ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Combinatorial Geometries

Edited by

NEIL WHITE
University of Florida

*The right of the
University of Cambridge
to print and sell
all manner of books
was granted by
Henry VIII in 1534.
The University has printed
and published continuously
since 1584.*

CAMBRIDGE UNIVERSITY PRESS
Cambridge
New York New Rochelle Melbourne Sydney

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
32 East 57th Street, New York, NY 10022, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1987

Printed in Great Britain at the University Press, Cambridge

British Library Cataloguing in Publication Data

Combinatorial geometries. – (Encyclopedia
of mathematics and its applications; v. 29)

1. Combinatorial geometry
I. White, Neil
516′.13 QA167

Library of Congress Cataloguing in Publication Data

Combinatorial geometries.

(Encyclopedia of mathematics and its applications; v. 29)
Includes bibliographies and index.
1. Matroids. 2. Combinatorial geometry. I. White,
Neil. II. Series.
QA166.6.C66 1987 516′.13 86–31001

ISBN 0 521 33339 3

TM

7

The Möbius Function and the Characteristic Polynomial

THOMAS ZASLAVSKY

The effort to generalize graph theory to matroids has yielded analogs of the chromatic polynomial and related graph invariants and (although there is still no exact analog for an arbitrary matroid) a partial extension of vertex coloring. The 'characteristic polynomial' provides every matroid with an algebraic analog of the chromatic polynomial; Crapo and Rota's 'critical problem' defines a kind of proper coloring for submatroids of finite vector spaces. We shall begin our account with the characteristic polynomial, its logical building block the combinatorial Möbius function, and the related beta invariant; then we present examples including the connection with graph coloring and conclude with the critical problem.

As usual in enumeration we assume throughout this chapter that all matroids, lattices, and other combinatorial objects are finite.

7.1. The Möbius Function

The combinatorial Möbius function, which we will need for geometric lattices, can just as easily be defined for any finite partially ordered set. Let P be such a set and consider integral functions $P \times P \rightarrow \mathbb{Z}$. The function μ (or μ_P) which satisfies

$$\sum_{x \leqslant y \leqslant z} \mu(x, y) = \delta(x, z) \quad \text{if} \quad x \leqslant z \tag{7.1}$$

(where δ is the Kronecker delta) together with ordering property

$$\mu(x, z) = 0 \quad \text{if} \quad x \nleqslant z$$

is called the *Möbius function* of P. [Hall (1936). Weisner (1935) for lattices. The basic reference is Rota (1964). A good recent treatment is Aigner (1979).]

To see that μ exists and is uniquely defined, let us rewrite (7.1) as two equations:

$$\mu(x,x)=1, \tag{7.2}$$

$$\mu(x,z)=-\sum_{x\leqslant y<z}\mu(x,y) \quad \text{if} \quad x<z. \tag{7.3}$$

We can calculate $\mu(x,z)$ first for $z=x$ from (7.2), then recursively from (7.3) for successively higher z by induction on the length of the longest chain from x to z. Thus the value of $\mu_P(x,z)$ depends only on the order structure of the interval $[x,z]$ and not on the rest of P.

To understand the Möbius function better, let us introduce the incidence algebra $I(P)$: the set of all functions $\phi: P\times P\to\mathbb{Z}$ such that $\phi(x,y)=0$ if $x\not\leqslant y$, with pointwise addition and the convolution product

$$(\phi*\psi)(x,z)=\sum_{x\leqslant y\leqslant z}\phi(x,y)\psi(y,z).$$

This product is a form of matrix multiplication. If we extend $\leqslant_P$ to a linear ordering of P denoted by subscripts, so $p_i<_P p_j$ implies $i<j$, then an incidence function is a $|P|$ by $|P|$ upper-triangular matrix and convolution is matrix multiplication. Hence multiplication is associative and has δ for identity. Also, any incidence function ϕ with $\phi(x,x)\equiv 1$ is invertible. The *zeta function* of P is the function $\zeta\in I(P)$ with

$$\zeta(x,y)=1 \quad \text{if} \quad x\leqslant y.$$

We can now restate the definition (7.1): *μ is the left inverse of ζ.*

The recursive formula (7.3) is an effective way to compute the Möbius function of a small interval. Some useful values are the following.

7.1.1. Proposition. *In a partially ordered set,*

$$\begin{aligned}&\mu(x,x)=1,\\ &\mu(x,y)=-1 \quad \textit{if } y \textit{ covers } x,\\ &\mu(x,z)=n-1 \quad \textit{if } [x,z] \textit{ is an } n\textit{-point line.}\end{aligned}$$

Proof. Exercise. □

Before we concentrate on geometric lattices, we shall give some important general properties of the Möbius function.

7.1.2. Proposition. *The Möbius function of P can be defined by replacing* (7.1) *by*

$$\sum_{x\leqslant y\leqslant z}\mu(y,z)=\delta(x,z) \quad \textit{if} \quad x\leqslant z,$$

or by replacing (7.3) *by*

$$\mu(x,z) = -\sum_{x<y\leqslant z} \mu(y,z) \quad \textit{if} \quad x<z.$$

Proof. Exercise. □

The *raison d'être* of the Möbius function is the inversion property. This is the common generalization of the principle of inclusion and exclusion (which is Möbius inversion on the power set of a set) and of number-theoretic Möbius inversion [in which P is the set of natural numbers ordered by divisibility; the classical $\mu(n) = \mu_P(1, n)$]. If $\phi \in I(L)$ and $f : P \to A$ (an abelian group, which will often be the integers), define

$$(\phi * f)(x) = \sum_{y\geqslant x} \phi(x,y) f(y),$$

$$(f * \phi)(y) = \sum_{x\leqslant y} f(x)\phi(x,y).$$

These are the incidence-algebra versions of the product of a vector by a matrix.

7.1.3. Proposition (Möbius Inversion). *Let P be a finite poset. Let f and g be functions on P with values in any ring* (*or $\mathbb{Z}$-module, i.e., abelian group*). *Then*

$$g(x) = \sum_{y\geqslant x} f(y)$$

implies

$$f(x) = \sum_{y\geqslant x} \mu_P(x,y) g(y),$$

and vice-versa. In addition

$$g(y) = \sum_{x\leqslant y} f(x)$$

implies

$$f(y) = \sum_{x\leqslant y} g(x) \mu_P(x,y),$$

and vice versa.

Proof. Exercise. □

Now we specialize to the case of a finite matroid $M = M(E)$. Its lattice of flats L has Möbius function μ_L. [The value $\mu_L(0, 1)$ is often called the *Möbius invariant* of L and written $\mu(L)$. As we noted earlier, the Möbius invariant of an interval $[x, y]$ in L, $\mu([x, y])$, is equal to $\mu_L(x, y)$.] The *Möbius function of M* is defined by

$$\begin{aligned} \mu_M(X,F) &= \mu_L(X,F) && \text{if} \quad X, F \in L, \\ \mu_M(X,F) &= 0 && \text{if} \quad X \notin L, \quad F \in L; \end{aligned}$$

$\mu_M(X, F)$ is not defined if $F \notin L$. The purpose of this extended definition of μ_M is to allow matroids in which $\varnothing$ is not closed to obey the same formulas as other matroids–the same reason for which the chromatic polynomial of a graph with loops is taken to be identically 0. (These two cases are virtually the same, as our discussion of the chromatic polynomial will show.)

One such formula of basic importance is the following expansion (valid more generally for any closure on S). It seems to originate with Weisner. The non-trivial case (where $W \in L$) is a special case of Weisner (1935), Equation (15) with property P' = 'minimal'. For a graphic matroid it is implied by a result of Whitney (1932).

7.1.4. Proposition (Boolean Expansion Formula). *Let L be the lattice of flats of the matroid $M = M(E)$. Let $W \subseteq E$ and $F \in L$. Then*

$$\mu_M(W, F) = \sum_{\substack{W \subseteq X \subseteq F \\ \operatorname{cl} X = F}} (-1)^{|X - W|}.$$

Proof. See Exercise 7.9. □

7.1.5. Example. *Uniform matroids, Boolean algebras, and circuits.* In the uniform matroid U_{rm} of rank r on an m-set E, the flats of rank k (for $k < r$) are the k-subsets of E. We have

$$\mu(U_{rm}) = \sum_{k=0}^{r-1} (-1)^{k+1} \binom{m}{k}, \quad \text{if} \quad 0 < r \leqslant m.$$

In particular for the Boolean algebra $B_m = U_{mm}$ we have $\mu(B_m) = (-1)^m$. For the m-point circuit $C_m = U_{m-1,m}$ we have $\mu(C_m) = (-1)^{m-1}(m-1)$. (Exercise.)

Another useful formula, also valid for any closure, is:

7.1.6. Proposition. [*Special case of Weisner's theorem* (*Weisner 1935, Theorem 9; Rota 1964, p. 351, Corollary*)] *In the matroid $M = M(E)$ let F be a flat, e a point in F, and $F_1, F_2, \ldots$ the flats such that F covers F_i and $e \notin F_i$. Then*

$$\mu_M(\varnothing, F) = -\sum_i \mu_M(\varnothing, F_i).$$

Proof. For fixed e and any flat F containing e, let

$$f(F) = \mu_M(\varnothing, F) + \sum_i \mu_M(\varnothing, F_i).$$

We want to show $f \equiv 0$. Since that is trivially true if $\varnothing$ is not closed, we may assume $\operatorname{cl}(e)$ is an atom A in the lattice L of flats. Let

$$\begin{aligned} g(F) &= \sum_{A \leqslant F' \leqslant F} f(F') \\ &= \sum_{F'} \left[\mu(\varnothing, F') + \sum_i \mu(\varnothing, F'_i) \right]. \end{aligned}$$

Each flat $E' \leqslant F$ appears exactly once in the latter sum. For if $E' \geqslant A$, then E' is an F'; but if $E' \ngeqslant A$, then E' is one of the F'_i associated with that F' which equals $E' \vee A$. Hence

$$g(F) = \sum_{E' \leqslant F} \mu(\varnothing, E') = 0$$

since $F \geqslant A > 0$. We therefore have

$$\sum_{F' \in [A,F]} f(F') = g(F) = 0.$$

Applying Möbius inversion (Proposition 7.1.3), we see that $f \equiv 0$. □

Now we are ready to prove the main properties of the Möbius function of a matroid. The first theorem is the core of Brylawski (1972, Theorem 4.2), which will reappear in Theorem 7.2.4 and Section 7.4.

7.1.7. Theorem. *The Möbius invariant of a matroid $M = M(E)$ satisfies:*
(i) *the deletion-contraction rule: if $e \in E$ is not an isthmus,*

$$\mu(M) = \mu(M - e) - \mu(M/e);$$

(ii) *the direct sum rule: if $M = M_1 \oplus M_2$, then*

$$\mu(M) = \mu(M_1)\mu(M_2).$$

Proof of (i). If e is a loop, $M - e = M/e$ and both sides of the equation are 0. Suppose then that e is neither an isthmus nor a loop.

We rewrite the left-hand side by Proposition 7.1.4:

$$\begin{aligned}\mu(M) &= \sum_{\substack{X \subseteq E \\ \mathrm{cl}X = E}} (-1)^{|X|} \\ &= \sum_{\substack{X \subseteq E - e \\ \mathrm{cl}X = E}} (-1)^{|X|} - \sum_{\substack{e \in X \subseteq E \\ \mathrm{cl}X = E}} (-1)^{|X - e|}. \qquad (7.4)\end{aligned}$$

Since e is not an isthmus, a set $X \subseteq E - e$ spans M if and only if it spans $M - e$. Hence the first sum in (7.4) equals $\mu(M - e)$. The second sum equals $\mu(M/e)$, for an X containing e spans M if and only if $X - e$ spans M/e.

Proof of (ii). See Exercise 7.10. □

Next is the fundamental theorem on the sign of μ in a geometric lattice.

7.1.8. Theorem. (*Rota 1964, Theorem 4, p. 357*) *The Möbius function of a geometric lattice L is non-zero and alternates in sign. Precisely,*

$$(-1)^{r(y)-r(x)}\mu_L(x, y) > 0 \quad \textit{if} \quad x \leqslant y \quad \textit{in} \quad L.$$

Proof. It will suffice to prove

$$(-1)^{r(L)}\mu_L(0,1) > 0. \tag{7.5}$$

We use induction on the rank and nullity of the combinatorial geometry $G = G(E)$ whose points are the atoms of L.

If G has nullity 0, it is a Boolean algebra. Hence by Example, 7.1.5, $\mu_G(0,1) = (-1)^{|E|} = (-1)^{r(L)}$, whence (7.5) is immediate. This case includes lattices with rank 0 or 1.

If G has positive nullity, it is not a Boolean algebra. Hence there is a point e which is not an isthmus. By induction on rank, $(-1)^{r(G/e)}\mu(G/e) > 0$. By induction on nullity, $(-1)^{r(G-e)}\mu(G-e) > 0$. By Theorem 7.1.7,

$$(-1)^{r(G)}\mu(G) = (-1)^{r(G/e)}\mu(G/e) + (-1)^{r(G-e)}\mu(G-e),$$

which is positive by the previous observations. Thus we have the theorem. □

7.1.9. Corollary. (*Brylawski 1972, Theorem 4.2 and Corollary 4.3*) *The magnitude of the Möbius invariant of a matroid satisfies*

$$|\mu(M)| = |\mu(M-e)| + |\mu(M/e)|$$

if $e \in E$ is neither an isthmus nor a loop, and

$$|\mu(M_1 \oplus M_2)| = |\mu(M_1)|\ |\mu(M_2)|. \qquad \square$$

The last result on μ is an expansion formula which will be needed to prove Stanley's modular-element factorization of the characteristic polynomial, Theorem 7.2.5 below.

7.1.10. Lemma. *Let x be a fixed element of the lattice L and let $v \in L$. Then*

$$\mu(0,v) = \sum_{\substack{y \\ y \leqslant x, z \wedge x = 0 \\ y \vee z = v}} \sum_{z} \mu(0,y)\mu(0,z).$$

Proof. Let $f(v)$ denote the right-hand side. Then

$$\begin{aligned}\sum_{u \leqslant v} f(u) &= \sum_{y \leqslant x \wedge v} \sum_{\substack{z \leqslant v \\ z \wedge x = 0}} \mu(0,y)\mu(0,z) \\ &= \delta(0, x \wedge v) \sum_{\substack{z \leqslant v \\ z \wedge x = 0}} \mu(0,z).\end{aligned}$$

Either $\delta(0, x \wedge v) = 0$, or else $x \wedge v = 0$ so that the z-sum ranges over all $z \leqslant v$ and consequently equals $\delta(0,v)$. Thus $\sum_{u \leqslant v} f(u) = \delta(0,v)$. Inverting this sum yields $f(v) = \mu(0,v)$, as desired. □

7.2. The Characteristic Polynomial

The characteristic polynomial is the matroid analog of the chromatic polynomial of a graph. While it does not count proper colorings–indeed there is no way known to color a general matroid corresponding to vertex coloring of a graph–the characteristic polynomial has most of the algebraic properties of the chromatic polynomial and can for many examples be interpreted in an interesting way related to coloring (in the 'critical problem').

The *characteristic polynomial*[†] *of a matroid* M is defined to be

$$p(M;\lambda)=\sum_{F\in L}\mu_M(\varnothing,F)\lambda^{r(M)-r(F)},$$

where L denotes the lattice of flats of M. Clearly, $p(M;\lambda)$ is monic of degree $r(M)$ except when $\varnothing$ is not closed, in which case $p(M;\lambda)\equiv 0$. The coefficient of $\lambda^{r(M)-k}$ is known as the *k-th Whitney number of the first kind of* M, written $w_k(M)$ (cf. Chapter 8); thus

$$p(M;\lambda)=\sum_{k=0}^{r(M)}w_k(M)\lambda^{r(M)-k},$$

$$w_k(M)=\sum_{\substack{F\in L\\ r(F)=k}}\mu_M(\varnothing,F).$$

We also see that $\mu(M)=p(M;0)$. Because of this, many properties of the Möbius invariant are specializations of those of the characteristic polynomial.

We also define the *characteristic polynomial of a geometric lattice* L; it is

$$p(L;\lambda)=\sum_{x\in L}\mu_L(0,x)\lambda^{r(L)-r(x)}.$$

This polynomial is always monic of degree $r(L)$; its coefficients are the Whitney numbers (of the first kind) of L. (Frequently in the literature $p(M;\lambda)$ is defined to be $p(L;\lambda)$ where L is the lattice of M. This is adequate for simple matroids but our definition is better in general.)

From our knowledge of the Möbius function we get at once two useful results. Setting $W=\varnothing$ and summing over all $F\in L$ in Proposition 7.1.4:

7.2.1. Proposition. *The characteristic polynomial of the matroid* $M=M(E)$ *has the Boolean expansion*

$$p(M;\lambda)=\sum_{X\subseteq E}(-1)^{|X|}\lambda^{r(M)-r(X)}. \qquad \square$$

7.2.2. Example. *Uniform matroids, Boolean algebras, and circuits.* For the

[†] Also called the *Birkhoff* or *Poincaré polynomial.*

uniform matroid U_{rm} with $0 < r \leqslant m$ we have

$$p(U_{rm};\lambda) = \sum_{k=0}^{r-1} (-1)^k \binom{m}{k}[\lambda^{r-k} - 1]$$

$$= (-1)^{r-1}(\lambda - 1)\sum_{j=0}^{r-1} (-\lambda)^j \binom{m-1}{r-1-j}.$$

In particular $p(B_m;\lambda) = (\lambda - 1)^m$ and

$$P(C_m;\lambda) = (\lambda - 1)\frac{(\lambda - 1)^{m-1} - (-1)^{m-1}}{\lambda}.$$

From Rota's sign theorem, Theorem 7.1.8:

7.2.3. Proposition. *If L is a geometric lattice, then the coefficients of $(-1)^{r(L)}p(L;1-\lambda)$ are all positive. In other words,*

$$|w_k(L)| = (-1)^k w_k(L). \qquad \square$$

And from Proposition 7.2.1 we can deduce an analog of Theorem 7.1.7 contained essentially in Brylawski (1972, Theorem 4.2).

7.2.4. Theorem. *The characteristic polynomial of a matroid $M = M(E)$ satisfies*:

(i) *the deletion-contraction rule*: *if $e \in E$ is not an isthmus,*

$$p(M;\lambda) = p(M - e;\lambda) - p(M/e;\lambda);$$

(ii) *the direct sum rule*: *if $M = M_1 \oplus M_2$,*

$$p(M;\lambda) = p(M_1;\lambda)p(M_2;\lambda).$$

Proof. Exercise. See also Section 7.4. □

Theorem 7.2.4(ii) shows that some characteristic polynomials factor in an interesting way. We can find a second kind of factorization by setting $\lambda = 1$. From the definition of μ_M, $p(M;1) = 0$ for every matroid M whose point set is not empty. Hence $\lambda - 1$ divides $p(M;\lambda)$. Both factorizations are special cases of a theorem due to Stanley.

7.2.5. Theorem. [*Modular factorization* (*Stanley 1971, Theorem 2*)] *If x is a modular element of the geometric lattice L, then*

$$p(L;\lambda) = p([0,x];\lambda) \sum_{\substack{z \in L \\ z \wedge x = 0}} \mu(0,z)\lambda^{r(L)-r(x)-r(z)}.$$

Proof. The right-hand side equals

$$\sum_{y \leqslant x} \sum_{z \wedge x = 0} \mu(0,y)\mu(0,z)\lambda^{r(L)-r(y)-r(z)}. \qquad (7.6)$$

We now need a lemma. Recall that $(v, w)M$ means v and w are a modular pair in L.

7.2.6. Lemma. *If $(v, w)M$ and $v \wedge w \leqslant u \leqslant v$, then $(u, w)M$.*

Proof of Lemma. We want to prove that

$$u \wedge (w \vee t) = (u \wedge w) \vee t \quad \text{for all} \quad t \leqslant u.$$

The inequality $\geqslant$ is a lattice identity, so it suffices to prove $\leqslant$. We have, by the assumption $(v, w)M$,

$$v \wedge (w \vee t) = (v \wedge w) \vee t \quad \text{for all} \quad t \leqslant v.$$

Note that $v \wedge w = u \wedge w$ and $v \geqslant u$. Hence

$$u \wedge (w \vee t) \leqslant (u \wedge w) \vee t \quad \text{for all} \quad t \leqslant v,$$

which is stronger than what we need. □

In the theorem, $(x, z)M$ because x is a modular element; and $x \wedge z = 0 \leqslant y \leqslant x$. The lemma implies $(y, z)M$, whence

$$r(y) + r(z) = r(y \vee z) + r(y \wedge z) = r(y \vee z).$$

Thus (7.6) equals

$$\sum_{y \leqslant x} \sum_{z \wedge x = 0} \mu(0, y)\mu(0, z)^{r(L) - r(y \vee z)}$$
$$= \sum_{v \in L} \lambda^{r(L) - r(v)} \sum_{\substack{y \leqslant x \\ y \vee z = v}} \sum_{z \wedge x = 0} \mu(0, y)\mu(0, z).$$

The inner double sum equals $\mu(0, v)$ by Lemma 7.1.10. Thus we have the theorem. □

To see that Stanley's theorem includes the direct-sum factorization, suppose $M = M_1 \oplus M_2$. Then $L = L(M) = L_1 \times L_2$. In L the element $x = (1_1, 0)$ is modular; moreover $z \wedge x = 0$ if and only if $z \in \{0\} \times L_2$. Thus in Stanley's theorem the first factor is $p(L_1; \lambda)$ and the second is $p(L_2; \lambda)$.

We can use Theorem 7.2.5 to determine the cofactor of $\lambda - 1$ in $p(L; \lambda)$. Let a be any atom of L; then $p([0, a]; \lambda) = \lambda - 1$. Let $L(a) = L - [a, 1]$; then $L(a)$ is an ideal in L. Define

$$p(L(a); \lambda) = \sum_{z \in L(a)} \mu_L(0, z)\lambda^{r(L) - 1 - r(z)}.$$

Since any atom is a modular flat, we have:

7.2.7. Corollary. *Let a be any atom in the geometric lattice L. Then $p(L; \lambda) = (\lambda - 1)p(L(a); \lambda)$.* □

7.2.8. Corollary. *The polynomial $p(L(a);\lambda)$ is the same for every atom $a\in L$.* □

7.2.9. Proposition. *[Brylawski 1971, Theorem 6.16(v)] Let M be the parallel connection of M_1 and M_2 with respect to the basepoint p, and assume p is not a loop in either M_1 or M_2. Then*

$$p(M;\lambda)=\frac{p(M_1;\lambda)p(M_2;\lambda)}{\lambda-1}.$$

Proof. The assumptions imply that p is not a loop in M either. Hence by Corollary 7.2.7 the proposition is equivalent to the assertion that

$$p(L(p);\lambda)=p(L_1(p);\lambda)p(L_2(p);\lambda), \tag{7.7}$$

where L_i is the lattice of flats of M_i, provided that $\varnothing$ is closed in M_1 and M_2, which we may clearly assume. In full, (7.7) says

$$\sum_{\substack{F\in L\\ p\notin F}}\mu_L(0,F)\lambda^{r(L)-1-r(F)}$$

$$=\sum_{\substack{F_1\in L_1\\ p\notin F_1}}\sum_{\substack{F_2\in L_2\\ p\notin F_2}}\mu_{L_1}(0,F_1)\mu_{L_2}(0,F_2)\lambda^{r(L)-1-r(F_1)-r(F_2)},$$

since $r(L)-1=[r(L_1)-1]+[r(L_2)-1]$. By Brylawski (1971, Proposition 5.11) (see White 1986, Chapter 9), the flats F not containing p are precisely the unions $F_1\cup F_2$ of flats of M_1 and M_2 where $p\notin F_1$ and $p\notin F_2$, and $[0,F]\cong[0,F_1]\times[0,F_2]$. So $r(F)=r(F_1)+r(F_2)$ and $\mu(0,F)=\mu(0,F_1)\mu(0,F_2)$, which is just what we need to prove the equation. □

7.3. The Beta Invariant

An informative number associated with a matroid is Crapo's beta invariant. With it one can decide whether a matroid is connected and whether it comes from a series-parallel network. The invariant can sometimes also establish that two matroids are not dual.

The *beta invariant* of the matroid $M=M(E)$, whose lattice of flats is L, is defined by

$$\beta(M)=(-1)^{r(M)-1}\frac{\mathrm{d}}{\mathrm{d}\lambda}p(M;1),$$

which equals $(-1)^{r(M)-1}\sum_F\mu_M(\varnothing,F)[r(M)-r(F)]$, so that

$$\beta(M)=(-1)^{r(M)}\sum_{F\in L}\mu_M(\varnothing,F)r(F).$$

In view of Proposition 7.2.1 we could equally well define

$$\beta(M)=(-1)^{r(M)}\sum_{X\subseteq E}(-1)^{|X|}r(X),$$

as Crapo (1967) did when introducing the invariant. Some simple properties of β are summarized in Proposition 7.3.1.

7.3.1. Proposition. *Let $M=M(E)$, $L=$ the lattice of flats of M.*

(a) *If M has no loops, $\beta(M)$ depends only on L.*

(b) $\beta(\text{isthmus})=1$.

(c) $\beta(M)=0$ *if $E=\varnothing$ or if M contains a loop.*

(d) *If $e\in E$ is not a loop,*

$$\beta(M)=(-1)^{r(M)-1}\sum_{\substack{F\in L\\ e\notin F}}\mu_M(\varnothing,F).$$

Proof. Exercise 7.17. □

We define the beta invariant of a geometric lattice to be that of the underlying combinatorial geometry. Proposition 7.3.1 shows that $\beta(L)=0$ if $r(L)=0$, 1 if $r(L)=1$.

The fundamental properties of β are those in Theorem 7.3.2.

7.3.2. Theorem. (*Crapo 1967*) *The beta invariant of the matroid $M=M(E)$ satisfies*

(a) $\beta(M)\geqslant 0$.

(b) $\beta(M)>0$ *if and only if M is connected and is not a loop.*

(c) *If $e\in E$ is neither an isthmus nor a loop,*

$$\beta(M)=\beta(M-e)+\beta(M/e).$$

(d) $\beta(M^*)=\beta(M)$ *except when M is an isthmus or a loop.*

Proof of (c). Exercise 7.18. □

Proof of (a). Exercise 7.18. □

Proof of (b). By Exercise 7.18, $\beta(M)=0$ if M is disconnected. We have to prove $\beta(M)>0$ if M is connected and not a loop. If M is connected and $|E|\geqslant 3$, then [White 1986, Proposition 7.69 (1)] for every element e either M/e is connected or $M-e$ is connected. Then, by induction, since $|E-e|\geqslant 2$, either $\beta(M/e)>0$ or $\beta(M-e)>0$, hence by (c) and (a) we have $\beta(M)>0$. The cases with $|E|\leqslant 2$ are easily checked to start the induction. □

Proof of (d). Since M is disconnected if and only if M^* is, the disconnected case follows from (b). We may now assume that M is connected and $|E|\geqslant 2$.

Since no point is an isthmus or a loop, we have from (c):

$$\begin{aligned}\beta(M) &= \beta(M-e)+\beta(M/e),\\ \beta(M^*) &= \beta(M^*-e)+\beta(M^*/e)\\ &= \beta((M/e)^*)+\beta((M-e)^*).\end{aligned}$$

Then (d) follows by induction on $|E|$ provided $|E-e|\geqslant 2$. But if $|E-e|=1$, M and M^* are both isomorphic to the 2-point circuit; (d) follows. □

One of the uses of the beta invariant is to characterize series-parallel networks. First we establish the behaviour of β under series and parallel connections.

7.3.3. Proposition. [*Brylawski 1971, Theorem 6.16 (vi)*] *Let $M=M(E)$ be the series or parallel connection of two matroids M_1 and M_2, each having at least two points, with respect to the basepoint p. Then $\beta(M)=\beta(M_1)\beta(M_2)$.*

Proof. Suppose M is the parallel connection. The proposition follows from Proposition 7.3.1(d), Corollary 7.2.7, and Proposition 7.2.9.

But if M is the series connection, M^* is the parallel connection of M_1^* and M_2^*; the result follows from the former case and Theorem 7.3.2(d). □

7.3.4. Proposition. [*Brylawski 1971, Theorem 7.6(2)*] *M is the matroid of a series-parallel network if and only if it is not an isthmus and $\beta(M)=1$.*

Proof. The smallest series-parallel matroid is the 2-point circuit C_2. By Proposition 7.3.1, $\beta(C_2)=1$. As White (1986, Chapter 6) shows, any series-parallel matroid is obtained from C_2 by a succession of parallel duplications of a point [which by Proposition 7.3.1(a) leave β unaltered] and dualizations [which do not change β due to Theorem 7.3.2(d)]. Hence $\beta(M)=1$ if M is the matroid of a series-parallel network.

Conversely, suppose that $\beta(M)=1$ and let $e\in E$, the point set of M. If $|E|=1$, M must be an isthmus. Assuming now $|E|\geqslant 2$, M is connected [by Theorem 7.3.2 (b)] so Theorem 7.3.2(c) holds; since β is always a non-negative integer, we conclude that $\beta(M-e)=0$ or $\beta(M/e)=0$. Say the former: then $M-e=\mathrm{M}(E_1)\oplus M(E_2)$; and $\beta(M)=\beta(M-E_2)\beta(M-E_1)$ by Proposition 7.3.3. So M is the series connection of two matroids with $\beta=1$, which by induction on $|E|$ are series-parallel matroids. But then M is a series-parallel matroid. □

Oxley [1982, Proposition (2.5)] extends Proposition 7.3.4 to larger values of β. He shows that, if $\beta(M)=k>1$, then either M is a series-parallel extension of a 3-connected matroid with $\beta=k$ or M is a 2-sum of two matroids with $\beta<k$. See Oxley's paper for the definitions and proofs.

The beta invariant may be regarded as almost the Möbius inverse of the rank function. Let L be a geometric lattice; then the signed beta function $B(x) \equiv (-1)^{r(L)-r(x)}\beta(L/x)$ equals

$$\sum_{y \geqslant x} \mu_L(x, y) r(y).$$

Inverting,

$$r(x) = \sum_{y \geqslant x} B(y).$$

An expression essentially equivalent to this one appears in the cluster analysis of percolation processes on a graph (cf. Essam 1971, Sections 3.6–3.7).

7.4. Tutte–Grothendieck Invariance

The *rank generating function* of a matroid $M = M(E)$, introduced in Crapo (1970), is the two-variable polynomial

$$R(M; u, v) = \sum_{X \subseteq E} u^{r(M)-r(X)} v^{|X|-r(X)}.$$

The Boolean expansion theorems 7.1.5 and 7.2.1 amount to saying that $\mu(M)$ and $p(M;\lambda)$ are approximately specializations of $R(M;u,v)$; specifically,

$$\mu(M) = (-1)^{r(M)} R(M; 0, -1),$$
$$p(M;\lambda) = (-1)^{r(M)} R(M; -\lambda, -1).$$

Those observations and all the ideas of this section are based on Tutte (1947), where they were developed for graphs. Their extension to matroids is due to Crapo, Rota, and Brylawski.

The rank generating polynomial has an important property which generalizes Theorems 7.1.7 and 7.2.4. We need some definitions. An *invariant* of matroids is any function f of matroids which is the same for isomorphic matroids:

$$M \cong M' \quad \text{implies} \quad f(M) = f(M').$$

(We are only concerned, as usual, with finite matroids.) A *Tutte–Grothendieck invariant of matroids* is an invariant satisfying the direct-sum rule

$$f(M_1 \oplus M_2) = f(M_1) f(M_2)$$

and the deletion-contraction rule

$$f(M) = f(M - e) + f(M/e)$$

for each point e of M that is neither a loop nor an isthmus.

7.4.1. Proposition. *The rank generating function is a Tutte–Grothendieck invariant of matroids.*

Proof. Exercise 7.24. This result is implicit in Crapo (1970, Propositions 9 and 10), and is made explicit in Brylawski (1972). □

Theorems 7.1.7 and 7.2.4 are special cases because any specialization of $R(M;u,v)$ is automatically a Tutte–Grothendieck invariant. The remarkable thing is that there is a converse.

7.4.2. Proposition. (*Brylawski 1972*) *If $f(M)$ is a Tutte–Grothendieck invariant of matroids, then it is an evaluation of $R(M;u,v)$. It is obtained by setting $u = f(\text{isthmus}) - 1$ and $v = f(\text{loop}) - 1$.*

Proof: Exercise 7.25. □

This is a fundamental result but it still does not capture the essence of the characteristic polynomial. For that we need to define a *Tutte–Grothendieck invariant of geometries.* This is a matroidal Tutte–Grothendieck invariant with the additional property that

$$f(M) = f(G(M)) \quad \text{if} \quad M \text{ is loopless.}$$

7.4.3. Theorem. (*Brylawski 1972, Corollary 4.4*) *The invariant $(-1)^{r(M)}p(M;\lambda)$ is a Tutte–Grothendieck invariant of geometries. Moreover, it is a universal such invariant: if f is any such invariant, then $f(M) = (-1)^{r(M)}p(M; 1 - f(\text{isthmus}))$.*

Proof. The geometric invariance of $(-1)^{r(M)}p(M;\lambda)$ follows from the definition of $p(M;\lambda)$ and from Theorem 7.2.4. Given f, in view of Proposition 7.4.2 it is enough to show that $f(B_1^*) = 0$. Let us consider $M = C_2$, the 2-point circuit. We have

$$f(B_1) = f(C_2) = f(C_2 - p) + f(C_2/p) = f(B_1) + f(B_1^*),$$

whence $f(B_1^*) = 0$. □

7.5. Examples

Aside from the graphic matroids, chosen for their historical and motivating importance, our examples are of matroids whose characteristic polynomials are particularly simple in form because they belong to the class of 'supersolvable' geometries.

The chromatic polynomial. One of the *raisons d'être* of the characteristic polynomial, indeed its original motivation, is that it generalizes the chromatic polynomial of a graph. Let $\chi(\Gamma;\lambda)$ be the chromatic polynomial, $c(\Gamma)$ the number of components, and M the matroid of the graph Γ.

7.5.1 Proposition. $\chi(\Gamma;\lambda) = \lambda^{c(\Gamma)}p(M;\lambda)$.

This formula can be traced back to G.D. Birkhoff's paper of 1912, where it was stated (not for graphs, but for maps) in the form

$$\chi(\Gamma;\lambda) = \sum_{i=1}^{n} \lambda^i \sum_{k=0}^{n-i} (-1)^k c_k(0, n-i), \tag{7.8}$$

n being the number of vertices and $c_k(0, n-i)$ the number of chains of length k from rank 0 to rank $n-i$ in the lattice of contractions of Γ [isomorphic to $L(M)$]. The equivalence of (7.8) with Proposition 7.5.1 is a consequence of Philip Hall's theorem (Exercise 7.13) and the fact that $c(\Gamma) = n - r(M)$ (White 1986, Chapter 6).

Proposition 7.5.1 is often proved by observing that $\chi(\Gamma;\lambda)/\lambda^{c(\Gamma)}$ is, like $p(M;\lambda)$, a Tutte–Grothendieck invariant of graphic matroids, comparing the two for a loop and an isthmus, and deducing their equality. But that approach does not explain the appearance of the Möbius function. For that it is better to carry out a proof by Möbius inversion (due essentially to Whitney 1932).

Proof. Let γ be any coloring of Γ in λ colors, whether proper or not, and let $I(\gamma)$ be the set of edges which are improperly colored, that is, $e \in I(\gamma)$ if and only if $I(\gamma)$ gives the same values to the two end points of e. It is easy to see that $I(\gamma)$ is closed in the graphic matroid M. Let L be the lattice of closed sets, and let $v(F)$ = the number of colorings γ for which $I(\gamma) = F$. Clearly

$$\sum_{F \in L} v(F) = \lambda^n.$$

More generally,

$$\sum_{F \geqslant F'} v(F) = \lambda^{c(F')},$$

since the colorings γ being counted, those which are improper on F' at least, have to be constant on each component of F'. Inverting,

$$\sum_{F \geqslant F'} \mu(F', F)\lambda^{c(F)} = v(F').$$

Setting $F' = 0$, on the left we have $\lambda^{c(\Gamma)} p(M;\lambda)$ and on the right $\chi(\Gamma;\lambda)$. (The trivial case where $\varnothing$ is not closed can be handled separately.) □

Supersolvable geometric lattices (Stanley 1972). A geometric lattice is *supersolvable* when it contains a complete chain of modular elements. For such a lattice the modular-element factorization theorem makes computation of the characteristic polynomial easy.

7.5.2. Proposition. (*Stanley 1971, p. 217; 1972, Theorem 4.1*) *Suppose L is a geometric lattice of rank r with a complete chain $0 < x_1 < x_2 < \cdots < x_r = 1$ consisting of modular flats. Let N_k = the number of atoms which are $\leqslant x_k$ but*

$\nleq x_{k-1}$. *Then*

$$\begin{aligned} p(L;\lambda) &= (\lambda-1)(\lambda-N_2)(\lambda-N_3)\cdots(\lambda-N_r),\\ \mu(L) &= (-1)^r N_2 N_3 \cdots N_r,\\ \beta(L) &= (N_2-1)(N_3-1)\cdots(N_r-1),\\ w_k(L) &= (-1)^k \sigma_k(1,N_2,N_3,\ldots,N_r), \end{aligned}$$

where σ_k is the k-th elementary symmetric function. □

One class of supersolvable geometric lattices is the Boolean algebras, or lattices of free matroids. Less trivial examples appear below.

Partitions. The partition lattice Π_n has characteristic polynomial

$$p(\Pi_n;\lambda) = (\lambda-1)(\lambda-2)\cdots(\lambda-n+1). \tag{7.9}$$

The coefficient of λ^k in $\lambda(\lambda-1)\cdots(\lambda-n+1)$ is by definition the Stirling number $s(n,k)$ of the first kind [hence the name 'Whitney number of the *first* kind' for w_{n-k}, since by (7.9), the Whitney number $w_{n-k}(\Pi_n)$ equals the Stirling number $s(n,k)$].

Projective geometries. Consider L_q^n, the lattice of subspaces of the n-dimensional vector space over $GF(q)$, equivalently of the projective geometry PG_q^{n-1}. Let σ_k denote the k-th elementary symmetric function.

7.5.3. Proposition. *We have*

$$\begin{aligned} p(L_q^n;\lambda) &= (\lambda-1)(\lambda-q)(\lambda-q^2)\cdots(\lambda-q^{n-1}),\\ \mu(L_q^n) &= (-1)^n q^{\binom{n}{2}},\\ w_k(L_q^n) &= (-1)^k \sigma_k(1,q,q^2,\ldots,q^{n-1})\\ &= (-1)^k \sum_{0\leqslant i_1<i_2<\cdots<i_k<n} q^{i_1+i_2+\cdots+i_k},\\ \beta(L_q^n) &= (q-1)(q^2-1)\cdots(q^{n-1}-1). \end{aligned}$$

Proof. Excercise. □

From this proposition it is possible to compute $W_k(L_q^n)$, the number of distinct $(k-1)$-dimensional subspaces of PG_q^{n-1}. See Exercise 7.31 (*c*).

7.6. The Critical Problem

The problem of coloring a graph is solved by finding the smallest positive integral argument such that $\chi_\Gamma(\lambda) > 0$. In the matroidal analog introduced by Crapo and Rota (1970), colors become vectors over the finite field of order q and one must find the smallest positive integral exponent d for which $p(M; q^d) > 0$.

The problem concerns a set E of vectors in the n-dimensional vector space K^n over $K = GF(q)$. Let $M(E)$ be the linear dependence matroid of E and $L(E)$ the lattice of flats of $M(E)$. A set of linear functionals $f_i: K^n \to K$ is said to *distinguish* E if for each point $p \in E$ some functional is non-zero on p; or in other words the intersection of the hyperplanes $\operatorname{Ker} f_i$ is disjoint from E. The *critical problem* is to find the smallest size of a distinguishing set for E. We call this number c the critical exponent of E.

7.6.1. Theorem. [*Critical Theorem* (*Crapo and Rota 1970, Theorem 16.1*)] *Let $E \subseteq K^n, m = \dim E$, and $d \geqslant 0$. The number of* (*ordered*) *d-tuples of linear functionals which distinguish E* (*equivalently, the number of linear mappings $f: K^n \to K^d$ whose kernel avoids E*) *is equal to $(q^d)^{n-m} p(M(E); q^d)$.*

The most important conclusion to be drawn is that *the critical exponent of E is the smallest non-negative integer c such that $p(M(E); q^c) > 0$.* We also see:

7.6.2. Corollary. *Let E be a non-empty subset of a linear* (*or projective*) *space over GF(q), not containing the zero vector. Then there is an integer $c > 0$ such that $p(M(E); q^d) = 0$ if $0 \leqslant d < c$ but $p(M(E); q^d) > 0$ for all $d \geqslant c$.* □

Proof of Theorem. The proof is similar to that of Proposition 7.5.1. First we observe that, given $X \subseteq K^n$ with $\dim X = e$, the number of linear mappings $f: K^n \to K^d$ whose kernel contains X is $q^{d(n-e)}$; for if we extend X to a spanning set by adjoining $p_{e+1}, \ldots, p_n$, we get such an f by setting $f|X = 0$ and choosing $f(p_i)$ arbitrarily from among the q^d vectors of K^d for $i = e+1, \ldots, n$. Now for each $F \subseteq K^n$, let us write $\nu(F)$ for the number of linear $f: K^n \to K^d$ such that $E \cap \operatorname{Ker} f = F$. Obviously $E \cap \operatorname{Ker} f$ is closed in $M(E)$, so we have for each $X \in L(E)$:

$$\sum_{F \geqslant X} \nu(F) = (q^d)^{n-e}.$$

After Möbius inversion and setting $X = 0 = \operatorname{cl} \varnothing$,

$$\sum_{F \in L(E)} \mu_E(0, F)(q^d)^{n - \dim F} = \nu(0).$$

But the left-hand side equals $(q^d)^{n-m} p(L(E); q^d)$. Modulo obvious remarks about the case where $\varnothing$ is not closed, this is the theorem. □

The case of critical exponent 1 is easy to interpret geometrically. A combinatorial geometry is *affine* if it is isomorphic to the affine dependence matroid of a point set in an affine geometry AG_q^n. (We regard q as fixed.) A subset of PG_q^n is *affinely embedded* if it lies in the complement of a hyperplane.

Clearly $M(E)$ is affine if E is affinely embedded. We have the following converse and criterion. (The criterion, i.e., $c=1$, is Theorem 16.2 of Crapo and Rota 1970. It is a q-analog of the Two-Color Theorem of graph theory; see below.)

7.6.3. Corollary. *Let $E \subseteq PG_q^n$. The following are equivalent:*

(i) *E is affinely embedded.*
(ii) *$M(E)$ is affine.*
(iii) *E has critical exponent* 1.

Proof. Exercise. □

The Critical Theorem shows in principle how to find the critical number (although drawing conclusions in specific cases is another matter!), but what it counts is not very geometrical. One can deduce more complicated expressions for the number of d-tuples of hyperplanes (as distinct from functionals) which distinguish E and the number of e-dimensional subspaces which avoid E.

7.6.4. Corollary. *Let $E \subseteq K^n$ and let $m = \dim E$. (Or let $E \subseteq PG_q^{n-1}$ and $m = 1+\dim E$.) The number of d-tuples of hyperplanes which distinguish E (i.e., whose intersection avoids E) is equal to*

$$(q-1)^{-d}\sum_{e=0}^{d}(-1)^{d-e}(q^e)^{n-m}p(M(E);q^e)$$

$$=\sum_{k=0}^{m} w_k(M(E))\left(\frac{q^{n-k}-1}{q-1}\right)^d.$$

Proof. Let κ_d (respectively ν_d) be the number of d-tuples of hyperplanes (respectively functionals) that distinguish E. We have to take account of two factors: some functionals are 0 (not corresponding to any hyperplane), and one hyperplane corresponds to $q-1$ functionals.

We can obtain all d-tuples f of functionals that distinguish E in the following way. First we choose $e = 0, 1, \ldots,$ or d (e will be the number of nonzero functionals in f) and one of the κ_e e-tuples of distinguishing hyperplanes, $h = (h_1, h_2, \ldots, h_e)$. Next for each h_j we pick one of the $q-1$ functionals g_j with h_j for kernel. Then we pick e indices, $1 \leqslant i_1 < i_2 < \cdots < i_e \leqslant d$, and we let $f_{i_j} = g_j$, but $f_i = 0$ if i is not one of the selected indices. This determines f, and since the e-tuple h is recoverable from f, we obtain in this way all possible f. So

$$\nu_d = \sum_{e=0}^{d}\kappa_e(q-1)^e\binom{d}{e}.$$

Inverting this binomial relation,

$$\kappa_d = (q-1)^{-d}\sum_{e=0}^{d}(-1)^e\binom{d}{e}\nu_e.$$

We obtain the value of ν_e from the Critical Theorem.

The alternate form of κ_d arises upon expanding $p(M(E);q^d)=\sum w_k(M(E))(q^{m-k})^d$ and rearranging the sum. □

Finally, we have the most geometrical version of the Critical Theorem. But first this lemma.

7.6.5. Lemma. *Let x be an $(n-e)$-dimensional subspace of K^n. The number of linear mappings $f:K^n\to K^d$ whose kernel is x equals*

$$(q^d-1)(q^d-q)\cdots(q^d-q^{e-1}),$$

interpreted as 1 *if* $e=0$.

Proof. There is a one-to-one correspondence between such f and the mappings $\bar{f}:K^n/x\to K^d$ with zero kernel. To count the latter is a critical problem: we want the number of mappings $\bar{f}:K^e\to K^d$ whose kernel avoids $E=K^e-\{0\}$. This number is $p(M(E);q^d)$. But we know that polynomial from Proposition 7.5.3 since $L(E)\cong L_q^e$. So we have the lemma. □

7.6.6. Proposition. (*Dowling 1971, Theorem 2, p. 220*) *Let $E\subseteq K^n$ have dimension m. The number of $(n-d)$-dimensional subspaces of K^n not meeting E is equal to*

$$\sum_{e=0}^{d}\frac{(-1)^e(q^{d-e})^{n-m}p(M(E);q^{d-e})}{(q^e-1)(q^{e-1}-1)\cdots(q-1)(q^{d-e}-1)(q^{d-e}-q)\cdots(q^{d-e}-q^{d-e-1})}.$$

Notice that the terms with $e>d-c$, c the critical exponent of E, are all 0.

Proof. Let σ_{n-d} denote the number of $(n-d)$-dimensional subspaces avoiding E. We will set up and solve a recurrence for σ_{n-d}.

Each subspace counted by σ_{n-e} is the kernel of the number of mappings $K^n\to K^d$ given by Lemma 7.6.5. So the total number of mappings $K^n\to K^d$ whose kernels avoid E is given by

$$\sum_{e=0}^{d}\sigma_{n-e}\prod_{i=0}^{e-1}(q^d-q^i).$$

The number of such mappings is also given by the Critical Theorem; thus we have

$$(q^d)^{n-m}p(M(E);q^d)=\sum_{e=0}^{d}\sigma_{n-e}\prod_{i=0}^{e-1}(q^d-q^i).$$

The trick is to rewrite this as an identity involving the *Gaussian coefficients*,

$$\begin{bmatrix} d \\ e \end{bmatrix}=\frac{(q^d-1)(q^{d-1}-1)\cdots(q^{d-e-1}-1)}{(q^e-1)(q^{e-1}-1)\cdots(q-1)},$$

which is to be proved in Exercises 7.5 and 7.31 to equal the number of

e-dimensional subspaces of K^d. That is, we want to prove

$$(q^d)^{n-m}p(M(E);q^d) = \sum_{e=0}^{d} \sigma_{n-e} \begin{bmatrix} d \\ e \end{bmatrix} \prod_{i=0}^{e-1} (q^e - q^i). \tag{7.10}$$

Equation (7.10) has the form

$$a_d = \sum_{e=0}^{d} b_e \begin{bmatrix} d \\ e \end{bmatrix}, \tag{7.11}$$

valid for all $d \geqslant 0$. We wish to solve for b_e. That we can do by defining, for $x \in L_q^n$ with dim $x = d$,

$$a(x) = a_d \quad \text{and} \quad b(x) = b_d.$$

Now (7.11) can be written

$$a(x) = \sum_{y \leqslant x} b(y),$$

which by Möbius inversion in L_q^n becomes

$$b(x) = \sum_{y \leqslant x} a(y)\mu(x, y).$$

The interval $[x, y]$ being a projective geometry, its Möbius invariant is given by Proposition 7.5.3; converting back to the notation of (7.11) we have

$$b_d = \sum_{e=0}^{d} a_{d-e}(-1)^e q^{\binom{e}{2}} \begin{bmatrix} d \\ e \end{bmatrix}.$$

The result of inverting (7.10) in this fashion is

$$\sigma_{n-d} \prod_{i=0}^{d-1} (q^d - q^i) = \sum_{e=0}^{d} (-1)^e q^{\binom{e}{2}} \begin{bmatrix} d \\ e \end{bmatrix} (q^{d-e})^{n-m} p(M(E); q^{d-e}).$$

Isolating σ_{n-d} and simplifying yields the result. □

7.6.7. Corollary. *The largest dimension of a substance of K^n not meeting E is $n - c$, where c is the critical exponent of E.* □

7.6.8. Example. *Independent sets.* Any independent set of points has critical exponent 1 and therefore lies in the complement of a hyperplane in K^n.

Graph coloring as a critical problem. Since a graphic matroid can be represented by vectors over any field, it has a critical problem for each prime power q. Let Γ, a graph with n vertices, be represented by the vector set $E(\Gamma) \subseteq K^n$, where $K = GF(q)$, in the usual way: vertex v_i corresponds to the i-th coordinate and an edge e_{ij} corresponds to the vector $p_i - p_j$ (or $p_j - p_i$), $\{p_i\}$ being the standard basis of K^n. Each linear mapping $f: K^n \to K^d$ corresponds to a coloring of Γ by K^d, that is, a map $\gamma: V(\Gamma) \to K^d$ defined by $\gamma(v_i) = f(p_i)$; and conversely each γ determines one linear mapping f. Moreover, f distinguishes $E(\Gamma)$ if and only if, for each edge e_{ij} of Γ, $f(p_i - p_j) \neq 0$; in other words, γ is a proper coloring. So in the graphic case the Critical Theorem says that $\chi(\Gamma; q^d)$ *is the number of proper colorings of* Γ *by vectors in* K^d; the critical exponent is the smallest dimension d for which there is a proper coloring by K^d. (One should now reread Corollary 7.6.3 as a q-color theorem!)

The most interesting case is the binary one, for the statement: *the critical exponent of a planar graph, over* $GF(2)$, *is at most* 2, is the Four-Color Theorem. An aim of Crapo and Rota in formulating the critical problem was to put the Four-Color Problem in a general setting which might lead to techniques powerful enough to solve it and other problems of the type. ('The fact that the problem of coloring a graph was the first historically to arise, was a distressing accident, which prevented it from being studied at that level of generality which has been found indispensible in solving most problems of mathematics.') It must be admitted that this hope has not yet been realized, although it is undoubtedly worthy of continued pursuit.

Linear codes and the critical problem. Another example was pointed out by Dowling (1971). A *linear code* in K^n with *distance d* is a linear subspace whose non-zero vectors have minimum weight d. (The *weight* of a vector is the number of non-zero coordinates.) The problem of linear coding theory is to find large codes with given dimension and given (or bigger) distance. Suppose we let

$$E_\delta = \{p \in K^n\colon\ 0 \leqslant \mathrm{wt}(p) \leqslant \delta\},$$

and c_δ = the critical exponent of E_δ. Then a code with distance $> \delta$ is merely a subspace avoiding E_δ; by the Critical Theorem the largest dimension of such a subspace is $n - c_\delta$ and its size is q^{n-c_δ}. So if we can calculate $p(M(E_\delta);\lambda)$ we will know the maximum size of a linear code with distance $> \delta$.

This is a difficult calculation in general, although easy when $\delta = 1$ (Exercise). Dowling accomplished the calculation for $\delta = 2$. Then $L(E_2)$ is the *Dowling lattice* $Q_n(K^*)$ of the multiplicative group K^* of K (Dowling 1973a; for the Dowling lattices of any finite group see Dowling 1973b). The characteristic polynomial of $Q_n(K^*)$ evaluated at q^d equals

$$(q-1)^n\left(\frac{q^d-1}{q-1}\right)\left(\frac{q^d-1}{q-1}-1\right)\cdots\left(\frac{q^d-1}{q-1}-n+1\right),$$

by Dowling's results. Thus c_2 is the integer such that

$$2^{c_2-1} \leqslant n < 2^{c_2}, \quad \text{if} \quad q = 2, \text{ or}$$

$$\frac{q^{c_2-1}-1}{q-1} < n \leqslant \frac{q^{c_2}-1}{q-1}, \quad \text{if} \quad q > 2.$$

Then we know the maximum size of a linear code over $GF(q)$ that corrects one error (which is what $\delta = 2$ signifies). This problem was what led Dowling to investigate his lattices and thence to the theory of Dowling (1973b).

Unfortunately, for $\delta \geqslant 3$ this approach does not succeed. The reason is roughly that $M(E_2)$ is essentially graphic, as one can see from the presentation given in Dowling (1973a, p. 109); moreover, it is supersolvable. For larger δ, $M(E_\delta)$ is no longer graphic; the techniques to calculate its characteristic polynomial have not been discovered. This is one of the important open problems in matroid theory.

A different connection between linear codes and the critical problem and also one between codes and the rank generating function (Section 7.4) are developed in Greene (1976).

Exercises

7.1. Prove Proposition 7.1.1 using the recursive definition, equations (7.1)–(7.3).

7.2. Prove Proposition 7.1.2: first from the definition of μ, then using the incidence algebra.

7.3. (a) Evaluate $\mu(U_{rm})$ (Example 7.1.5).

(b) Find and factor the characteristic polynomial of the m-point line U_{2m}.

(c) Deduce Example 7.2.2 from Proposition 7.2.1. Calculate the Whitney numbers of the first kind of U_{rm}, B_m, C_m.

7.4. (a) For the partition lattice Π_n, evaluate $\mu(\Pi_n)$:

(i) from the definition (7.1.) for $n = 4$;

(ii) from the alternative recurrence (Proposition 7.1.2) (Frucht and Rota 1963).

(iii) Deduce that, if $\pi \leqslant \tau$ in Π_n and π partitions n_i different blocks of τ into i parts each for $i = 1, 2, 3, \ldots,$ then

$$\mu(\pi, \tau) = (-1)^{|\pi| - |\tau|}(1!)^{n_2}(2!)^{n_3}(3!)^{n_4} \ldots .$$

(Schützenberger 1954)

(b) Deduce a formula for $p(\Pi_n; \lambda)$ from the definition of the characteristic polynomial and Exercise 7.4(a). What are the Whitney numbers $w_k(\Pi_n)$?

7.5. (a) For the lattice L_q^n of the projective geometry PG_q^{n-1} of dimension $n - 1$ over $GF(q)$, evaluate $\mu(L_q^n)$. Then calculate $\mu(L(AG_q^{n-1}))$, where AG_q^{n-1} is the affine geometry. (You may express the result in terms of the numbers $W_k(L)$ of rank k subspaces of PG_q^{n-1}.)

(b) Find the characteristic polynomial and Whitney numbers of the first kind of L_q^n, based on your solution to (a). Do the same for $L(AG_q^{n-1})$.

7.6. Let V_n consist of all the points in the real affine space $AG^n(\mathbb{R})$ with coordinates ± 1; we call this the *verticial hypercube*. If $n = 3$, it is called the real affine cube. For the geometric lattice of its affine dependence matroid, compute the Möbius invariant and the characteristic polynomial when $n \leqslant 3$. The general problem is unsolved, difficult, and important. It would yield an exact formula for the number of threshold switching functions of n variables (Winder 1966; Zaslavsky 1975, Section 5F).

7.7. (a) Let $\hat{D}_n$ consist of all the points in the real vector space $\mathbb{R}^n$ with exactly two non-zero coordinates, whose values are in the set $\{+1, -1\}$. Let $\hat{B}_n$ be $\hat{D}_n$ with the unit basis vectors adjoined. Let L denote the lattice of the linear dependence matroid. Compute $\mu(L(\hat{D}_n))$ and $\mu(L(\hat{B}_n))$ for $n \leqslant 3$, then $n = 4$ if time allows. [For general n, see Zaslavsky (1981).]

(b) Like Exercise 7.5(b) but for $\hat{D}_n$ and $\hat{B}_n$. *Hint*: $p(L(\hat{B}_n); \lambda) = (\lambda - 1)(\lambda - 3) \cdots (\lambda - 2n + 1)$.

7.8. Prove Proposition 7.1.3.

7.9. Prove Proposition 7.1.4. *Hints*: For the case $W \notin L$, factor the sum. For $W \in L$, define the function

$$\phi(W, F) = \sum_{\substack{W \subseteq X \subseteq F \\ \text{cl} X = F}} (-1)^{|X - W|}$$

and employ the incidence algebra.

7.10. Prove Theorem 7.1.7 (ii). *Hint*: Use Proposition 7.1.4.

7.11. Prove that the sum $i_0 - i_1 + i_2 - \cdots \pm i_r$, where i_k is the number of independent sets of rank k in a matroid M of rank r, equals zero if and only if M has an isthmus. *Hint*: Use Proposition 7.1.4.

7.12. Prove Rota's sign theorem, Theorem 7.1.8, from Weisner's theorem, Proposition 7.1.6. (Rota 1964)

7.13. [Philip Hall's Theorem: Hall 1936, (2.21); Rota 1964, Proposition 6, p. 346.] For $x, y \in P$ and $i \geqslant 0$, let $c_i(x, y)$ be the number of chains $x = x_0 < x_1 < \cdots < x_i = y$ of length i from x to y. Let

$$\phi(x, y) = c_0(x, y) - c_1(x, y) + c_2(x, y) - c_3(x, y) + \cdots.$$

Prove that $\mu(x, y) = \phi(x, y)$.

7.14. Prove Theorem 7.2.4 in a manner analogous to the proof of Theorem 7.1.7.

7.15. If $x \in L$ is modular, $L(x) = \{y \in L\colon\ y \wedge x = 0\}$, and $p(L(x); \lambda) = \sum\{\mu(0, y)\lambda^{r(L) - r(x) - r(y)}\colon\ y \in L(x)\}$, is $(\lambda - 1)p(L(x); \lambda)$ always the characteristic polynomial of a matroid? (Brylawski 1975, Section 7)

7.16. Discover and prove an analog of Proposition 7.2.9 for the generalized parallel connection of M_1 and M_2 along a common modular flat F (Brylawski 1975, Section 5; see White 1986, Chapter 9. *Hint:* Remember Stanley's theorem, Theorem 7.2.5 (Brylawski 1975, Theorem 7.8)).

7.17. Prove Proposition 7.3.1.

7.18. Prove Theorem 7.3.2(c), (a). Also show that $\beta(M) = 0$ when M is disconnected.

7.19. Use Theorem 7.3.2 to evaluate the beta invariant of (a) the m-point line U_{2m} and (b) Π_4.

7.20. Determine the value of $\beta(U_{rm})$. For which values of m and r is U_{rm} a series-parallel matroid?

7.21. Calculate β for the examples of Exercises 7.5, 7.6, 7.7. Is any one a series-parallel matroid?

7.22. Prove that $\beta(L) = (-1)^{r(L)-1}\prod\{\mu(0, x)\colon x \in L, x \ngeqslant a\}$ for every atom a of the geometric lattice L (Zaslavsky 1975, Section 7).

7.23. Calculate the rank generating function of U_{rm} directly from the definition.

7.24. Prove Proposition 7.4.1.

7.25. Prove Proposition 7.4.2. *Hint*: Use induction on the size of M.

7.26. Calculate $R(U_{rm}; u, v)$ from the Tutte–Grothendieck recurrence and the values for $m \leqslant 1$.

7.27. Compute $R(M(K_n);u,v)$, where $M(K_n)$ is the graphic geometry of the complete graph. How does your result, evaluated at $v = -1$ and $u = -\lambda$, compare with $p(\Pi_n;\lambda)$ from Exercise 7.4?

7.28. (a) Prove that Π_n is supersolvable. (*Hint*: What about a partition with only one non-singleton block?) Deduce (7.9) and $\mu(\Pi_n)$ and $\beta(\Pi_n)$.

(b) Prove (7.9) by graph theory *via* Proposition 7.5.1, since $\Pi_n \cong L(M(K_n))$.

(c) Compare (7.9) to your answer to Exercise 7.4(b). What Stirling number identity is thereby proved?

7.29. Prove Proposition 7.5.1 by the Tutte–Grothendieck method.

7.30. Prove Proposition 7.5.2.

7.31. (a) Prove that $W_k(L_q^n) = \dfrac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$ by counting ordered bases.

(b) Deduce p and μ of Proposition 7.5.3 from supersolvability (Stanley 1972, Example 4.2).

(c) Compare with your results from Exercise 7.5(a). Deduce that

$$W_k(L_q^n) = \sum_{0 \leqslant j_1 \leqslant j_2 \leqslant \cdots \leqslant j_k \leqslant n-k} q^{j_1+j_2+\cdots+j_k}.$$

7.32. (a) Calculate the critical exponent over $K = GF(q)$ of an m-point line $U_{2m}, 2 \leqslant m \leqslant q+1$. Is U_{2m} affine in PG_q^{n-1}?

(b) The same, for a circuit C_{r+1} of rank $r \geqslant 3$. Is C_{r+1} affine in PG_q^{n-1}? *Hint*: Almost always.

(c) The same, for U_{rm} where $2 < r < m-1$. (Assume U_{rm} is such that it embeds in PG_q^{n-1}.)

7.33. How many hyperplanes avoid a fixed non-empty set $E \subseteq K^n$? How many $(n-2)$-dimensional subspaces?

7.34. Prove Example 7.6.8. How many $(n-d)$-dimensional subspaces avoid a fixed basis?

7.35. If $q = p^e, PG_p^n$ is a spanning subset of PG_q^n. What is its critical exponent?

7.36. Prove Corollary 7.6.3.

7.37. Deduce Corollary 7.6.7 directly from the Critical Theorem.

7.38. Calculate the critical exponent of the set $\hat{A}_n$ of all vectors in K^{n+1} with exactly two non-zero coordinates, one equal to $+1$ and the other equal to -1 (note that $+1 = -1$, if q is even). *Hint*: $M(\hat{A}_n) \cong M(K_{n+1})$, the complete-graph matroid.

7.39. What is the critical exponent of $\hat{B}_n$? (See Exercise 7.7. Assume q is odd. *Hint*: The matroid of $\hat{B}_n$ is the same for $K = \mathbb{R}$ and $K = GF(q)$ as long as q is odd.)

7.40. (a) Calculate the critical exponent c_1 of E_1. What is the maximum size of a linear code with distance $\geqslant 2$ (a code that detects one error)?

(b) Express compactly the maximum size of a linear code with distance $\geqslant 3$ (a code that corrects one error).

References

Aigner, M. (1979). Combinatorial Theory. *Grundlehren der Math. Wiss.* **234**, Springer-Verlag, Berlin–New York.

Birkhoff, G.D. (1912). A determinant formula for the number of ways of coloring a map. *Annals of Math.* (2) **14**, 42–6.

Brylawski, T.H. (1971). A combinatorial model for series-parallel networks. *Trans. Amer Math. Soc.* **154**, 1–22.

Brylawski, T.H. (1972). A decomposition for combinatorial geometries. *Trans Amer. Math. Soc.* **171**, 235–82.

Brylawski, T.H. (1975). Modular constructions for combinatorial geometries. *Trans Amer. Math. Soc.* **203**, 1–44.

Crapo, H.H. (1967). A higher invariant for matroids. *J. Comb. Theory* **2**, 406–17.

Crapo, H.H. (1970). The Tutte polynomial. *Aequationes Math.* **3**, 211–29.

Crapo, H.H. and Rota, G.C. (1970). *On the Foundations of Combinatorial Theory: Combinatorial Geometries* (preliminary edition). MIT Press, Cambridge, Mass.

Dowling, T.A. (1971). Codes, packings, and the critical problem, in *Atti del Convegno di Geometria Combinatoria e Sue Applicazioni* (*Perugia, 1970*), pp. 209–24. Ist. Mat., Univ. di Perugia, Perugia, Italy.

Dowling, T.A. (1973a). A q-analog of the partition lattice, in *A Survey of Combinatorial Theory*, (J.N. Srivastava *et al*., eds.), pp. 101–15. North-Holland, Amsterdam.

Dowling, T.A. (1973b). A class of geometric lattices based on finite groups. *J. Comb. Theory Ser. B* **14**, 61–86. Erratum, *ibid.* **15**, 211.

Essam, J.W. (1971). Graph theory and statistical physics. *Discrete Math.* **1**, 83–112.

Frucht, W.L. and Rota, G.C. (1963). La función de Möbius para paritiones de un conjunto. *Scientia* (*Valparaíso, Chile*) **122**, 111–15.

Greene, C. (1976). Weight enumeration and the geometry of linear codes. *Stud. Appl. Math.* **55**, 119–28.

Hall, P. (1936). The Eulerian functions of a group. *Quarterly J. Math.* **7**, 134–51.

Oxley, J.G. (1982). On Crapo's beta invariant for matroids. *Stud. Appl. Math.* **66**, 267–77.

Rota, G.C. (1964). On the foundations of combinatorial theory, I. Theory of Möbius functions. *Z. Wahrscheinlichkeitstheorie verw. Gebiete* **2**, 340–68.

Schützenberger, M.P. (1954). Contribution aux applications statistiques de la théorie de l'information, in *Publ. Inst. Statist. Univ. Paris 3*, Nos. 1–2, pp. 3–117.

Stanley, R.P. (1971). Modular elements of geometric lattices. *Algebra Universalis* **1**, 214–17.

Stanley, R.P. (1972). Supersolvable lattices. *Algebra Universalis* **2**, 197–217.

Tutte, W.T. (1947). A ring in graph theory. *Proc. Camb. Phil. Soc.* **43**, 26–40.

Weisner, L. (1935). Abstract theory of inversion of finite series. *Trans. Amer. Math. Soc.* **38**, 474–92.

White, N.L., ed. (1986). *Theory of Matroids.* Cambridge University Press.

Whitney, H. (1932). A logical expansion in mathematics. *Bull. Amer. Math. Soc.* **38**, 572–9.

Winder, R.O. (1966). Partitions of N-space by hyperplanes. *SIAM J. Appl. Math.* **14**, 811–18.

Zaslavsky, T. (1975). Facing up to arrangements: Face-count formulas for partitions of space by hyperplanes. *Mem. Amer. Math. Soc.* **1**, Issue 1; No. 154.

Zaslavsky, T. (1981). The geometry of root systems and signed graphs. *Amer. Math. Monthly* **88**, No. 2 (February).