ON THE APPLICATIONS OF MOBIUS INVERSION IN COMBINATORIAL ANALYSIS

E. A. BENDER AND J. R. GOLDMAN

1. Introduction. Inversion of a finite series is one of the most useful tools in combinatorics and probability. The classical inclusion-exclusion principle is a special case (Feller (1968), Ryser (1963)). Although many inversion problems can be phrased in terms of inclusion-exclusion, the framework often seems artificial. Frequently a "natural" ordering of the objects being studied is possible. This is the gestalt of the technique of Möbius inversion.

Möbius inversion is an overcounting-undercounting, or sieving, procedure. We keep track of the over and undercount by indexing with the elements of a partially ordered set which classically was the subsets of a finite set. The Möbius inversion formula of number theory as given in Hardy and Wright (1960) indexes functions with the set of positive integers under the divisibility order. This latter formula lends its name to the general subject.

The principle of inclusion-exclusion, which after all is not a very deep statement, was investigated by several 19th century mathematicians and perhaps stated most clearly by Poincaré. It has been rediscovered many times in varying degrees of generality. A fairly complete development of this principle together with a history and development of classical applications in probability theory is given in the monograph of Fréchet (1940, 1943).

The statement of the general Möbius inversion formula was first given independently by Weisner (1935) and Philip Hall (1936); both authors were motivated by group theory problems. Neither author seems to have been aware of the combinatorial implications of his work and neither developed the theory of Möbius functions. In a fundamental paper on Möbius functions, Rota (1964) showed the importance of this theory in combinatorial mathematics and gave a deep treatment of it. He noted the relation between such topics as inclusion-exclusion, classical number theoretic Möbius inversion, coloring problems and flows in networks. Since then, under the strong influence of Rota, the theory of Möbius inversion and related topics has become an active area of combinatorics.

Here we present many applications of Möbius inversion in combinatorics with emphasis on recent results. This paper complements Rota's original paper (1964) (also to be referred to as Foundations I) in that Rota developed the theory of the Möbius function as related to the structure of the ordering. Foundations I contains an extensive bibliography. We have not reproduced this here but we have attempted to bring it up to date.

We begin with a series of examples to motivate the framework of Möbius inversion.

Example 1. *Finite Series.* Let $f(n)$ be a function on the positive integers (i.e., a series $f(1)$, $f(2)$, $f(3), \cdots$) and let $g(n) = \Sigma_{m \leq n} f(m)$. We invert the sum, i.e., express $f(n)$ in terms of g; the answer is obviously

$$f(n) = g(n) - g(n-1). \tag{1}$$

Example 2. *Inclusion-Exclusion Principles.* Given a set $S = \{s_1, s_2, \cdots, s_k\}$ and a collection of properties $P = \{p_1, p_2, \cdots, p_n\}$. A property p_i is defined by stating which elements have it and which do not (hence a property is subset of S; viz., those elements which satisfy it). For any collection T of properties, $T \subseteq P$, let $N_{\geqq}(T)$ (read "N sub $\geqq$ of T") be the number of elements of S which satisfy every property in *T and possibly others.* Let $N_{=}(T)$ be the number of elements which satisfy exactly the properties in *T and no others.* Clearly

$$N_{\geqq}(T) = \sum_{X \supseteq T} N_{=}(X),$$

for every element which satisfies at least all properties in T satisfies exactly some set X of properties where $X \supseteq T$. Our problem is to solve for $N_=(T)$ in terms of the function $N_\geq(X)$. Frequently we want $N_=(\emptyset)$, the number of elements satisfying no properties.

Example 3. *Classical Möbius Inversion.* The following problem from number theory motivates some of our general terminology and results. Let $f(n)$ be a function defined on the positive integers and define

$$h(n) = \sum_{k|n} f(k)$$

where "$k \mid n$" is read "k divides n" and the summation is therefore over all integral divisors of n. We wish to invert the sum, i.e., solve for $f(n)$ in terms of h. The problem is solved in many elementary number theory texts. See, for example, Hardy and Wright (1960). We shall derive it as a special case of a more general theory.

Example 4. *Spanning Sets of a Vector Space.* How many subsets of $V_n(q)$, the n-dimensional vector space over a field of q elements, span the whole space? For any subspace U of $V_n(q)$ let $N_=(U)$ be the number of subsets of vectors of V_n which span U. Let $N_\leq(U)$ be the number of sets spanning U or a subspace of U. Then we have $N_\leq(U) = \Sigma_{V \subseteq U} N_=(V)$ where the sum is over all subspaces of U. Our problem is to solve for $N_=(U)$ in terms of $N_\leq(U)$ and set $U = V_n(q)$.

Our four examples have a number of common ideas which we abstract in the following table:

		Example 1	Example 2	Example 3	Example 4
(i)	A set S	Positive Integers	Subsets of P	Positive Integers	Subspaces of $V_n(q)$
(ii)	An "order" relation	$\leq$	$\supseteq$ (Set inclusion)	$\mid$ divisibility	is a subspace of ($\leq$)
(iii)	A given function on S	$f(n)$	$N_=(T)$	$f(n)$	$N_=(U)$
(iv)	A summation function	$g(n) = \sum_{m \leq n} f(m)$	$N_\geq(T)$ $= \sum_{X \supseteq T} N_=(X)$	$h(n) = \sum_{k\|n} f(k)$	$N_\leq(U) = \sum_{V \leq U} N_=(V)$

In each case we want to invert a system of linear equations, i.e., solve for the given function in terms of the summation function. The summation function is with respect to a given "ordering." This ordering generalizes the usual notion of order for integers or real numbers.

To study the inversion problem in its proper generality we now review the theory of "order" relations or, as they are more commonly known, "partially ordered sets."

2. Partially ordered sets.

DEFINITION: *A partially ordered set* (*POS*) $\Sigma = (S, \leqq)$ is a pair consisting of a set S and a binary relation $\leqq$ on S, satisfying the following properties:

(a) (reflexive) $x \leqq x$ for all $x \in S$,

(1) (b) (transitive) if $x \leqq y$ and $y \leqq z$ then $x \leqq z$,

(c) (anti-symmetric) if $x \leqq y$ and $y \leqq x$ then $x = y$.

We read "$x \leqq y$" as "x is less than or equal to y." Partially ordered sets are also called *ordered* *sets*. The notation and terminology of ordered sets is similar to that for ordinary inequality, e.g., $x < y$ means $x \leqq y$ and $x \neq y$, and $x \nleqq y$ means $x \leqq y$ is not true.

What distinguishes ordered sets from ordinary inequality is that elements may be "incomparable." x and y are *incomparable* if $x \leqq y$ is false and $y \leqq x$ is also false. If for every two elements x, y either $x \leqq y$ or $y \leqq x$ is true, then $\Sigma = (S, \leqq)$ is called a *linearly ordered set* or a *chain.*

Example 1. (a) *Integers with ordinary ordering*: Let S be the positive integers Z^+ or all integers Z with the usual ordering ($a \leqq b$ if and only if $b - a$ is positive). $\Sigma = (S, \leqq)$ is linearly ordered.

(b) Let S be the integers between 1 and n with the ordinary ordering. $(S, \leqq)$ is a linearly ordered set.

(c) *Subsets of a set* (Boolean algebra) (see Example 1.2): Let T be a set and S the collection 2^T of subsets of T. If $A, B \subseteq T$, then $A \leqq B$ iff $A \subseteq B$ (A is a subset of B). $(S, \leqq)$ is not a linearly ordered set, e.g., any two 1 element subsets are incomparable. This ordered set is often called the "subsets of T ordered by *inclusion.*"

(d) *Integers under divisibility* (see Example 1.3): Let S be the positive integers and let $a \leqq b$ iff $a \mid b$ (a divides b). Let Δ denote this *POS.*

(e) *Divisors of n*: Let S be all divisors of the integer n and let $a \leqq b$ mean $a \mid b$ as in the previous example. This *POS* will be denoted by Δ_n or $D(n)$.

(f) *Subspaces of a vector space* (see Example 1.4): Let S be the set of subspaces of a vector space and let $\leqq$ mean "is a subset of."

(g) In general, given any "mathematical system," the "sub-systems" ordered by inclusion, form a partially ordered set, e.g., subgroups of a group.

DEFINITION: An *interval* $[x, y]$ is the set of all elements "between" x and y, i.e., $[x, y] = \{z \in S \mid x \leqq z \leqq y\}$. However, by an abuse of language, we sometimes use $[x, y]$ to denote the induced sub-*POS.* $(\{z \in S \mid x \leq z \leq y\}, \leq)$. A partially ordered set is *locally finite* if every interval has a finite number of elements.

Example 2. (a) The real numbers with the usual ordering is not locally finite.

(b) The *POS* of finite subsets of any set T is locally finite.

DEFINITION: Two partially ordered sets are *isomorphic* if they differ only by a labeling of their elements and ordering relation; more formally, $(S, \leqq)$ is *isomorphic* to $(S', \leqq')$, written $(S, \leqq) \cong (S', \leqq')$, if and only if there is a one-one onto map $\phi: S \to S'$ such that $x \leqq y$ if and only if $\phi(x) \leqq' \phi(y)$.

Example 3. *Subsets* (continued). Let $B(T_n)$ be the subsets of T_n ordered by inclusion, where $|T_n| = n$, and let S_n be the set of all n-tuples of zeros and ones with $a \leqq b$ meaning $a_i \leqq b_i$ for each of the n components of a and b. Let $\Sigma_n = (S_n, \leqq)$. We claim that $B(T_n) \cong \Sigma_n$: Let $t_1, \cdots, t_n$ be a listing of of elements of T_n. If $X \subseteq T_n$, define $\phi(X) = x = (x_1, \cdots, x_n) \in S_n$, where

$$x_i = \begin{cases} 0 & \text{if } t_i \notin X \\ 1 & \text{if } t_i \in X \end{cases}.$$

It is easy to see that ϕ is an isomorphism.

3. Möbius inversion. We can now formulate and solve the general inversion problem discussed in Section 1. Proofs are given in Foundations I.

THEOREM 1: MÖBIUS INVERSION FORMULA I. *Let $N_=(x)$ be a real valued function defined for all x in a locally finite partially ordered set $(S, \leqq)$ and assume there is an element $m \in S$ such that $N_=(x) = 0$ when $x \nleqq m$. Define $N_{\geqq}(x)$ by*

$$N_{\geqq}(x) = \sum_{y: y \geqq x} N_=(y). \tag{1a}$$

Then

$$N_=(x) = \sum_{y:y \geqq x} \mu(x,y) N_\geqq(y), \tag{1b}$$

where $\mu(x,y)$, *the Möbius function of* $(S, \leqq)$, *is an integer valued function of two variables on* S *defined by* $\mu(x,z) = 0$ *when* $x \nleqq z$ *and, when* $x \leqq z$, *by*

$$\sum_{y:x \leqq y \leqq z} \mu(x,y) = \delta(x,z). \tag{2}$$

($\delta(x,z)$, *the Kronecker delta, is given by* $\delta(x,x) = 1$, $\delta(x,z) = 0$ *if* $x \neq z$.)

NOTE: The condition $N_=(x) = 0$ when $x \nleqq m$ assures that all sums in our theorem are finite. Conditions under which infinite sums are allowed remains an open question (see Hille (1937)).

NOTE: It is not necessary to restrict $N_=(x)$ to real valued functions.

THEOREM 2: MÖBIUS INVERSION FORMULA II. *Let* $(S, \leqq)$ *be a locally finite partially ordered set. Let* $N_=(x)$ *be defined for all* $x \in S$ *and let there be an* $l \in S$ *such that* $N_=(x) = 0$ *when* $x \ngeqq l$. *Define*

$$N_\leq(x) = \sum_{y:y \leq x} N_=(y). \tag{3a}$$

Then

$$N_=(x) = \sum_{y:y \leq x} \mu(y,x) N_\leq(y), \tag{3b}$$

where μ *is defined by* (2).

COROLLARY 1. *The Möbius function* μ *of a locally finite POS can be computed recursively by either of the formulae*

$$\mu(x,z) = -\sum_{y:x \leqq y < z} \mu(x,y), \qquad x < z, \tag{4a}$$

$$\mu(x,z) = -\sum_{y:x < y \leqq z} \mu(y,z), \qquad x < z, \tag{4b}$$

together with $\mu(x,x) = 1$.

COROLLARY 2. *If* $x \leqq y \leqq z \leqq w$ *in a locally finite partially ordered set* Σ, *then* $\mu(y,z)$ *in* Σ *equals* $\mu(y,z)$ *in* $[x,w]$. (The "surroundings" don't matter — only the interval on which you want μ.)

COROLLARY 3. *If* Σ *and* Σ' *are isomorphic P.O.S's with Möbius functions* μ *and* μ' *and if* $[x,y] \cong [x',y']$, *then* $\mu(x,y) = \mu'(x',y')$.

Example 1. *Integers* (continued). If S is the set of integers with the usual ordering, the Möbius function is given by $\mu(n,n) = 1$, $\mu(n,n+1) = -1$, and $\mu(n,k) = 0$ otherwise. This follows immediately since we have already solved the inversion problem in equation (1.1) and we need only compare the coefficients of the terms in (1.1) with those of the general inversion formula in equation (3b). This is the method of undetermined coefficients. The Möbius function can also be derived from formula (4a) or (4b).

Direct products. Our main approach to computing Möbius functions will be to construct complicated *POS*'s from simple ones, compute μ for the simple sets by undetermined coefficients, and use these results to compute μ for complicated sets. Our construction tool is the "direct product." Other more sophisticated approaches are found in Rota (1964).

DEFINITION: Let $\Sigma_1=(S_1,\leqq_1)$ and $\Sigma_2=(S_2,\leqq_2)$ be *POS's*. The *direct product* $\Sigma=\Sigma_1\times\Sigma_2$ of Σ_1 and Σ_2 is the *POS* $(S,\leqq)$, where

(i) $S=S_1\times S_2=\{(a,b)\mid a\in S_1, b\in S_2\}$,

(ii) $a\leqq b$ in Σ if and only if $a_1\leqq_1 b_1$ and $a_2\leqq_2 b_2$,
where $a=(a_1,a_2)$ and $b=(b_1,b_2)$.

THEOREM 3: PRODUCT THEOREM. *If Σ_1 has Möbius function μ_1 and Σ_2 has Möbius function μ_2, then the Möbius function μ of $\Sigma_1\times\Sigma_2$ is given by*

$$\mu((x_1,x_2),(y_1,y_2))=\mu_1(x_1,y_1)\mu_2(x_2,y_2). \tag{5}$$

Example 2: *Inclusion-Exclusion, Subsets.* By Example 2.3 the Boolean algebra $B(T_n)$ is isomorphic to Σ_n, the set of n-tuples of 0's and 1's. But $\Sigma_n\cong\Sigma_1\times\overset{n\,\text{times}}{\cdots}\times\Sigma_1$. For Σ_1 and $y\geqq x$ we have $\mu(x,y)=(-1)^{y-x}$ since the only possibilities are $x=y$ or $x=0$, $y=1$. Under the isomorphism $B(T_n)\cong\Sigma_1\times\cdots\times\Sigma_1$, let $x\leftrightarrow(x_1,\cdots,x_n)$ and $y\leftrightarrow(y_1,\cdots,y_n)$, then

$$\mu(x,y)=\mu((x_1,\cdots,x_n),(y_1,\cdots,y_n))=\prod_{i=1}^{n}\mu(x_i,y_i)=(-1)^{\Sigma y_i-\Sigma x_i}=(-1)^{|y|-|x|}, \tag{6}$$

where $|y|$ is the number of elements in y. Substituting into equation (1b) we get

$$N_=(x)=\sum_{y\geqq x}(-1)^{|y|-|x|}N_{\geqq}(y),$$

the basic Inclusion-Exclusion Principle.

Example 3: *Divisors, Classical Möbius Inversion.* (See Examples 1.3 and 2.1e.) By the Unique Factorization Theorem $D(n)\cong D(p_1^{\alpha_1})\times\cdots\times D(p_s^{\alpha_s})$. Hence it suffices to compute μ on $D(p^\alpha)$. We have already done this because $D(p^\alpha)$ is the chain $1|p|p^2\cdots|p^\alpha$, which is isomorphic to the integers treated in Example 1. Hence

$$\mu(p^i,p^j)=\begin{cases}1 & \text{if}\quad i=j\\ -1 & \text{if}\quad j-i=1\\ 0 & \text{otherwise.}\end{cases}$$

By the product theorem

$$\mu\left(\prod_{i=0}^{s}p_i^{a_i},\prod_{i=0}^{s}p_i^{b_i}\right)=\begin{cases}(-1)^{\Sigma(b_i-a_i)} & \text{if}\quad b_i-a_i=0\quad\text{or}\quad 1\quad\text{for all}\quad i,\\ 0\quad\text{if}\quad b_i-a_i>1\quad\text{for some}\quad i.\end{cases}$$

Thus

$$\mu(a,b)=\mu(1,b/a)\equiv\mu(b/a), \tag{7}$$

where

$$\mu(n)=\begin{cases}1 & \text{if}\quad n=1\\ (-1)^k & \text{if}\quad n\quad\text{is a product of}\quad k\quad\text{distinct primes}\\ 0 & \text{if a square divides}\quad n.\end{cases} \tag{8}$$

This is the classical Möbius function. Since $D(n)$ is the interval $[1,n]$ of Δ, we have computed μ for Δ. We could have deduced (7) directly by observing $[a,b]\cong[1,b/a]$ by the unique factorization theorem. Equation (3b) becomes

$$N_=(x)=\sum_{y|x}\mu(y,x)N_\le(y)=\sum_{y|x}\mu\left(\frac{x}{y}\right)N_\le(y) \tag{9a}$$

as expected and (1b) gives

$$N_=(x)=\sum_{y:x|y}\mu(x,y)N_\ge(y)=\sum_{k=1}^{\infty}\mu(k)N_\ge(kx), \tag{9b}$$

a somewhat less known type of inversion using the classical Möbius function (Hardy and Wright, 1960).

We now present two applications of the former result.

(a) *The Euler phi-function.* The ϕ-function, $\phi(n)$, is the number of positive integers x not exceeding n which are prime to n; i.e., $\gcd(n,x)=1$.

Let $N_=(n)=\phi(n)$. To compute $N_\le(n)$ we break up the set $[n]=\{1,2,\cdots,n\}$ according to the gcd with n, i.e., let $S_d=\{i\in[n]\,|\gcd(i,n)=d\}$. The S_d are mutually disjoint and their union is $[n]$. Hence $n=\Sigma_{d|n}|S_d|$. But $i\in S_d$ iff $i=kd$, where $k\leqq i$ and $\gcd(k,n/d)=1$. Hence $|S_d|=\phi(n/d)$ and $n=\Sigma_{d|n}\phi(n/d)=\Sigma_{d'|n}\phi(d')=N_\le(n)$. By Möbius inversion

$$\phi(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)d=n-\frac{n}{p_1}-\frac{n}{p_2}\cdots+\frac{n}{p_1p_2}\cdots, \tag{10}$$

since $\mu(n/d)$ is non-zero only if n/d is a product of distinct primes. Thus

$$\phi(n)=n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

where the product ranges over all primes p dividing n.

(b) *Counting Necklaces.* Suppose we have k different colors of beads in unlimited supply, how many n bead necklaces can be formed? We must specify precisely when two necklaces are the same. Every necklace has a front and back, but shifting the beads circularly (bead at $i\rightarrow$ location $i+1$) does not change the necklace.

If we shift n beads circularly, we discover they eventually return to the initial color configuration after, say, d shifts where $d\,|\,n$. The *period* is the smallest number of shifts required for a return. Since

$$\text{RWBRWB}\rightarrow\text{BRWBRW}\rightarrow\text{WBRWBR}\rightarrow\text{RWBRWB},$$

this string has period 3. Suppose we have an n long string of period d. Including itself, it has d shifts all of which give the same necklace when the ends are joined. Furthermore, these are the only strings that give this necklace. Our circular problem is reduced to a linear one:

$$\#\text{ necklaces of length } n=\sum_{d|n}\frac{1}{d}(\#\text{ strings of period } d),$$

where we have omitted the length on the right hand side since the initial d beads determine the string. Clearly

$$\#\text{ of strings of length } n=\sum_{d|n}\#\text{ of strings of period } d.$$

The left side is clearly k^n since there are k colors of beads. Möbius inversion gives

$$\#\text{ of strings of period } d=\sum_{x|d}\mu\left(\frac{d}{x}\right)k^x.$$

Hence

$$\# \text{ of necklaces of length } n = \sum_{d|n} \frac{1}{d} \sum_{x|d} \mu\left(\frac{d}{x}\right) k^x = \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) k^d,$$

where the simplification involves the use of (10).

Example 4: *Convex polytopes.* A very detailed and beautiful study of convex polytopes is given by Grünbaum (1967).

A d-dimensional convex polytope is a bounded d-dimensional set of points in a Euclidean space which can be given as the intersection of half-spaces (i.e., all points on one side of a hyper-plane). For example the triangle in Figure 1 is the intersection of the three indicated half planes — determined by the lines (hyper-planes) a, b, c. We call $\overline{123}$ a 2-face (i.e., 2-dimensional face) of the polytope, $\overline{12}, \overline{23}, \overline{31}$ the 1-faces and $1, 2, 3$ the 0-faces. In higher dimensions the notion of a face can be defined in terms of supporting hyperplanes (Grünbaum, 1967). A polytope can also be thought of as the convex closure of a finite set of points in n-space R^n.

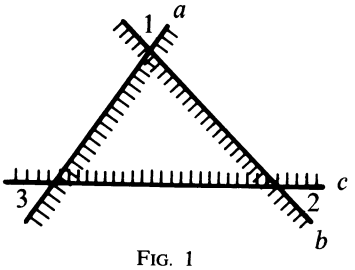

FIG. 1

Let P be a d-dimensional polytope and $\mathcal{F}_P$ the *POS* of faces of P ordered by inclusion, including the empty face $\emptyset$ of dimension -1 and the face P. For any $x \in \mathcal{F}_P$

$$(11) \qquad [\emptyset, x] \cong \mathcal{F}_x.$$

Let $f_k(x)$ be the number of k-dimensional faces containing x. The generalized Euler relation states $\Sigma_j (-1)^{d-j} f_j(x) = \delta(x, P)$, where $\delta(x, P)$ is the Knonecker delta (Grünbaum, 1967). We can rewrite this as

$$(12) \qquad \sum_{y:y \geqq x} (-1)^{d(P)-d(y)} = \delta(x, P),$$

where $d(y)$ is the dimension of y. From (12) and (2) we have $\mu(y, P) = (-1)^{d(P)-d(y)}$ and then by (11)

$$(13) \qquad \mu(x, y) = (-1)^{d(y)-d(x)}.$$

This suggests that a homology theory might be defined for *POS*'s with μ related to the Euler characteristic. This has been started by Rota (1964, 1971).

A k-dimensional simplex has $k+1$ vertices and every subset of $j+1$ vertices determines a j-dimensional face. A simplicial polytope is a polytope P in which every face, except possibly P, is a simplex, e.g., triangles, octahedrons and tetrahedrons, are simplicial polytopes. While Euler's relation (equivalently, equation (13)) is the only relation satisfied by the faces of a general polytope, we might expect other relations for a simplicial polytope. In this case, $x \leqq y < P$ implies that $[x, y]$ is isomorphic to the *POS* of subsets of a $d(y) - d(x)$ element set. By using (4a) to sum $\mu(x, P)$ over all $x \geqq w$ with $d(x) = j < d(P)$ we get

$$(14) \qquad (-1)^{d(P)-1} f_j(w) = \sum_k (-1)^k \binom{k \ \ -d(w)}{j \ \ -d(w)} f_k(w).$$

If we put $w = \emptyset$, then $d(w) = -1$ and we get the Dehn-Sommerville equations (Grünbaum, 1967).

Example 5: *Map coloring.* A map is a planar graph: a (finite) collection of connected, bounded regions in the plane whose boundaries are smooth curves. Two countries sharing a segment of a curve (more than a point) are *adjacent.* If the countries are colored so that no two adjacent countries are the same color, the result is a proper coloring. Let G be a map and let $M_G(\lambda)$ be the number of proper colorings. A *submap* of G is obtained by erasing boundaries between countries. Any map can be colored in $\lambda^{|G|}$ ways where $|G|$ *is the number of countries in G.* Any such coloring is proper for precisely one submap of G. (Just erase those boundaries between countries of the same color.) The relation "is a submap of" makes the submaps of G into an ordered set and

$$\lambda^{|G|} = \sum_{x \leqq G} M_x(\lambda).$$

Since $[0, y]$ is isomorphic to the ordered set of submaps of y, we have

$$\lambda^{|y|} = \sum_{x \in y} M_x(\lambda)$$

Hence if we set $N_=(x) = M_x(\lambda)$, then $N_{\leqq}(y) = \lambda^{|y|}$. By Möbius inverting and setting $y = G$, we obtain

$$M_G(\lambda) = \sum_{x \leqq G} \lambda^{|x|} \mu(x, G).$$

For obvious reasons, $M_G(\lambda)$ is called the *chromatic polynomial* of G. Computation of $M_G(\lambda)$ is difficult when we have no easy way to compute μ. The chromatic polynomials were introduced as a tool for attacking the 4–color problem by Birkhoff and Lewis (1946). Other references include Whitney (1932) who derives a formula by μ-inversion over Boolean algebras, Rota (1964), Wilf (1969), and Read (1968) who has a very nice introduction to the properties of chromatic polynomials. Redoing some of Read's proofs by using properties of the μ-function makes a good exercise.

By introducing the dual graph to a map, where the operation of erasing boundaries is replaced by contracting edges, the general problem of properly coloring the vertices of an arbitrary graph can be treated just as we have done for maps (Rota, 1964).

Using Möbius inversion as a key tool Crapo and Rota (1971) embed the four color problem and the study of chromatic polynomials into a more general problem namely the *critical problem* for combinatorial geometries. This problem, which is one of finding minimal sets of separating hyperplanes for sets of points in finite projective spaces, includes as special cases problems in coding theory and Segre's results characterizing sets of independent points in projective space, (Dowling, 1971).

4. Partitions of a set. An (unordered) *partition* of a finite n element set S_n is a collection $\{\pi_1, \pi_2, \cdots\}$ of non-empty mutually disjoint subsets of S_n whose union is S_n, i.e., $\pi_1 \cap \pi_j = \emptyset$ if $i \neq j$ and $\cup_i \pi_i = S_n$. For instance $\{\{1,3\},\{2\}\}$ is a partition of $\{1,2,3\}$. The sets π_i are called the *blocks* of the partition.

Let $S(n,k)$ denote the number of partitions of S_n into k blocks. The $S(n,k)$ are called *Stirling numbers of the second kind.* The numbers $B_n = \Sigma_{k=1}^n S(n,k)$ are called *Bell numbers.*

Although the study of Stirling and Bell numbers presents some difficulties, (Rota, 1964) the number of partitions having exactly b_i blocks of size i, $i = 1, 2, \cdots$ is easily derived. A partition of this sort is said to be of *type* $\vec{b}$. Thses are easily counted by enumerating permutations of the given set in two ways giving

$$\text{(1)} \qquad \# \text{ of partitions of type } \vec{b} = \frac{(\Sigma i b_i)!}{\Pi b_i!(i!)^{b_i}}.$$

Let P be the set of all partitions of S and let $\pi = \{\pi_1, \pi_2, \cdots\}$ and $\sigma = \{\sigma_1, \sigma_2, \cdots\}$ lie in P. We call π a *refinement* of σ if every block π_i of π is contained in some block σ_j of σ. Another was of thinking of this is to say that π is a refinement of σ if every block σ_i is gotten by merging blocks π_i. We make P into an ordered set $\Pi(S_n) = \Pi_n = (P, \leqq)$ by defining $\pi \leqq \sigma$ to mean π is a *refinement of* σ. *Π_n is called the POS of partitions of S_n ordered by refinement.*

We will compute $\mu(\pi, \sigma)$ for π, $\sigma \in P$ following Frucht and Rota (1965). By Corollary 3.2 it suffices to study $[\pi, \sigma]$. Since σ is gotten by merging blocks of π, the individual elements of the blocks of π are not essential; e.g., in saying that $\{\{1,2\},\{3\},\{4\}\}$ is a refinement of $\{\{1,2\},\{3,4\}\}$ the elements 1 and 2 are really inessential and we could write that $\{\{2\},\{3\},\{4\}\}$ is a refinement of $\{\{2\},\{3,4\}\}$. Hence in studying μ on the interval $[\pi, \sigma]$ we need only consider those π whose blocks contain one element, i.e., those π which are complete refinements of a set. We use 0 *to denote a complete refinement.* Thus we restrict ourselves to intervals of the form $[0, \sigma]$.

Let $\sigma = \{\sigma_1, \sigma_2, \cdots, \sigma_k\}$ (the σ_i are the blocks). Since every refinement of σ consists of some partition of each of the σ_i, we can regard a refinement ρ of σ as an ordered k-tuple $(\rho_1, \cdots, \rho_k)$ where ρ_i is a refinement of σ_i. Thus $[0, \sigma] \cong [0_1, \sigma_1] \times \cdots \times [0, \sigma_k]$. By the product theorem it suffices to consider μ on $[0, w]$ where w consists of one block. The partition consisting of one block is usually written as 1. Let 1 have n elements and write $\mu_n = \mu(0,1)$. We have shown that

$$\mu(\pi, \sigma) = \prod_{i=1}^{m} \mu_{n_i} \quad \text{for all} \quad \pi, \sigma \in P, \tag{2}$$

where $\sigma = \{\sigma_1, \cdots, \sigma_m\}$ and $\pi = \{\pi_1, \cdots, \pi_n\}$ and σ_i is the union of exactly n_i of the π_j's.

We now compute $\mu(0,1)$ by the method of undetermined coefficients. To do this we relate partitions to functions.

Let S_n be an n-set and X an arbitrary set with x elements. We associate with any function f: $S_n \to X$ a partition of S_n as follows: the blocks of the partition are the inverse images of the elements of X. This partition is called the *kernel* or co-image of the function. Different functions may have the same kernels. Kernels and their generalization form the basis for a combinatorial interpretation of finite differences (Mullin-Rota, 1970).

Let $N_=(\pi)$ be the number of functions from S_n to X whose kernel is π and let $N_\geq(\pi)$ be the number of functions whose kernel is $\geq \pi$ (in the ordering of Π_n). We have

$$N_{\geqq}(\pi) = \sum_{\sigma : \sigma \geqq \pi} N_=(\sigma). \tag{3}$$

By Möbius inversion

$$N_=(\pi) = \sum_{\sigma : \sigma \geqq \pi} \mu(\pi, \sigma) N_{\geqq}(\sigma). \tag{4}$$

Setting $\pi = 0$, we get

$$N_=(0) = \sum_{\sigma \in \Pi_n} \mu(0, \sigma) N_\geq(\sigma). \tag{5}$$

$N_=(0)$ is the number of one to one functions since the inverse image of every point must be a point. Hence $N_=(0) = x(x-1)\cdots(x-n+1) = (x)_n$. Suppose σ has $r(\sigma)$ blocks. Then a function is counted by $N_\geq(\sigma)$ if it maps all elements in the same block of σ into one point. Different blocks can map into the same point since the kernel need only be $\geqq \sigma$. Hence $N_\geq(\sigma) = x^{r(\sigma)}$. Substituting in (5) yields

$$x(x-1)\cdots(x-n+1) = \sum_{\sigma} \mu(0, \sigma) x^{r(\sigma)}. \tag{6}$$

Since this relation is true for infinitely many values of x it is a polynomial identity. This is an important combinatorial technique for deriving polynomial identities.

Clearly $r(\sigma) = 1$ if and only if $\sigma = 1$, the partition with one block. Equating coefficients of x on both sides of (6) we get

$$\mu_n = (-1)^{n-1}(n-1)! \tag{7}$$

Substituting this result into (2) we see that

$$\mu(\pi,\sigma) = \prod_i (-1)^{n_i-1}(n_i-1)! = (-1)^{r(\pi)-r(\sigma)} \prod_i (n_i-1)! \tag{8}$$

where the ith block of σ (for some fixed order) is the union of exactly n_i blocks of π.

Equation (6) gives some more information. Let $s(n,k) = \Sigma_{\sigma:r(\sigma)=k}\,\mu(0,\sigma)$. Then by (6)

$$(x)_n = \sum_{k=1}^{n} s(n,k)x^k. \tag{9}$$

The $s(n,k)$ are called *Stirling numbers of the first kind.* We have provided here a combinatorial interpretation of $s(n,k)$, due to Rota (1964), as a sum of values of a Möbius function.

Example 1: *Waring's Formula For Symmetric Functions.* In computing the Möbius function for partitions we derived equation (5) expressing 1–1 functions in terms of all functions. By repeating this argument in terms of a "generating function" associated with each function we are led to symmetric functions.

Let $S_n = \{1,2,\cdots,n\}$ and let $X = \{x_1,\cdots,x_l\}$, where $l \geq n$ and $x_1,\cdots,x_l$ are independent variables. To each function F: $S_n \to X$ with kernel σ associate the monomial generating function

$$g(F) = x_1^{|F^{-1}(x_1)|}x_2^{|F^{-1}(x_2)|}\cdots x_l^{|F^{-1}(x_l)|}.$$

The monomial has $r(\sigma)$ non-trivial factors and degree n. If F is a set of functions, the *generating function* $g(F)$, given by $g(F) = \Sigma_{f \in F}\, g(f)$, is a polynomial in several variables.

We now mimic the argument mentioned. Let $N_=(\sigma)$ be the generating function for the set of all functions from S_n to X with kernel σ. Then $N_\geq(\sigma)$ is the generating function for the set of all functions from S_n to X with kernel $\geq \sigma$. Möbius inverting and setting $\sigma = 0$ we obtain

$$N_=(0) = \sum_\pi \mu(0,\pi)N_\geq(\pi). \tag{10}$$

Now $N_=(0)$, the generating function of the set of all one-one functions is clearly

$$N_=(0) = \sum_{i_1,i_2,\cdots,i_n} x_{i_1}\cdots x_{i_n}$$

where the sum is over all sets of n distinct indices from $\{1,2,\cdots,l\}$. By definition this is $n\,!$ times the elementary symmetric function of degree n in l variables, denoted by a_n. We now show that

$$N_\geq(\pi) = (x_1+x_2+\cdots+x_l)^{b_1}(x_1^2+x_2^2+\cdots+x_l^2)^{b_2}\cdots(x_1^l+x_2^l+\cdots+x_l^l)^{b_l} \tag{11}$$

where π has b_i blocks of size i, and a given factor $(x_i^i+x_2^i+\cdots+x_l^i)$ corresponds to a specific block of size i. Each term in the expansion of the right hand side of (11) corresponds to a choice of images for each of the blocks. Hence we obtain the generating function for the set of all functions which are constant on the blocks of π. But this generating function is precisely $N_\geq(\pi)$ since prescribing the same image for two different blocks is equivalent to merging them in the kernel.

In the theory of symmetric functions, $x_1^i + x_2^i + \cdots = s_i$ is called the power sum symmetric function. If we substitute (11) in (10) and collect terms according to the type of π we will obtain *Waring's formula*:

$$a_n = \frac{1}{n!}\sum_{\pi} \mu(0,\pi) s_1^{b_1(\pi)} s_2^{b_2(\pi)} \cdots$$

$$= \sum_{b} \frac{1}{\Pi_i i!^{b_i} b_i!}(-1)^{n-\Sigma b_i} \prod_i (b_i-1)!\, s_i^{b_i}$$

by (1) and (8) where $\vec{b}$ ranges over all types; i.e., $b_1+2b_2+\cdots=n$. Hence

$$(12) \qquad a_n = \sum_{b}(-1)^n \prod_i \left(\frac{-s_i}{i!}\right)^{b_i} \Big/ b_i, \qquad b_1+2b_2+\cdots=n.$$

See Solomon and McEliece (1966, Section 7) for a generalization.

Doubilet (1972) has developed the basic theory of symmetric function by this approach.

Example 2: *Connected graphs.* We wish to count c_n, the number of connected labeled graphs on n vertices. Let S be the vertex set and $\Pi(S)$ the lattice of partitions of S. The number of loopless labeled graphs on n vertices is $2^{\binom{n}{2}}$ since we may choose any collection of pairs of vertices for edges. Let $N_=(\pi)$ be the number of labeled graphs such that each block of π labels a connected component, i.e., those graphs whose components induce the partition π on the vertices. Then $c_n = N_=(1)$ and we have

$$2^{\binom{n}{2}} = N_{\leq}(1) = \sum_{\pi} N_=(\pi).$$

We can compute $N_{\leq}(\pi)$. This counts all labeled graphs in which different blocks of π label distinct sets of components. Hence

$$(13) \qquad N_{\leq}(\pi) = \prod_i 2^{\binom{i}{2}b_i}$$

where π is of type $\vec{b}$. By Möbius inversion $N_=(1)$, the number of connected graphs, is

$$N_=(1) = \sum_{\pi} \mu(\pi,1) N_{\leq}(\pi)$$

which by (8) and (13)

$$= \sum_{\pi} (-1)^{\Sigma b_i - 1}\left(\sum b_i - 1\right)! \prod_i 2^{\binom{i}{2}b_i}$$

and by (1)

$$= n! \sum_{b:\Sigma ib_i = n} (-1)^{\Sigma b_i - 1}\left(\sum b_i - 1\right)! \prod_i \frac{2^{\binom{i}{2}b_i}}{b_i!(i!)^{b_i}}.$$

This formula is equivalent to the generating function equation $C(x) = \ln G(x)$ or $G(x) = \exp C(x)$. For a discussion of exponential formulas for generating functions of the form $A(x) = \exp B(x)$ see Doubilet, Rota and Stanley (1973) for a Möbius approach and Bender-Goldman (1971) for another approach.

5. Vector Spaces. Let $V_n(q)$ be an n dimensional vector space over the field of q elements. We partially order the subspaces of $V_n(q)$ by inclusion: if U and V are subspaces of $V_n(q)$, then $U \leqq V$ iff U is a subspace of V. The resulting *POS* is denoted by $L(V_n(q))$. It is a "geometric lattice" (Crapo-Rota, 1971), because $L(V_n(q))$ is the lattice of subspaces of a projective space.

The study of subspaces of a finite vector space has deep analogies with the study of subsets of a finite set (Goldman-Rota, 1969, 1970). The relation is probably deeper than just an analogy but as yet there is no explanation for this. Some of these analogies are discussed in this section.

Just as $\binom{n}{k}$ counts the k-subsets of an n-set, we introduce the Gaussian coefficient $\binom{n}{k}_q$ ($\left[\begin{matrix} n \\ k \end{matrix}\right]$ is also used in the literature) defined by $\binom{n}{k}_q$ = # k-dimensional subspaces of $V_n(q)$. To derive $\binom{n}{k}_q$ we reason by analogy with binomial coefficients:

$$\binom{n}{k} = \frac{\text{\# sequences of } k \text{ distinct elements in an } n\text{-set}}{\text{\# sequences of } k \text{ distinct elements in a } k\text{-set}}$$

(1)

$$\binom{n}{k}_q = \frac{\text{\# sequences of } k \text{ independent vectors in } V_n(q)}{\text{\# sequences of } k \text{ independent vectors in } V_k(q)}.$$

Let us compute the numerator of (1). We can choose the first vector in $(q^n - 1)$ ways (the number of non-zero vectors in $V_n(q)$). The vector chosen generates q vectors, viz. all multiples of it; hence we may choose the second vector in $(q^n - q)$ ways. The two vectors now chosen generate, by linear combinations, q^2 vectors; hence we may choose the third vector in $(q^n - q^2)$ ways. Continuing this argument we have

$$\text{\# sequences of } k \text{ independent vectors in } V_n(q)$$
$$= (q^n - 1)(q^n - q)(q^n - q^2)(q^n - q^3)\cdots(q^n - q^{k-1}).$$

When $n = k$ we obtain the denominator in (1). Hence

$$(2) \qquad \binom{n}{k}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

If in (2) we regard the right side as a function in the variable q and hence $\binom{n}{k}_q$ as a function defined by (2), then we have

$$(3) \qquad \lim_{q\to 1} \binom{n}{k}_q = \binom{n}{k}.$$

This is the first manifestation of the relation between subspaces and subsets which is as mysterious as it is fascinating. *In some sense* "a set is a vector space over a field with one element"; a concept which needs a definition. Unfortunately no good one is known.

The relation (3) is a strong heuristic guide to guessing relations over vector spaces in analogy with those over sets. It also provides a check on the correctness of vector space formulas by letting $q \to 1$. For example,

$$(4) \qquad \binom{n}{k}_q = \binom{n}{n-k}_q \quad \text{and} \quad \binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q.$$

When $q \to 1$ we obtain well-known binomial coefficient identities. Both of these identities can be derived immediately from (2) by algebraic manipulation. Combinatorial proofs are a bit more involved (Goldman-Rota (1970)).

To compute the Möbius function $\mu(x, y)$ for $L(V_n(q))$ we show first that the structure of $[x, y]$ depends only on $d(y) - d(x)$ where d denotes dimension. To see this, let $v_1, \cdots, v_{d(y)}$ be a basis for y such that the first $d(x)$ elements are a basis for x. Define

$$f(v_i) = 0 \quad \text{if} \quad i \leqq d(x) \quad \text{and} \quad f(v_i) = v_i \quad \text{otherwise.}$$

Using this map it can be shown that $[x, y] \cong [0, z]$ for some z where $d(z) = d(y) - d(x)$. In fact we can take z to be the quotient space y/x. Since all k-dimensional spaces over fields with q elements are isomorphic, we need only compute $\mu(0, V_n(q))$ for all n. The Möbius function is

$$\mu_n = \mu(0, V_n(q)) = (-1)^n q^{\binom{n}{2}}. \tag{5}$$

In (Rota, 1964) this result is derived from more general theorems on Möbius functions. With the tools presently at our disposal, it could be done by induction. We present here a proof by the method of undetermined coefficients: we count the number of one-one linear transformations from $V_n(q)$ into a vector space X with x vectors in two ways.

For every subspace $U \in L(V_n(q))$ let $N_=(U)$ be the number of linear transformations $f\colon V_n \to X$ whose null space is U, i.e., $f^{-1}(0) = U$. Then $N_{\geq}(U)$ is the number of linear maps from V_n to X whose null space contains U. By Möbius inversion

$$N_=(U) = \sum_{W \geqq U} \mu(U, W) N_{\geq}(W),$$

and with $U = 0$

$$N_=(0) = \sum_{W \in L(V_n)} \mu(0, W) N_{\geq}(W). \tag{6}$$

By definition $N_=(0)$ is the number of linear maps whose null space is 0, i.e., the number of one-one linear maps. Such a map is specified by giving a list of n independent vectors — the image of an ordered basis for $V_n(q)$. By the argument used to derive formula (2), we see that the number of one-one maps from V_n into X is given by $(x-1)(x-q)\cdots(x-q^{n-1})$.

We now compute $N_{\geq}(W)$. A linear map has null space containing W if it maps W onto 0 and does anything at all with the rest of the vectors. Hence, if $b_1, b_2, \cdots, b_n$ is a basis for V_n where $b_1, \cdots, b_{d(W)}$ is a basis for W, we must map $b_1, \cdots, b_{d(W)}$ onto 0 and the other $n - d(W)$ basis vectors onto any vectors in X. Thus $N_{\geq}(W) = x^{n-d(W)}$. Substituting in (6) we obtain

$$(x-1)(x-q)\cdots(x-q^{n-1}) = \sum_{W} \mu_{d(W)} x^{n-d(W)} = \sum_{k=0}^{n} \binom{n}{k}_q \mu_k x^{n-k}. \tag{7}$$

Since this identity is true for infinitely many values of x, it is a polynomial identity. Equating the constant terms on both sides gives

$$\mu_n = (-1)(-q)\cdots(-q^{n-1}) = (-1)^n q^{\binom{n}{2}}$$

which proves (5). As $q \to 1$ we have $\mu_n = (-1)^n$, the Möbius function for Boolean algebras.

Example 1: *q-identities.* Now that we have proved (5), we can rewrite (7) as

$$\prod_{k=0}^{n-1} (x - q^k) = \sum_{k=0}^{n} \binom{n}{k}_q (-1)^k q^{\binom{k}{2}} x^{n-k}. \tag{8}$$

A typical trick is to set $x = z/y$ and multiply by y^n to clear fractions. This introduces another variable:

$$\prod_{k=0}^{n-1} (z - yq^k) = \sum_{k=0}^{n} \binom{n}{k}_q (-y)^k q^{\binom{k}{2}} z^{n-k}. \tag{9}$$

One often obtains such q-binomial identities by counting in two ways. This can be done by considering vector spaces or by considering partitions of a number. To see how the latter enters write

$$\binom{n+k}{k}_q = \sum_{i=0}^{\infty} a_{nk}(i) q^i.$$

Then $a_{nk}(i)$ is the number of partitions of i into at most k parts each of size at most n (MacMahon, 1916). In "sum equals product" identities like (8), q often appears to a quadratic power. Here we have $q^{\binom{k}{2}}$. Cubic and higher powers apparently never do appear. This is not understood, but may be associated with the formula for μ_n.

Since (9) is true for infinitely many values of q, it is a polynomial identity. Setting $z = 1$ and choosing $|q| < 1$ we obtain as $n \to \infty$

$$\prod_{k=0}^{\infty} (1 - yq^k) = \sum_{k=0}^{\infty} (-y)^k q^{\binom{k}{2}} (1-q) \cdots (1-q^k).$$

By considering convergence in the q-adic norm (van der Waerden (1953)), many limits for q-identities can be simplified (Goldman-Rota, 1970).

We now present an example where inversion over subspaces is a natural tool.

Example 2: *Spanning Subsets.* Continuing our discussion of Example 1.4, we say by convention that $\varnothing$ spans nothing and $\{0\}$ spans the 0-dimensional subspace. Since every non-empty subset spans some subspace we see that $N_{\leq}(U)$ is given by

$$N_{\leq}(U) = 2^{q^{d(U)}} - 1.$$

Möbius invert to get $N_{=}(V_n(q))$:

$$\text{(10)} \qquad \#\ \text{spanning subsets of } V_n(q) = \sum_{k=0}^{n} \binom{n}{k}_q \mu_k (2^{q^{n-k}} - 1).$$

When $q \to 1$, we might reasonably expect one spanning subset, but (10) reduces to

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k (2-1) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = (1-1)^n = 0.$$

For (10) to be "right" at $q = 1$, we need to replace $2^{q^{n-k}}$ by 2^{n-k} at $q = 1$. This happens in

$$\text{(11)} \qquad \sum_{k=0}^{n} \binom{n}{k}_q \mu_k (2^{\binom{n-k}{1}_q} - 1).$$

In fact (11) counts spanning sets for projective spaces whereas (10) refers to affine spaces. This illustrates a limitation of the $q \to 1$ idea. In order to use this idea our formula must refer to objects counted in projective and not affine space, i.e., it must be in terms of objects in $L(V_n)$, the subspaces, and not contain any direct reference to the vectors in the space. Vectors are affine points whereas projective points are 1-dimensional subspaces.

P. Hall (1934) and Weisner (1935, 1935a) applied Möbius inversion to p-group enumeration problems. Since the value of μ for $L(V_n(p))$ enters and $p \mid \mu_k$ when $k \neq 0$, congruences modulo p are obtained.

Part of this work was supported by the AFOSR contract 73–2436.

References

1. E. A. Bender and J. R. Goldman, Enumerative uses of generating functions, Indiana University Math. J., 20 (1971) 753–765.

2. G. D. Birkhoff and D. C. Lewis, Chromatic polynomials, Trans. Amer. Math. Soc., 60 (1946) 355–451.

3. H. Crapo and G. C. Rota, On the Foundations of Combinatorial Theory: Combinatorial Geometries, M. I. T. Press, 1971.

4. P. Doubilet, On the foundations of combinatorial theory VII. Symmetric functions through the theory of distribution and occupancy, Studies in Applied Math., (51) 4 (1972) 377–396.

5. P. Doubilet, G. C. Rota, and R. P. Stanley, The idea of generating function, Proc. Sixth Berkeley Symp. Math. Stat. and Prob., vol. 2, University of California Press, 1973, pp. 267–318.

6. T. Dowling, Codes, packing, and the critical problem, Atti Convegno Geometria Combinatoria Sue Applicazioni, Perugia, (1971).

7. W. Feller, An Introduction to Probability Theorey and its Applications, 3rd ed., Wiley, New York, 1968, chap. 4.

8. H. J. Ryser, Combinatorial Mathematics, MAA, Carus Monograph No. 14, 1963.

9. M. Frechet, Les Probabilités associées à un système d'èvènement, compatible et dépendants, Actualités Sci. Indust., (1940 and 1943) 859 and 942. Paris, Hermann.

10. R. Frucht and G. C. Rota, Polinomios de Bell y Particiones de Conjunto Finitos, Scientia, 130 (1966) 67–74.

11. R. Gilman, A combinatorial identity with applications to representation theory, Illinois J. Math., 17 (1973) 347–351.

12. J. R. Goldman and G. C. Rota, The Number of Subspaces of a Vector Space, Recent Progress in Combinatorics, Academic Press, New York, 1969, pp. 75–83, edited by W. T. Tutte.

13. ———, On the foundations of combinatorial theory IV, Finite vector spaces and Eulerian generating functions, Studies in Appl. Math., 49 (1970) 239–258.

14. B. Grünbaum, Convex Polytopes, Interscience, New York, 1967.

15. P. Hall, A contribution to the theory of groups of prime-power order, Proc. London Math. Soc., 36 (1934) 24–80.

16. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 4th ed., Oxford University Press, New York, 1960, Theorem 270.

17. E. Hille, The inversion problem of Möbius, Duke Math. J., 3 (1937) 549–568.

18. P. A. MacMahon, Combinatory Analysis, vols. I, II, Cambridge University Press, New York, 1916. Reprinted as one volume by Chelsea, New York, Sect. 241.

19. R. Mullin and G.-C. Rota, On the Foundations of Combinatorial Theory, III: Theory of Binomial Enumeration, Graph Theory and its Applications, Academic Press, New York 1970, pp. 167–213, B. Harris, ed.

20. R. C. Read, An introduction to chromatic polynomials, J. Combinatorial Theory, 4 (1968) 52–71.

21. G.-C. Rota, On the foundations of combinatorial theory I, Theory of Möbius functions, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete, 2 (1964) 340–368.

22. ———, On the Combinatorics of the Euler Characteristic, Studies in Pure Mathematics, Academic Press, New York, 1971, pp. 221–233. (L. Mirsky, ed.)

23. ———, The number of partitions of a set, this MONTHLY, 71 (1964) 498–504.

24. G. Solomon and R. McEliece, Weights of cyclic codes, J. Combinatorial Theory, 1 (1966) 459–475.

25. B. L. van der Waerden, Modern Algebra, vol. I, Ungar, New York, 1953, pp. 235–236. (Trans. from German by F. Blum)

26. L. Weisner, Abstract theory of inversion of finite series, Trans. Amer. Math. Soc., 38 (1935) 474–484.

27. ———, Some properties of prime-power groups, Trans. Amer. Math. Soc., 38 (1935a) 485–492.

28. H. Whitney, A logical expansion in mathematics, Bull. Amer. Math. Soc., 38 (1932) 572–579.

29. H. S. Wilf, The Möbius Function In Combinatorial Analysis and Chromatic Graph Theory, Proof Techniques in Graph Theory, (F. Harary, ed.), Academic Press, New York, 1969, pp. 179–188.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT SAN DIEGO, LA JOLLA, CA 92037.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MINNESOTA, MINNEAPOLIS, MN 55455.

CORRECTION TO "AN ELEMENTARY PROOF OF THE KRONECKER-WEBER THEOREM"

M. J. GREENBERG

Joe L. Mott informed me that the argument for the case $m > 1$ in Lemma 4, Volume 81, (1974) 606, is incorrect. What is correct is that V_i is the unique subgroup of G of index λ, where i is the smallest index such that $V_i \neq G$; this can be proved using the transitivity of the different and Hilbert's formula — see P. Ribenboim, *Algebraic Numbers*, Wiley-Interscience, New York, 1972, p. 235.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SANTA CRUZ, CA 95064.