 1 to each edge. Then Figure 2 shows an assignment of (non-integer) flows to the edges of G, the first component contributes to a ϕ_1-flow and the second to a ϕ_2-flow.

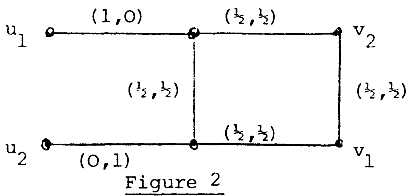


Figure 2

§3. Multicommodity flows in matroids

We can now extend the ideas of multicommodity flows in graphs to matroids exactly analogously to the way we extended the single commodity problem.

For each source sink pair u_i, v_i we introduce a new special edge e_i and let the collection of special edges $\{e_1, \ldots, e_k\} = F$. To each edge $e_i \in F$ we assign a demand $d_i = d(e_i)$ which represents the amount of commodity i we wish to transport from u_i to v_i.

To each edge $e \in E(G) \backslash F$ we assign a capacity c(e) which is the maximum amount of flow which that edge can accommodate. With this interpretation we can now define an (F,c,d)-flow for an arbitrary matroid M on S as follows.

Let $\mathcal{C}_F$ be the collection of circuits C such that $|C \cap F| = 1$, in other words $\mathcal{C}_F$ can be regarded as the analogues of 'paths through F'.

Then a map $\psi : \mathcal{C}_F \to \mathbb{R}^+$ is an (F,c,d)-flow if

$$\sum_{e \in C \in \mathcal{C}_F} \psi(C) \geq d(e) \quad \text{if} \quad (e \in F),$$

$$\sum_{e \in C \in \mathcal{C}_F} \psi(C) \leq c(e) \quad \text{if} \quad e \notin F.$$

Proposition 1. If M has a p-flow through F with p = (c,d) then for each cocircuit C* of M

$$d(C^* \cap F) \leq c(C^* \backslash F) .$$

Proof. Let ϕ be such a flow. If C is any circuit of M we know $|C \cap C^*| \neq 1$ and so if $C \cap F = \{f\}$

$$|C^* \cap f| \leq |C^* \backslash (C \backslash f)|,$$

which means $|C \cap C^* \cap F| \leq |C \cap (C^* \backslash F)|$.

Now by hypothesis

$$\sum_{C \in \mathcal{C}_F} \phi(C) \geq d(e) \qquad e \in F,$$

$$\sum_{C \in \mathcal{C}_F} \phi(C) \leq c(e) \qquad e \in E \backslash F,$$

where in both cases the left hand sums are over those C containing e. Hence

$$\begin{aligned} d(C^* \cap F) &= \sum_{e \in C^* \cap F} d(e) \\ &\leq \sum_{e \in C^* \cap F} \Big(\sum_{e \in C \in \mathcal{C}_F'} \phi(C)\Big) \\ &= \sum_{C \in \mathcal{C}_F} \sum_{e \in c^* \cap C \cap F} \phi(C) \\ &= \sum_{C \in \mathcal{C}_F} \phi(C) \, |C^* \cap C \cap F|. \end{aligned}$$

Similarly $c(C^* \backslash F) \geq \sum_{C \in \mathcal{C}_F} \phi(C) \, |C \cap (C^* \backslash F)|$ and the result follows.

Example. (2.1 revisited). Consider the corresponding matroid - insert special edges e_1, e_2 joining (u_1, v_1) and (u_2, v_2) respectively. We find that G_0 together with these edges is essentially the graph K_4, see Figure 1 below.

This gives an example in which $|F| = 2$, $F = \{e_1, e_2\}$ and in which the converse of Proposition 1 fails if we restrict attention to the integers though it is in fact true over the rationals and (a fortiori) over the reals.

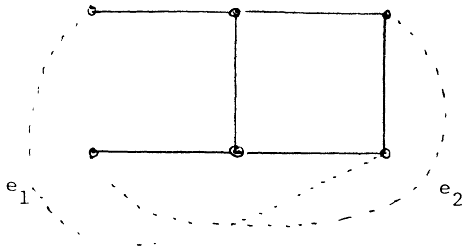


Figure 1

Accordingly we say M is F-flowing over $\mathbb{Z}^+(\mathbb{R}^+)$ if for all $p \in \mathbb{Z}^+(\mathbb{R}^+)$

$$c(C^*\backslash F) \geq d(C^* \cap F) \quad \forall C^*$$

$\Rightarrow$ the existence of an F-flow with values in $Z^+(\mathbb{R}^+)$.

We go further and describe M as k-flowing over $\mathbb{Z}^+$ (or over $\mathbb{R}^+$) if M is F-flowing over $\mathbb{Z}^+$ (or over $\mathbb{R}^+$) for all subsets $F \subseteq S$ with $|F| = k$.

Obviously we have:

(1) M is k-flowing over $\mathbb{Z}^+$ $\Rightarrow$ M is k-flowing over $\mathbb{R}^+$.

However the matroid $M(K_4)$ above with $k = 2$ shows that the converse is not true.

The max flow min-cut theorem can be restated, albeit exotically, as:

(2) Graphic matroids are 1-flowing over $\mathbb{Z}^+$.

The 2-commodity flow theorem can be restated as

(3) Graphic matroids are 2-flowing over $\mathbb{R}^+$.

Cographic matroids

Consider the matroid form of the max-flow min-cut theorem. It can be stated as:

"The minimum number of circuits C_i which contain e and are otherwise pairwise disjoint is equal to min $|C^*| - 1$ where the minimum is taken over all C^* containing e".

The dual form of this is not only true but is very easy to prove: it says

(4) The maximum number of cocircuits C_i^* which are pairwise disjoint except for a single edge e is equal to the minimum size of $|C| - 1$ taken over all circuits C which pass through e.

For a proof see Welsh [76, Chapter 19].

In other words, it is easy to prove

(5) Cographic matroids are 1-flowing over $\mathbb{Z}^+$.

§4. A summary of results

A very recent paper by Seymour [81] almost completely characterises k-flowing matroids for each k. We can do no more than summarize some of these delightful results in the next section.

For example one result which completely generalises (3.5) is:

(1) Cographic matroids are ∞-flowing .

Since being 1-flowing is equivalent to having the max flow min cut property, the fact that $U_{2,4}$ is not 1-flowing, together with the fact that M being k-flowing implies M is k'-flowing for $k' \leq k$ shows:

(2) If M is k-flowing then M is binary.

The max flow min cut theorem of §1 can be restated as:

(3) M is 1-flowing over $\mathbb{Z}^+$ if and only if $M \not> F_7^*$.

We now indicate the proof idea behind all the following results by proving:

(4) M is 2-flowing in $\mathbb{Z}^+$ if and only if $M \in Ex(M(K_4))$.

Proof. First we use the fact that $Ex(M(K_4))$ is the class of matroids which can be formed by taking 1 or 2 sums of matroids having ≤ 3 elements. It is easy to prove that all of these are ∞-flowing (i.e. k-flowing for all k).

It is straightforward to check that if M_1 and M_2 are k-flowing then so are the 1 and 2 sums of M_1 and M_2. Hence $EX(M(K_4))$ is ∞-flowing in $\mathbb{Z}^+$. Since $M(K_4)$ is not 2-flowing in $\mathbb{Z}^+$ (see Example 3.1) the result follows. □

This last result completely settles the first column of the table below

	$\mathbb{Z}^+$	$\mathbb{R}^+$
1-flowing	$Ex(F_7^*)$	?
2-flowing	$Ex(M(K_4))$	$Ex(AG(3,2),S_8)$
3-flowing	$Ex(M(K_4))$	$Ex(F_7,R_{10},M(H_6))$
4-flowing	$Ex(M(K_4))$	$Ex(F_7,R_{10},M(K_5))$
∞-flowing	$Ex(M(K_4))$	$Ex(F_7,R_{10},M(K_5))$

Various points about the above table need clarification.

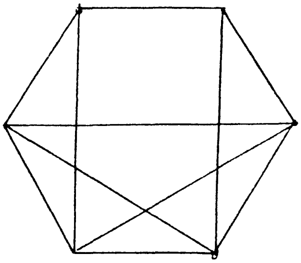
First: the matroid S_8 is the matroid whose binary representation is the set of columns of the matrix A:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

In other words S_8 with one element deleted is F_7^* .

Secondly: the graph H_6 whose cycle matroid is 2-flowing but not 3-flowing has the following form:

H_6:



Thirdly: we notice that the only open question in the above classification is characterising those matroids not 1-flowing over $\mathbb{R}^+$.

Three exluded minors for this are:- AG(3,2), T_{11} and T^*_{11}, where T_{11} is the eleven point matroid got from the representation of R_{10} in §6.3 by adding on the vector (1,1,1,1,1).

Finally we close with a curiosity. Fulkerson [68, 70] showed (in different terminology) that

(5) M is 1-flowing over $\mathbb{R}^+ \Leftrightarrow M^*$ is 1-flowing in $\mathbb{R}^+$.

The proof hinges on a linear programming argument. No such argument seems to be known for the statement:

(6) M is 2-flowing over $\mathbb{R}^+ \Leftrightarrow M^*$ is 2-flowing over $\mathbb{R}^+$.

Nevertheless (6) is true since by the above theory of Seymour M is 2-flowing over $\mathbb{R}^+$ if and only if $M \in \mathrm{Ex}(AG(3,2), S_8)$ and this is a set closed under duality!

References

Aho, A.V., Hopcroft, J.E. & Ullmann, J.D. *The Design and Analysis of Computer Algorithms*, Addison Wesley, Reading, Mass. (1974).

Appel, K. & Haken, W., Every planar map is four colourable, *Bull. Amer. Math. Soc.* 82 (1976), 711-712.

Birkoff, G., Lattice Theory, *A.M.S. Colloq. Publ.* *25* (1967).

Bixby, R.E., Kuratowski's and Wagner's theorems for matroids *J. Combinatorial Theory* *22* (1977), 31-53.

Bixby, R.E., On Reid's characterisation of the matroids representable over GF(3), *J. Combinatorial Theory* *B26* (1979), 174-205.

Bollobás, B., *Extremal Graph Theory*, Lond. Math. Soc. Monograph No. 11, Academic Press, London (1978).

Bondy, J.A. & Murty, U.S.R., *Graph Theory with Applications*, Macmillan, (London & New York) (1976).

Borodin, A. & Munro, I., *The Computational Complexity of Algebraic and Numeric Problems*, Elsevier (New York) (1975).

Bryant, V. & Perfect H., *Independence Theory in Combinatorics*, Chapman Hall (London) (1980).

Brylawski, T.H., Modular constructions for combinatorial geometries, *Trans. Amer. Math. Soc.* *203* (1975), 1-44.

Brylawski, T.H. & Kelly, D., *Matroids and Combinatorial Geometries*, University of North Carolina Press (1980).

Cook, S.A., The complexity of theorem-proving procedures, *Proc. 3rd Ann. ACM Symposium on Theory of Computing*, Assoc. for Computing Machinery New York (1971) 151-158.

Crapo, H.H. & Rota, G.L., On the foundations of combinatorial theory: combinatorial geometries, M.I.T. Press, Cambridge, Mass. 1970.

Cunningham, W.H., A combinatorial decomposition theory, Thesis, University of Waterloo (1973).

Cunningham, W.H. & Edmonds, J., A combinatorial decomposition theory, *Can. J. Math.* (to appear).

Datta, B.T., Non existence of six-dimensional tangential 2-blocks, J. Combinatorial Theory 21 (1976), 171-193.

Dirac, G.A., Some theorems on abstract graphs, Proc. Lond. Math. Soc. 2 (1952) 69-81.

Edmonds, J.R., Minimum partition of a matroid into independent subsets, J. Res. Nat. Bur. Stand. 69B (1965), 67-72.

Edmonds, J.R., Lehman's switching game and a theorem of Tutte and Nash-Williams, J. Res. Nat. Bur. Stand. 69B (1965) 73-77.

Edmonds, J., Maximum matching and a polyhedron with 0-1 vertices, J. Res. Nat. Bur. Stand. 69B (1965) 125-130.

Edmonds, J., Submodular functions, matroids and certain polyhedra, Proc. Int. Conf. on Combinatorics, (Calgary) Gordon and Breach; New York (1970) 69-87.

Even, S. & Tarjan, R.E., A combinatorial problem which is complete in polynomial space, J. Assoc. Comput. Mach. 23 (1976) 710-719.

Ford, L.R. Jr. & Fulkerson, D.R., Flows in Networks, Princeton University Press 1962.

Fulkerson, D.R., Networks, frames and blocking systems, Mathematics of the Decision Sciences, Amer. Math. Soc. (1968), 303-335.

Fulkerson, D.R., Blocking polyhedra, Graph Theory and its Applications, (B. Harris Ed.) Acad. Press (1970), 93-112.

Gallai, T., Über regülare Kettengruppen, Acta. Math. Acad. Sci. Hungar. 10 (1959), 227-240.

Gallai, T., Maximum-minimum satze und verallegemeinerte Faktoren von Graphen, Acta. Math. Acad. Sci. Hungar. 12 (1961), 131-173.

Garey, M.R. & Johnson, D.S., Computers and Intractability, (1979) W.H. Freeman and Co. (San Francisco).

Hausmann, D. & Korte, B., Oracle algorithms for fixed point problems - an axiomatic approach, Univ. of Bonn Tech. Report No. 7766-OR (to be published) (1980).

Hopcroft, J.E. & Ullman, J.D., Introduction to Automata Theory, Languages and Computation, Addison Wesley, Reading, Ma. (1979).

Hu, T.C., Multicommodity network flows, Operations Research 11 (1963), 344-360.

Jaeger, F., On nowhere-zero flows in multi-graphs, Proc. 5th British Combinatorial Conference, Aberdeen (Utilitas) (1975), 373-379.

Jaeger, F., Flows and generalised colouring theorems in graphs, J. Combinatorial Theory B26 (1979), 205-217.

Jensen, P.M. & Korte, B., Complexity of matroid property algorithms, Univ. of Bonn Tech. Report No. 78124-OR (to appear) (1980).

Karp, R.M., Reducibility among combinatorial problems, Complexity of Computer Computations (ed. R.F. Miller and J.W. Thatcher) Plenum Press, New York, (1972), 85-103.

Khachian, L.G., A polynomial algorithm for linear programming, Dokl. Akad. Nauk. SSSR 244, (1979) 1093-1096, (Translated in Sov. Math. Dokl. 20, 191-194).

Lawler, E., Combinatorial Optimisation: Networks and Matroids, Holt Reinhardt and Wilson, New York (1976).

Lehman, A., A solution of the Shannon switching game, J. Soc. Indust. Appl. Math. 12 (1964), 687-725.

Lovász, L., Flats in matroids and geometric graphs, Proc. Sixth British Combinatorial Conference Academic Press (1977), 23-45.

Lovász, L., The matroid matching problem, Algebraic Methods in Graph Theory, Proc. Conf. Szeged (1978).

Lovász, L., Matroid matching and some applications, J. of Combinatorial Theory B28 (1980), 208-236.

Lovász, L., Selecting independent lines from a family of lines in a space, Acta. Sci. Math. Univ. Szeged (1980) to appear.

MacLane, S., Some intepretations of abstract linear dependence in terms of projective geometry, Amer. J. Math. 58 (1936) 236-240.

Mansfield, A.J., On the computational complexity of a rigidity problem (1980) (to be published).

Meyer, A.R. & Stockmeyer, L.J., The equivalence problem for regular expressions with squaring requires exponential space, 13th Annual IEEE Symposium on Switching and Automata Theory (1972), 125-129.

Milner, E.C. & Welsh, D.J.A., On the computational complexity of graph theoretical properties, Proc. Fifth British Combinatorial Conference (ed. C. St. J.A. Nash-Williams and J. Sheehan) Utilitas Winnipeg (1976) 471-487.

Minty, G.J., On the axiomatic foundations of the theories of directed linear graphs, electrical networks and network programming, Journ. Math. Mech. 15 (1966), 485-520.

Mirsky, L., Transversal Theory, Academic Press (London) 1971.

Ore, O., The Four Colour Problem, Academic Press (1967).

Oxley, J.G., Thesis, Oxford (1978).

Rado, R., Note on independence functions, Proc. Lond. Math. Soc. 7 (1957), 300-320.

Reid, R., (Unpublished theorem) (1970).

Recski, A., Engineering applications of matroids - a survey, Proc. Varenna Conference (1980).

Robinson, G.C. & Welsh, D.J.A., The computational complexity of matroid properties, Math. Proc. Camb. Phil. Soc. 87 (1980), 29-45.

Seymour, P.D., The matroids with the max-flow min-cut property, J. Combinatorial Theory B23 (1977), 189-222.

Seymour, P.D., A two-commodity cut theorem, Discrete Math. 23 (1978) 177-181.

Seymour, P.D., Matroid representation over GF(3), J. Combinatorial Theory B26 (1979) 159-174.

Seymour, P.D., A short proof of the two commodity flow theorem, J. Combinatorial Theory B26 (1979) 370-372.

Seymour, P.D., Decomposition of regular matroids, J. Combinatorial B28 (1980) 305-360.

Seymour, P.D., Matroids and multicommodity flows, European Journal of Combinatorics (1981), (to be published).

Seymour, P.D., On nowhere zero 6-flows (to be published) (1981).

Strassen, V., Gaussian elimination is not optimal, Numerische Mathematik 13 (1969), 354-356.

Tutte, W.T., A contribution to the theory of chromatic polynomials, Canad. J. Math. 6 (1954), 80-91.

Tutte, W.T., A homotopy theorem for matroids I and II, Trans. A.M.S. 88 (1958) 144-174.

Tutte, W.T., Matroids and graphs, Trans. A.M.S. 90 (1959) 512-552.

Tutte, W.T., An algorithm for determining whether a given binary matroid is graphic, Proc. Amer. Math. Soc. 11 (1960), 905-917.

Tutte, W.T., A theory of 3-connected graphs, Indag. Math. 23 (1961) 441-455.

Tutte, W.T., Lectures on matroids, J. Res. Nat. Bur. Stand. 69B (1965), 1-48.

Tutte, W.T., Connectivity in matroids, Canad. J. Math. 18 (1966), 1301-1324.

Tutte, W.T., A geometrical version of the four colour problem, Combinatorial Math. and ıts Applications (ed. R.C. Bose and T.A. Dowling), Univ. of North Carolina Press, Chapel Hill (1969), 553-61.

Tutte, W.T., Introduction to the theory of matroids, American Elsevier, New York (1970).

Veblen, O., An application of modular equations in analysis situs, Ann. Math. 14 (1912), 86-94.

Wagner, K., Beweis einer Abschwachung der Hadwiger-Vermütung, Math. Ann. 153 (1964), 139-141.

Walton, P.N. & Welsh, D.J.A., On the chromatic number of binary matroids, Mathematika 27 (1980), 1-9.

Welsh, D.J.A., Matroid Theory, Lond. Math. Soc. Monographs No. 8 (Academic Press) (1976).

Welsh, D.J.A., Colouring problems and matroids, Proc. Seventh British Combinatorial Conference, Cambridge University Press (1979), 229-257.

Welsh, D.J.A., Colourings flows and projective geometries, Niew Archief voor Wiskunde (3) (1980), 159-176.

Whitney, H., On the abstract properties of linear dependence, Am. J. Math. 57 (1935), 509-533.

CENTRO INTERNAZIONALE MATEMATICO ESTIVO

(C.I.M.E.)

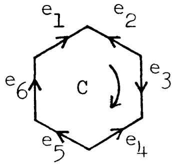
VOLTAGE-GRAPHIC MATROIDS

THOMAS ZASLAVSKY

Voltage-Graphic Matroids

Thomas Zaslavsky
The Ohio State University

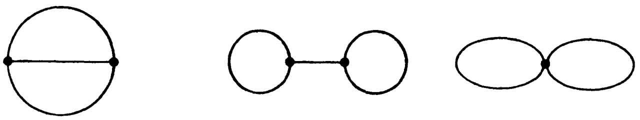
1. A *voltage graph* is a pair $\Phi = (\Gamma,\varphi)$ consisting of a graph $\Gamma = (N,E)$ and a *voltage*, a mapping $\varphi\colon E \to \mathfrak{G}$ where $\mathfrak{G}$ is a group called the *voltage group*. The voltage on an edge depends on the sense in which the edge is traversed: if for e in one direction the voltage is $\varphi(e)$, then in the opposite direction it is $\varphi(e)^{-1}$. The voltage on a circle is the product of the edge voltages taken in order with consistent direction; if the product equals 1 the circle is called *balanced*. (While in general the starting point and orientation of C influence its voltage, they have no effect on whether it is balanced.) A subgraph is balanced if every circle in it is balanced. Assuming N is finite, let $n = |N|$ and, for $S \subseteq E$, let $b(S)$ = the number of balanced components of (N,S).



$$\varphi(C) = \varphi(e_1)\varphi(e_2)^{-1}\varphi(e_3)\varphi(e_4)^{-1}\varphi(e_5)\varphi(e_6)$$

Matroid Theorem. The function $\operatorname{rk} S = n - b(S)$ is the rank function of a matroid $G(\Phi)$ on the set E. A set $A \subseteq E$ is closed iff every edge $e \notin A$ has an endpoint in a balanced component of (N,A) but does not combine with edges in A to form a balanced circle. A set is a circuit iff it is a balanced circle or a bicircular graph containing no balanced circle.

Bicircular graphs



Theta graphs

Handcuffs

We call $G(\Phi)$ a voltage-graphic matroid. When it is a simple matroid, it is a subgeometry of the Dowling geometry $Q_n(\mathfrak{G})$.

EXAMPLES

1) $G(\Gamma)$, the graphic (polygon) matroid: $\mathfrak{G} = \{1\}$, $\varphi \equiv 1$.

2) Matroids of signed graphs Σ : $\mathfrak{G} = \{+1,-1\}$.

3) $EC(\Gamma)$, the even-cycle matroid (M. Doob, Tutte): $\mathfrak{G} = \{+1,-1\}$, $\varphi \equiv -1$.

4) $B(\Gamma)$, the bicircular matroid (Simões-Pereira, Klee): $\mathfrak{G} = \mathbb{Z}_2^{E}$, $\varphi(e) = e$; or $\mathfrak{G} =$ the free abelian group on E, $\varphi(e) = e$.

5) $B(\Gamma^{o})$, $\Gamma^{o} = \Gamma$ with a loop at every node. The lattice of flats is the set of spanning forests of Γ.

6) $ED(\vec{\Gamma})$, the equidirected circle matroid of a digraph $\vec{\Gamma}$ (Matthews): $\mathfrak{G} = \mathbb{Z}$, $\varphi(e) = +1$ when e is taken in the direction assigned by $\vec{\Gamma}$. (Similarly one has $ED_n(\vec{\Gamma})$, the equidirected circle matroid modulo n, when $\mathfrak{G} = \mathbb{Z}_n$.)

7) $A(\vec{\Gamma})$, the anticoherent cycle matroid of $\vec{\Gamma}$ (Matthews): $\mathfrak{G}$ = the free group on N , $\varphi(e) = vw$ if e is directed $v \to w$.

8) $\Phi = \mathfrak{G}\cdot\Delta$, Δ = a graph on n nodes; Φ is Δ with each edge replaced by every possible $\mathfrak{G}$-labelled edge.

9) $Q_n(\mathfrak{G})$, the Dowling geometry of rank n of $\mathfrak{G}$, is $G(\mathfrak{G}\cdot K_n^o)$.

2. Now let $\mathfrak{G}$ have finite order g . A <u>proper</u> μ-<u>coloring</u> of Φ is a mapping

$$\kappa : N \to \{0\} \cup (\{1,\dots,\mu) \times \mathfrak{G})$$

such that, for any edge e from v to w (including loops), we have $\kappa(v) \neq 0$ or $\kappa(w) \neq 0$ and also

$$\kappa_1(v) \neq \kappa_1(w) \quad \text{or} \quad \kappa_2(w) \neq \kappa_2(v)\varphi(e) \qquad \text{if } \kappa(v), \kappa(w) \neq 0 ,$$

where κ_1 and κ_2 are the numerical and group parts of κ . Let $\chi_\Phi(\mu g + 1)$ = the number of proper μ-colorings of Φ and let $\chi^b_\Phi(\mu g)$ = the number which do not take the value 0 .

<u>Chromatic Polynomial Theorem</u>. $\chi_\Phi(\mu g + 1)$ is a polynomial in μ . Indeed $\chi_\Phi(\lambda) = \lambda^{b(E)}p(\lambda)$, where $p(\lambda)$ is the characteristic polynomial of $G(\Phi)$.

<u>Balanced Chromatic Polynomial Theorem</u>. $\chi^b_\Phi(\mu g)$ is a polynomial in μ . Indeed $\chi^b_\Phi(\lambda) = \Sigma_A \, \mu(\emptyset, A)\lambda^{b(A)}$, summed over balanced flats $A \subseteq E$.

<u>Fundamental Theorem</u>. Let $\chi^b_X(\lambda)$ denote the balanced chromatic polynomial of the induced voltage graph on $X \subseteq N$. Then

$$\chi_\Phi(\lambda) = \sum_{X \text{ stable}} \chi^b_X(\lambda - 1) \quad .$$

This theorem reduces calculation of $\chi_{\Phi}(\lambda)$, or of $p(\lambda)$, to that of $\chi_{\Phi}^{b}(\lambda)$, which is often easy.

EXAMPLES (continued)

1) $\chi_{\Phi}^{b}(\lambda) = \chi_{\Gamma}(\lambda)$.

4) $\chi_{\Phi}^{b}(\lambda) = \Sigma_{k} (-1)^{n-k} f_{k} \lambda^{k}$, where f_{k} = the number of k-tree spanning forests in Γ .

3) $\chi_{\Phi}^{b}(\lambda) = \Sigma_{A} 2^{n-\mathrm{rk}\,A} \chi_{\Gamma/A}(\lambda/2)$, summed over flats A of $G(\Gamma)$.

8) $\chi_{\Phi}^{b}(\lambda) = g^{n} \chi_{\Delta}(\lambda/g)$.

9) $p(Q_{n}(\mathfrak{G});\lambda) = g^{n}((\lambda-1)/g)_{n}$, where $(x)_{n}$ is the falling factorial.

3. There is a geometric realization when $\mathfrak{G} \subseteq \mathbb{R}^{\times}$. Let $\mathcal{H}[\Phi]$ be the set of all hyperplanes $x_{j} = \varphi(e)x_{i}$ in $\mathbb{R}^{n}$ where $e \in E$ is an edge from v_{i} to v_{j} .

Representation Theorem. The lattice of all intersections of subsets of $\mathcal{H}[\Phi]$, ordered by reverse inclusion, is isomorphic to the lattice of flats of $G(\Phi)$.

Corollary. $\mathcal{H}[\Phi]$ cuts $\mathbb{R}^{n}$ into $|\chi_{\Phi}(-1)|$ regions (n-dimensional cells).

4. Each Φ has a covering graph $\tilde{\Phi} = (\mathfrak{G} \times N, \mathfrak{G} \times E)$, an unlabelled graph. If e goes from v to w , the covering edge (g,e) extends from (g,v) to $(g\varphi(e),w)$. Let $p\colon \mathfrak{G} \times E \to E$ be the covering projection.

Covering Theorem. A set $S \subseteq E$ is closed in $G(\Phi)$ iff $p^{-1}(S)$ is closed in $G(\tilde{\Phi})$.

5. The Matroid Theorem does not essentially require a voltage. All we need is a specified class of "balanced" circles in Γ , such that if two circles in a theta graph are balanced, then the third is also. The pair $(\Gamma, \mathcal{B})$ is a biased graph. Although a biased graph cannot be colored in the usual sense, it has algebraically defined "chromatic polynomials" that satisfy the Fundamental Theorem.

References

T. A. Dowling, "A class of geometric lattices based on finite groups", J. Combinatorial Theory Ser. B, 14 (1973), 61-86. MR 46 #7066. Erratum, ibid. 15 (1973), 211. MR 47 #8369.

L. R. Matthews, "Matroids from directed graphs", Discrete Math. 24 (1978), 47-61.

T. Zaslavsky, "Biased graphs", manuscript, 1977.

T. Zaslavsky, "Signed graphs", submitted. Proofs of the Matroid, Covering, and Representation Theorems for signed graphs, and examples.

T. Zaslavsky, "Signed graph coloring" and "Chromatic invariants of signed graphs", submitted. Proofs of coloring and enumeration results.

T. Zaslavsky, "Bicircular geometry and the lattice of forests of a graph", submitted. Details on the bicircular and forest examples and their geometric realizations.

Department of Mathematics
The Ohio State University
231 West 18th Avenue
Columbus, Ohio 43210
U.S.A.

MATROIDS WHOSE GROUND SETS ARE DOMAINS OF FUNCTIONS

James OXLEY *IAS, Australian National University, Canberra, Australia.*

Kevin PRENDERGAST *Hydro Electric Commission, Hobart, Australia.*

Don ROW* *University of Tasmania, Hobart, Australia.*

ABSTRACT

From an integer valued function f *we obtain, in a natural way, a matroid* M_f *on the domain of* f. *We show that the class* $\mathcal{M}$ *of matroids so obtained is closed under restriction, contraction, duality, truncation and elongation, but not under direct sum. We give an excluded-minor characterisation of* $\mathcal{M}$ *and show that* $\mathcal{M}$ *consists precisely of those transversal matroids with a presentation in which the sets in the presentation are nested. Finally, we show that on an* n*-set there are exactly* 2^n *members of* $\mathcal{M}$.

*Speaker.