PACIFIC JOURNAL OF MATHEMATICS
Vol. 96, No. 2, 1981

THE FIXED-POINT PARTITION LATTICES

PHIL HANLON

Let σ be a permutation of the set $\{1, 2, \cdots, n\}$ and let $\Pi(N)$ denote the lattice of partitions of $\{1, 2, \cdots, n\}$. There is an obvious induced action of σ on $\Pi(N)$; let $\Pi(N)_\sigma = L$ denote the lattice of partitions fixed by σ.

The structure of L is analyzed with particular attention paid to $\mathscr{M}$, the meet sublattice of L consisting of 1 together with all elements of L which are meets of coatoms of L. It is shown that $\mathscr{M}$ is supersolvable, and that there exists a pregeometry on the set of atoms of $\mathscr{M}$ whose lattice of flats G is a meet sublattice of $\mathscr{M}$. It is shown that G is supersolvable and results of Stanley are used to show that the Birkhoff polynomials $B_{\mathscr{M}}(\lambda)$ and $B_G(\lambda)$ are

$$B_G(\lambda) = (\lambda - 1)(\lambda - j) \cdots (\lambda - (m-1)j)$$

and

$$B_{\mathscr{M}}(\lambda) = (\lambda - 1)^{r-1} B_G(\lambda) .$$

Here m is the number of cycles of σ, j is square-free part of the greatest common divisor of the lengths of σ and r is the number of prime divisors of j. $\mathscr{M}$ coincides with G exactly when j is prime.

1. **Preliminaries.** Let $(P, \leqq)$ be a finite partially ordered set. An *automorphism* σ of $(P, \leqq)$ is a permutation of P satisfying $x \leqq y$ iff $x\sigma \leqq y\sigma$ for all $x, y \in P$. The group of all automorphisms of P is denoted $\Gamma(P)$. For $\sigma \in \Gamma(P)$, let $P_\sigma = \{x \in P: x\sigma = x\}$. The set P_σ together with the ordering inherited from P is called the *fixed point partial ordering of* σ. If P is lattice then P_σ is a sublattice of P. To see this, let $x, y \in P_\sigma$. Then $(x \vee y)\sigma \geqq x\sigma = x$ and $(x \vee y)\sigma \geqq y\sigma = y$, so $(x \vee y)\sigma \geqq x \vee y$. If $(x \vee y)\sigma > x \vee y$, then $(x \vee y) < (x \vee y)\sigma < (x \vee y)\sigma^2 < \cdots$ forms an infinite ascending chain in P which is impossible since P is finite. So $(x \vee y)\sigma = x \vee y$ hence the set P_σ is closed under joins in P. Similarly P_σ is closed under meets.

A *partition* ρ of a finite set $\Omega = \{\omega_1, \cdots, \omega_n\}$ is a collection $\rho = B_1/B_2/ \cdots /B_k$ of disjoint, nonempty subsets of Ω whose union is all of Ω. The set of all partitions of Ω is denoted $\Pi(\Omega)$; if $\Omega = \{1, 2, \cdots, n\}$ this is written $\Pi(N)$. $\Pi(\Omega)$ ordered by refinement is a lattice.

Let S_n denote the symmetric group on the numbers $\{1, 2, \cdots, n\}$. Define an action of S_n on $\Pi(N)$ as follows; for $\sigma \in S_n$ and $B_1/ \cdots /B_k \in \Pi(N)$

$$(B_1/ \cdots /B_k)\sigma = B_1\sigma/B_2\sigma/ \cdots /B_k\sigma$$

where $B_i\sigma = \{b\sigma : b \in B_i\}$. It is easily checked that this permutation representation is faithful and that each $\sigma \in S_n$ acts as an automorphism of $\Pi(N)$.

Recall that a lattice L is *upper semimodular* provided that all pairs of elements $x, y \in L$ satisfy the condition (*):

(*) If x and y both cover $x \wedge y$ then $x \vee y$ covers both x and y.

A lattice G is *geometric* if it is upper semimodular and if each element of G is a join of atoms. Its easy to check that every finite partition lattice is geometric.

Let L be a finite lattice and Δ a maximal chain in L from 0 to 1. If, for every chain K of L the sublattice of L generated by K and Δ is distributive, then we call Δ an *M-chain* of L and we call (L, Δ) a *supersolvable lattice* (SS-lattice).

Let L be a finite lattice with rank function r and let $m = r(1)$. The *Birkhoff polynomial of* L, denoted $B_L(\lambda)$ is defined by

$$B_L(\lambda) = \sum_{x \in L} \mu(0, x)\lambda^{m-r(x)} .$$

Here μ is the usual Möbius function of L.

It is assumed in §§ 3 and 5 that the reader is familiar with the structure theory for supersolvable lattices given by Stanley and particularly with his elegant results concerning Birkhoff polynomials of supersolvable geometric lattices (see Stanley [4]). For more about lattice theory see Dilworth and Crawley, [2].

If K is a lattice and S a subset of K we say S is a *meet-sublattice* of K if S together with the inherited ordering is a lattice in which the meet agrees with the meet in K.

2. The structure of $(\Pi(N))_\sigma$. Throughout this section we assume that n is a fixed positive integer and that σ is a permutation of $\{1, 2, \cdots, n\}$. We write

$$\sigma = (c_{1,1}, \cdots, c_{1,l_1}) \cdots (c_{m,1}, \cdots, c_{m,l_m})$$

according to its disjoint cycle decomposition as a permutation of $\{1, 2, \cdots, n\}$. We refer to $(c_{i,1}, \cdots, c_{i,l_i})$ as the ith *cycle of* σ and denote it by C_i. Note that l_i is the length of C_i and so $l_1 + \cdots + l_m = n$.

Let L denote the fixed point partition lattice $(\Pi(N))_\sigma$. Observe that if $\beta = B_1/ \cdots /B_k \in L$ then $B_1/ \cdots /B_k = B_1\sigma/ \cdots /B_k\sigma$ and so σ permutes the blocks of β. We let $Z(\sigma; \beta)$ denote the cycle indicator of this induced action of σ on the set of blocks of β. The following observation is presented without proof.

LEMMA 1. *Suppose* $\beta = B_1/ \cdots /B_k \in L$ *and* $m_{s,u} \in B_{i_0}$. *Then there exists an integer* d *which divides* l_s *and there exist distinct blocks* $B_{i_0}, B_{i_1}, \cdots, B_{i_{d-1}}$ *such that the elements of the cycle* C_s *are evenly divided amongst the* d *blocks* $B_{i_0}, \cdots, B_{i_{d-1}}$ *according to the rule*

$$m_{s,t} \in B_{i_r} \quad \text{iff} \quad u - t \equiv r \mod (l_s/d) .$$

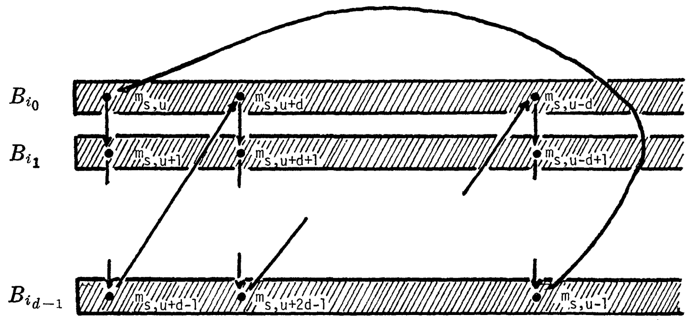


FIGURE 1

In a similar way, β induces a partition of the set of cycles $\{C_1, \cdots, C_m\}$ which is defined in terms of the equivalence relation $\sim$ by $C_i \sim C_j$ iff there exists $c \in C_i$, $d \in C_j$ and a block of β containing both c and d. This relation is transitive since each cycle is divided amongst a cyclically permuted set of blocks. We denote the resulting partition of $\{C_1, \cdots, C_m\}$ by $\rho(\sigma; \beta)$.

EXAMPLE 1. Let $n = 4$ and $\sigma = (1, 2)(3, 4)$. The partition $\beta = 1/2/34$ is in L; the cycle indicator $Z(\sigma; \beta) = x_1x_2$ and the partition $\rho(\sigma; \beta)$ puts each cycle in a block by itself.

If instead we let $\beta = 13/24$ we have $Z(\sigma; \beta) = x_2$ whereas the partition $\rho(\sigma; \beta)$ has just one block containing the two cycles. The lattice L appears in the figure below.

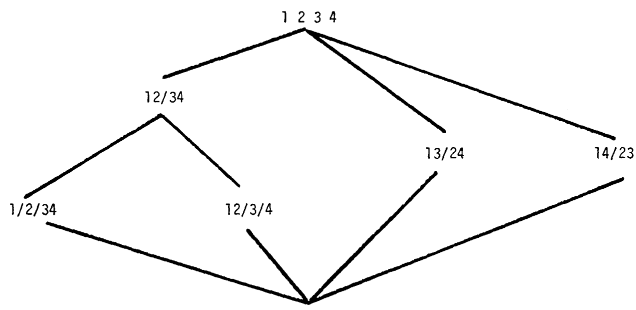


FIGURE 2

Note that L is not Jordan; in general the fixed point lattices $(\Pi(N))_\sigma$ are not themselves highly structured. However the meet sublattice $\mathscr{M}$ of L consisting of 1 together with all meets of coatoms in L is highly structured, in the above case isomorphic to the lattice of partitions of a 3 element set. We begin by investigating the coatoms of L.

LEMMA 2. *There are two kinds of coatoms γ in L:*

(a) *γ has 2 blocks, $\gamma = B_1/B_2$. Each block is setwise invariant under σ hence each block is a union of cycles. $Z(\sigma, \gamma) = x_1^2$ and $\rho(\sigma, \gamma)$ is a coatom in the lattice of partitions of $\{C_1, \cdots, C_m\}$.*

(b) *γ has p blocks, $\gamma = B_1/ \cdots /B_p$, where p is a prime. The blocks B_p are cyclically permuted by σ and every cycle C_i is divided evenly amongst the blocks $B_1, \cdots, B_p$. The integer p divides* $\gcd(l_1, \cdots, l_m)$, *$Z(\sigma, \gamma) = x_p$ and $\rho(\sigma, \gamma)$ is the 1 in the lattice of partitions of $\{C_1, \cdots, C_m\}$.*

Proof. Clearly each of the 2 sorts of partitions above is fixed by σ and each is a coatom in L.

Let γ be a coatom of L where $\gamma = B_1/ \cdots /B_k$ $(k \geqq 2)$. Suppose the blocks of γ can be split into two disjoint σ-invariant sets

$$S = \{B_{i_1}, \cdots, B_{i_u}\}$$
$$T = \{B_{j_1}, \cdots, B_{j_v}\} .$$

Consider the partition $\gamma' = (\bigcup_{B_i \in S} B_i)/(\bigcup_{B_j \in T} B_j)$. Clearly $\gamma' \in L$ and $\gamma \leqq \gamma' < 1$. As γ is a coatom of L, $\gamma' = \gamma$ and so $u = v = 1$. Thus γ is of type (a).

Otherwise, σ acts transitively on the set of blocks $\{B_1, \cdots, B_k\}$. Assume the B_i's are numbered so that $B_i\sigma = B_{i+1}$ for $i < k$ and $B_k\sigma = B_1$. Suppose k factors as $k = rs$ where $r > 1$ and $s \geqq 1$. Consider the partition

$$\gamma' = \left(\bigcup_{i=0}^{s-1} B_{1+ri}\right)\Big/\left(\bigcup_{i=0}^{s-1} B_{2+ri}\right)\Big/ \cdots \Big/\left(\bigcup_{i=0}^{s-1} B_{r+ri}\right) .$$

Clearly $\gamma' \in L$ and $\gamma \leqq \gamma' < 1$, so $\gamma = \gamma'$. Thus $s = 1$ and γ is of type (b). □

There are $2^{m-1} - 1$ coatoms of the kind outlined in (a); these will be called coatoms of *type* a. For each prime p dividing $\gcd(l_1, \cdots, l_m)$ there are p^{m-1} coatoms of the kind outlined in (b); these will be called coatoms of *type* b.

Note that the coatoms of type a generate a sublattice of $\mathscr{M}$ isomorphic to the lattice of partitions of $\{C_1, \cdots, C_m\}$. In the case that $\gcd(l_1, \cdots, l_m) = 1$ there are no coatoms in L of type b and so this sublattice is all of $\mathscr{M}$.

A partition β in L with $Z(\sigma, \beta) = x_j^i$ will be called *periodic* with period j. The preceding lemma states that every coatom of L is periodic with period 1 or with prime period. The next lemma will imply that every partition in $\mathscr{M}$ is periodic.

LEMMA 3. *Let $\beta_1, \beta_2 \in L$ and suppose β_1 is periodic with period j_1 and β_2 is periodic with period j_2. Then $\beta_1 \wedge \beta_2$ is periodic with period $j = lcm(j_1, j_2)$.*

Proof. Choose a block B of $\beta_1 \wedge \beta_2$ and let $c_{s,u} \in B$. Applying Lemma 1 and the fact that β_1 has period j_1 we see that $c_{s,t}$ is in the same block of β_1 as $c_{s,u}$ iff $t \equiv u \mod (l_s/j_1)$. Similarly, $c_{s,t}$ is the same block of β_2 as $c_{s,u}$ iff $t \equiv u \mod (l_s/j_2)$. Hence $c_{s,t}$ is in the same block of $\beta_1 \wedge \beta_2$ iff $t \equiv u \mod (l_s/j_1)$ and $t \equiv u \mod (l_s/j_2)$ iff $t \equiv u \mod (l_s/j)$ where $j = lcm(j_1, j_2)$. Applying Lemma 1 again we have that the block B falls in a j-cycle under the action of σ. As B was chosen arbitrarily we see that every block of β falls in a j-cycle under the action of σ and so $Z(\sigma, \beta) = x_j^i$. $\square$

Write $\gcd(l_1, \cdots, l_m) = p_1^{a_1} \cdots p_r^{a_r}$ and let $j = p_1 \cdots p_r$. Lemma 3 tells us that every partition in $\mathscr{M}$ has period i where i/j. Let $\hat{\sigma}$ be the permutation of $\{1, 2, \cdots, mj\}$ which consists of m cycles of length j,

$$\hat{\sigma} = (1, 2, \cdots, j)(j + 1, \cdots, 2j) \cdots ((m - 1)j + 1, \cdots, mj) .$$

Let $\hat{L}$ be the fixed point partition lattice of $\hat{\sigma}$ and let $\hat{\mathscr{M}}$ be the meet sublattice of $\hat{L}$ consisting of 1 together with all meets of coatoms of $\hat{L}$. Let L and $\mathscr{M}$ be as above.

LEMMA 4. *The lattices $\mathscr{M}$ and $\hat{\mathscr{M}}$ are isomorphic.*

Proof. This follows from the classification of coatoms given in Lemma 2. Returning to σ note that $c_{1,1}, c_{1,j+1}, c_{1,2j+1}, \cdots$ are in the same block of every coatom in L, and hence they are in the same block of every partition in $\mathscr{M}$. The same is true of $c_{i,k}, c_{i,k+j}, c_{i,k+2j}, \cdots$ as i ranges from 1 to m and k ranges from 1 to j. So there is a natural 1-1 correspondence φ between the coatoms of $\hat{\mathscr{M}}$ and the coatoms of $\mathscr{M}$ given as follows; let γ be a coatom of $\hat{\mathscr{M}}$ and let $c_{i,k}, c_{r,s} \in \{1, 2, \cdots, n\}$. Write $k = jk' + u$ and $s = js' + v$ where $1 \leqq u \leqq j$ and $1 \leqq v \leqq j$. Then $c_{i,k}$ and $c_{r,s}$ are in the same block of $\varphi(\gamma)$ iff $(i - 1)j + u$ and $(r - 1)j + v$ are in the same block of γ.

This is easily seen to be a 1-1 onto mapping between coatoms which extends to a lattice isomorphism between $\hat{\mathscr{M}}$ and $\mathscr{M}$. $\square$

In the next section we will study the structure of the lattice $\mathscr{M}$ and in § 4 its associated geometry. By Lemma 4 we may reduce to the case of σ having m cycles of length j, where j is a product of distinct primes.

5. The supersolvability of $\mathscr{M}$. In this section we study the structure of $\mathscr{M}$. Without loss of generality, we assume that $n = mj$ where j is the product of r distinct primes $j = p_1 \cdots p_r$. We assume that σ is the permutation

$$\sigma = (1, 2, \cdots, j)(j + 1, \cdots, 2j) \cdots ((m - 1)j + 1, \cdots, mj)$$

and as before we call $((i - 1)j + 1, \cdots, ij)$ the ith cycle of σ and denote it C_i. Since σ is fixed we abbreviate $Z(\sigma; \beta)$ and $\rho(\sigma; \beta)$ by $Z(\beta)$ and $\rho(\beta)$. Let $L = (\Pi(N))_\sigma$ be the fixed point partial ordering of σ and let $\mathscr{M}$ be the meet sublattice of L consisting of 1 together with all meets of coatoms.

Let h be the partition in L which puts each cycle in a block by itself:

$$h = \{1, 2, \cdots, j\}/\{j + 1, \cdots, 2j\}/ \cdots /\{(m - 1)j + 1, \cdots, mj\} .$$

Note that h is the meet of all type a coatoms in L and so $h \in \mathscr{M}$. We call h the *hinge* of $\mathscr{M}$.

LEMMA 5. *In $\mathscr{M}$ we have*

$$[h, 1] \cong \Pi(M)$$
$$[0, h] \cong D_j \cong B_r$$

where D_j denotes the lattice of divisors of j and B_r denotes the lattice of subsets of $\{1, 2, \cdots, r\}$.

Proof. First consider the interval $[h, 1]$. In $\Pi(N)$, this interval is isomorphic to $\Pi(\{1, 2, \cdots, m\})$ and every element of this interval is a meet of coatoms in the interval. Also each partition above h is fixed by σ and so $[h, 1] \subseteq L$. It follows that $[h, 1] \subseteq \mathscr{M}$ which proves the first assertion.

For the second assertion, recall that each partition in $\mathscr{M}$ is periodic with period d dividing j. For $d \mid j$, there is a unique partition $\tau(d)$ below h of period d consisting of dm blocks. This partition is arrived at by dividing each cycle C_i of σ into d blocks according to:

$(i-1)j+s$ and $(i-1)j+t$ are in the same block
iff $s \equiv t \bmod d$.

If $d = p_{i_1} p_{i_2} \cdots p_{i_u}$ then $\tau(d)$ can be realized as a meet of coatoms in L by taking the meet of all coatoms of type a and one coatom of period p_{i_l} for $1 \leqq l \leqq u$. It follows that $[0, h] \cong D_j$. $\square$

Recall that in a lattice K, a *complement* of an element k is an element k' with $k \vee k' = 1$ and $k \wedge k' = 0$.

LEMMA 6. *In the lattice* $\mathscr{M}$, *h has* j^{m-1} *complements, and each complement c has the following properties*:

(a) $\rho(c) = 1$
(b) $Z(c) = x_j^m$
(c) $[c, 1] \cong D_j$
(d) $[0, c] \cong \Pi(\{1, 2, \cdots, m\})$.

Proof. Let F be the set of functions mapping $\{1, 2, \cdots, m-1\}$ into the set $\{1, 2, \cdots, j\}$, and let $f \in F$. Define a partition $c(f)$ of the set $\{1, 2, \cdots, mj\}$ as follows:

(1) The element $(m-1)j+1$ (i.e., the first element in C_m) will be in a block with exactly one element from every other cycle, these $m-1$ elements being $(s-1)j+f(s)$ $s = 1, 2, \cdots, m-1$.

(2) Rotate this block cyclically under the action of σ; the element $(m-1)j+i$ $1 \leqq i \leqq j$ will be in a block with exactly one element from every other cycle, these $m-1$ elements being $(s-1)j+(i+f(s))$ where $1 \leqq s \leqq m-1$ and where $f(s)+i$ is taken mod j.

It is clear that $c(f)$ uniquely determines f and so there are j^{m-1} such partitions $c(f)$. Note that each has $\rho(c(f)) = 1$ and $Z(c(f)) = x_j^m$.

Consider the join $h \vee c(f)$ in $\Pi(N)$. In h, every pair of elements in a common cycle are in the same block. In $c(f)$, every two cycles have elements in the same block. So $h \vee c(f) = 1$.

Next consider the meet $h \wedge c(f)$ in $\Pi(N)$. In $c(f)$, no two elements in the same cycle are in the same block whereas in h, no two elements in distinct cycles are in the same block. It follows that $h \wedge c(f) = 0$.

So $c(f)$ is a complement to h in $\Pi(N)$ hence $c(f)$ will be a complement to h in L. Hence $c(f)$ will be a complement to h in $\mathscr{M}$ provided $c(f)$ is in $\mathscr{M}$. We examine the coatoms in L which sit above $c(f)$; clearly all are of type b. Let p be a prime dividing j. Recall that if γ is a type b coatom of period p then the element $(m-1)j+1$ is in a block with exactly (j/p) elements from each block C_i, and specifying any of these elements in C_i specifies them all. It follows that there is a unique coatom of period p above $c(f)$ for each prime p dividing j. The meet of these r coatoms has period j (by Lemma 3) and has the property that $(m-1)j+1$ is in a block with at least one other element from each cycle. Clearly this meet is $c(f)$, and so $c(f) \in \mathscr{M}$. Let the r coatoms above $c(f)$ be labelled $\gamma_i, \cdots, \gamma_r$ so that γ_i is the coatom of period p_i. Define a mapping $\varphi\colon B_r \to [c(f), 1]$ by $\varphi(\phi) = 1$, $\varphi(S) = \bigwedge_{i \in S} \gamma_i$ for $S \neq \varnothing$ (here $[c(f), 1]$ denotes the interval in $\mathscr{M}$). Obviously $\varphi(S) \leqq \varphi(T)$ iff $T \subseteqq S$, and it is easy to check that φ is onto. φ is one-to-one by Lemma 3 and the fact that the p_i's are distinct primes. It follows that $[c(f), 1] \cong B_r \cong D_j$. It is equally simple to show that $[0, c(f)] \cong \Pi(\{1, 2, \cdots, m\})$. To obtain the isomorphism ψ, recall that $[h, 1] \cong \Pi(\{1, 2, \cdots, m\})$. Define $\psi\colon [h, 1] \to [0, c(f)]$ by $\psi(x) = c(f) \wedge x$. We've thus shown that $c(f)$ is a complement of h in M having the required properties for each $f \in F$.

It remains to show that every complement of h in $\mathscr{M}$ is of the form $c(f)$ for $f \in F$. Let c be any complement of h in $\mathscr{M}$. As $h \wedge c = 0$, no two elements in a common cycle are in the same block of c. As $h \vee c = 1$, every cycle must have an element in a block of c with some element of C_m. By the invariance of c under σ, we may assume that the block of c containing $(m-1)j+1$ contains exactly one element from every other cycle. It is now clear how to define $f \in F$ with $c(f) = c$. □

EXAMPLE 2. Let $m = 3$ and $j = 2$. So our permutation $\sigma = (1, 2)(3, 4)(5, 6)$. The lattice $\mathscr{M}$ appears below; note that $\mathscr{M}$ is geo-

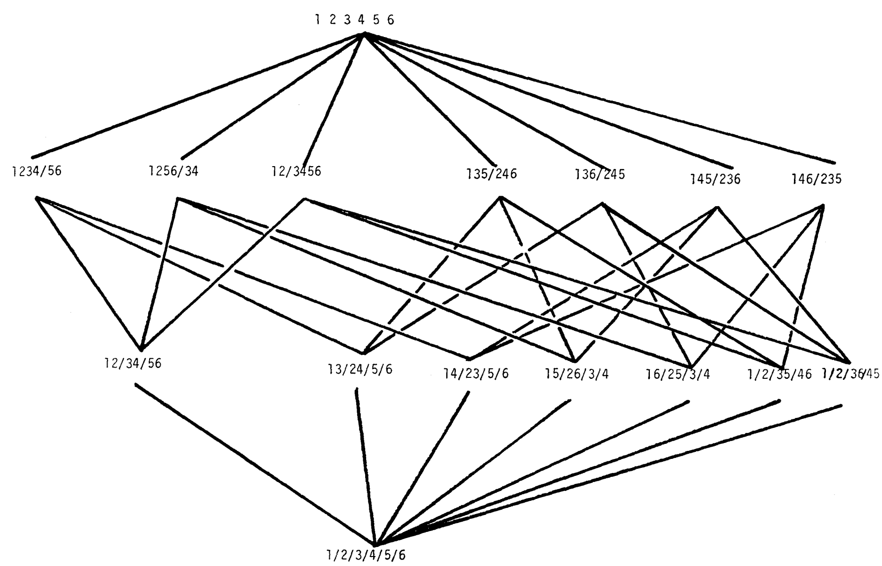


FIGURE 3

metric. We will see later that $\mathscr{M}$ is geometric iff j is a prime. Here the hinge h is the partition 12/34/56. The coatoms of type a are the three to the left, those of type b are the four to the right. j^{m-1} is four; the four complements of h are the four coatoms of type b.

In this section we prove that $\mathscr{M}$ is supersolvable. This will require careful analysis of certain elements of $\mathscr{M}$. Recall that if $x \in \mathscr{M}$ then x is periodic of some period d which divides j. We let $\Pi(x)$ denote this number d. In the following sequence of lemmas, we explore the functions Π and ρ and show that a certain miximal chain from 0 to 1 in $\mathscr{M}$ consists of modular elements.

For $x, y \in \mathscr{M}$ we let $x \vee y$ denote the join of x and y in $\mathscr{M}$ and we let $x \bigvee_L y$ denote the join of x and y in L. As $\mathscr{M}$ is a meet sublattice of L we have $x \bigvee_L y \leqq x \vee y$; in general equality does not hold. For example, let $j = 2$ and $m = 3$ so $\sigma = (1, 2)(3, 4)(5, 6)$. Let $x = 13/24/5/6$ and let $y = 14/23/5/6$. Then $x \bigvee_L y = 1234/5/6$ but $x \vee y$ must have period 1 since both C_1 and C_2 are in the same block of $x \bigvee_L y$. Hence $x \vee y = 1234/56$ (see Figure 3).

The function ρ, introduced in § 2, is defined for all $x \in L$. It is easy to check that ρ respects the join in L, that is $\rho(x) \vee \rho(y) = \rho(x \bigvee_L y)$. In fact ρ also respects the join in $\mathscr{M}$.

LEMMA 7. *Let $x, y \in \mathscr{M}$. Then $\rho(x \vee y) = \rho(x) \vee \rho(y)$.*

Proof. Note that if $\omega, z \in \mathscr{M}$ and $\omega \leqq z$ then $\rho(\omega) \leqq \rho(z)$. So $\rho(x) \vee \rho(y) = \rho(x \bigvee_L y) \leqq \rho(x \vee y)$.

Let z be the unique partition in $\mathscr{M}$ with $\rho(z) = \rho(x) \vee \rho(y)$ and $\Pi(z) = 1$. Then $z \geqq x$ and $z \geqq y$ so $x \vee y \leqq z$. Hence $\rho(x \vee y) \leqq \rho(z) = \rho(x) \vee \rho(y)$.

It should be pointed out that the analogous statement for meets is false; i.e., in general we do not have $\rho(x \wedge y) = \rho(x) \wedge \rho(y)$. As a counter example let $j = 2$ and $m = 2$ so $\sigma = (1, 2)(3, 4)$. Let $x = 13/24$ and let $y = 14/23$. Then $x \wedge y = 1/2/3/4$ so $\rho(x \wedge y) = 1/2$. But $\rho(x) = \rho(y) = 12$ so $\rho(x \wedge y) = 1/2 \neq 12 = \rho(x) \wedge \rho(y)$. However one case where equality holds will be of particular interest to us.

LEMMA 7. *Let $x \in \mathscr{M}$ and suppose $\Pi(x) = 1$. For any $y \in \mathscr{M}$, $\rho(x \wedge y) = \rho(x) \wedge \rho(y)$.*

Proof. As $\Pi(x) = 1$, each cycle C_i is contained in a block of x. Let C_p and C_q be cycles with p and q in the same block of $\rho(x) \wedge \rho(y)$. Then p and q lie in the same block of $\rho(y)$ so there exist $u \in C_p$ and $v \in C_q$ such that u and v lie in the same block of y. Also p and q lie in the same block of $\rho(x)$ so some block of x contains both cycles

C_p and C_q. Hence a and v lie in the same block of $x \wedge y$ so p and q lie in the same block of $\rho(x \wedge y)$. This shows that $\rho(x) \wedge \rho(y) \leqq \rho(x \wedge y)$; the reverse inequality is easy to show.

We next consider the function Π. Again we will be interested in how it behaves with respect to the join operation in $\mathscr{M}$.

LEMMA 9. *Let* $x, y \in \mathscr{M}$.
(A) *If* $x \leqq y$ *then* $\Pi(y) | \Pi(x)$.
(B) $\Pi(x \vee y)$ *divides* $\gcd(\Pi(x), \Pi(y))$.
(C) *If* $\Pi(x \vee y) = \gcd(\Pi(x), \Pi(y))$ *then* $x \vee y = x \bigvee_L y$.

Proof. Note that $\Pi(x) = d$ iff the elements of each cycle C_i are evenly divided amongst d blocks according to the rule that u and v are in the same block iff $u \equiv v \pmod{d}$, for $u, v \in C_i$. From this observation (A) follows immediately, and (B) follows easily from (A).

For (c) suppose first that $u, v \in C_i$ and $u \equiv v \pmod{\gcd(d, e)}$: say $u = v + k \gcd(d, e)$. Write $k \gcd(d, e) = \alpha d + \beta e$ for $\alpha, \beta \in \boldsymbol{Z}$ and let ω be the unique element of C_i satisfying $u + \alpha d \equiv \omega \pmod{j}$. Then u and ω are equivalent $\bmod\, d$ hence are in the same block of x. Also

$$\omega + \beta e = (u + \alpha d) + \beta e = u + k \gcd(d, e) = v$$

so w and v are equivalent $\bmod\, e$ hence are in the same block of y. Thus u and v are in the same block of $x \bigvee_L y$, which shows that if $u \equiv v \pmod{\gcd(\Pi(x), \Pi(y))}$ and $u, v \in C_i$ then u and v are in the same block of $x \bigvee_L y$.

Suppose u and w are in the same block of $x \vee y$ with $u \in C_p$ and $w \in C_q$. Since

$$\rho(x \vee y) = \rho(x) \vee \rho(y) \quad \text{and} \quad \rho(x) \vee \rho(y) = \rho(x \bigvee_L y)$$

there exists a sequence $u = u_0, u_1, \cdots, u_n$ such that u_i, u_{i+1} are in the same block of either x or y and such that $u_n \in C_q$. It follows that u and u_n are in the same block of $x \bigvee_L y$ hence of $x \vee y$ so w and u_n are in the same cycle and in the same block of $x \vee y$. So $u_n - w \equiv 0 \pmod{\Pi(x \vee y)}$. Since $\Pi(x \vee y) = \Pi(x \bigvee_L y)$ we see that $u_n \equiv w$ (mod $\Pi(x \bigvee_L y)$). By the above observation, u_n and w (hence u and w) are in the same block of $x \bigvee_L y$ so $x \vee y \leqq x \bigvee_L y$ and equality must hold.

Note that the sufficient condition for the equality of $x \vee y$ and $x \bigvee_L y$ given in (C) is not a necessary condition. For a counterexample let $j = 2$ and $m = 4$ so $\sigma = (1, 2)(3, 4)(5, 6)(7, 8)$. Let $x = 14/23/58/67$ and let $y = 13/24/57/68$. Then

$$x \vee y = x \bigvee_L y = 1234/5678 \quad \text{so} \quad \Pi(x \vee y) = 1\ .$$

But $\Pi(x) = \Pi(y) = 2$ so $2 = \gcd(\Pi(x), \Pi(y))$.

We can now construct the bottom half of our maximal chain of modular elements. Suppose $\rho(x) = 0$ and $\Pi(x) = d$. Then each block of x contains j/d elements; the blocks partition each cycle C_i into d parts. The unique element x of $\mathscr{M}$ satisfying these conditions is denoted $\tau(d)$. Note that $\tau(j) = 0$ and $\tau(1) = h$.

LEMMA 10. *Let d/j and let $y, z \in \mathscr{M}$.*
(A) *If $z \leqq y$ then $z \vee (\tau(d) \wedge y) = (z \vee \tau(d)) \wedge y$.*
(B) *If $z \leqq \tau(d)$ then $z \vee (\tau(d) \wedge y) = (z \vee y) \wedge \tau(d)$.*

Proof. We first prove (A). Note that for any $x \in \mathscr{M}$, $\tau(d) \wedge x = \tau(e)$ where $e = lcm(d, \Pi(x))$ and $\tau(d) \vee x$ is the unique element of $\mathscr{M}$ above x which has period $\gcd(d, \Pi(x))$ and cycle partition $\rho(x)$. From this it follows that $z \vee (\tau(d) \wedge y)$ is the unique element of $\mathscr{M}$ above z which satisfies

$$\begin{aligned}\rho(z \vee (\tau(d) \wedge y)) &= \rho(z)\\ \Pi(z \vee (\tau(d) \wedge y)) &= \gcd \Pi(z), lcm(d, \Pi(y)) .\end{aligned}$$

By a similar argument one shows that $(z \vee \tau(d)) \wedge y$ is the unique element of $\mathscr{M}$ above z which satisfies

$$\begin{aligned}\rho((z \vee \tau(d)) \wedge y) &= \rho(z)\\ \Pi((z \vee \tau(d)) \wedge y) &= lcm(\Pi(y), \gcd(\Pi(z), d)) .\end{aligned}$$

Here one needs to use the fact that $z \leqq y$.

As $z \leqq y$ we have $\Pi(y) | \Pi(z)$. Also, the lattice of divisors of j is modular which together with $\Pi(y) | \Pi(z)$ gives

$$lcm(\Pi(y), \gcd(\Pi(z), d)) = \gcd(\Pi(z), lcm(d, \Pi(y))) .$$

The proof of (B) is somewhat easier. Assume $z = \Pi(e)$ where $d | e$. Then

$$\begin{aligned} z \vee (\tau(d) \wedge y) &= \tau(e) \vee (\tau(d) \wedge y)\\ &= \tau(lcm(e, \gcd(d, \Pi(y)))) .\\ (z \vee y) \wedge \tau(d) &= (\tau(e) \vee y) \wedge \tau(d)\\ &= \tau(\gcd(d, lcm(e, \Pi(y)))) .\end{aligned}$$

As before, the condition $d | e$ together with the modularity of the lattice of divisors of j proves the desired equality.

Recall that j was assumed to be the product of r distinct primes $j = p_1 p_2 \cdots p_r$. For $i = 1, 2, \cdots, r$ let $t_i = \tau(p_1 p_2 \cdots p_i)$, and let $t_0 = 0$. Then $0 = t_0 < t_1 < \cdots < t_r = h$ is a maximal chain from 0 to h consisting of modular elements of $\mathscr{M}$ (by Lemma 10).

For $i = 1, 2, \cdots, m$ let s_i denote the element of $\mathscr{M}$ which has the following $i+1$ blocks; block 1 contains only cycle C_1, block 2 contains only cycle $C_2, \cdots$, block i contains only cycle C_i and block $i+1$ contains the remaining cycles $C_{i+1}, \cdots, C_m$. Let $s_0 = 1$ so

$$h = s_{m-1} < s_{m-2} < \cdots < s_0 = 1$$

is a maximal chain from h to 1. Note that $\Pi(s_i) = 1$ and $\rho(s_i) = \{1\}/\{2\}/\cdots/\{i\}/\{i+1, i+2, \cdots, m\}$. We will use the fact that $\rho(s_i)$ is a modular element of $\Pi(M)$.

LEMMA 11. *Let $y, z \in \mathscr{M}$. For $i = 0, 1, \cdots, m-1$ we have the following*:

(A) *If $z \leqq y$ then $z \vee (s_i \wedge y) = (z \wedge s_i) \wedge y$.*

(B) *If $z \leqq s_i$ then $z \vee (s_i \wedge y) = (z \vee y) \wedge s_i$.*

Proof. We first prove (A); assume $z \leqq y$.

$$\begin{aligned} \rho(z \vee (s_i \wedge y)) &= \rho(z) \vee \rho(s_i \wedge y) && \text{by Lemma 7} \\ &= \rho(z) \vee (\rho(s_i) \wedge \rho(y)) && \text{by Lemma 8} \\ &= (\rho(z) \vee \rho(s_i)) \wedge \rho(y) \end{aligned}$$

the last equality holding since $\rho(s_i)$ is a modular element of $\Pi(M)$. Using Lemma 7 again we have

$$\rho(z \vee (s_i \wedge y)) = \rho(z \vee s_i) \wedge \rho(y) = \rho((z \vee s_i) \wedge y) .$$

The last equality follows from Lemma 8 upon observing that $z \vee s_i \geqq s_i$ so $\Pi(z \vee s_i) | \Pi(s_i) = 1$.

Also $\Pi(s_i) = \Pi(s_i \vee z) = 1$ so $\Pi((s_i \vee z) \wedge y) = \Pi(y)$ and $\Pi(s_i \wedge y) = \Pi(y)$. The latter equality implies that $\Pi(z \vee (s_i \wedge y)) | \Pi(y)$. But $y \geqq z$ and $y \geqq s_i \wedge y$ so $y \geqq z \vee (s_i \wedge y)$ hence $\Pi(y) | \Pi(z \vee (s_i \wedge y))$. Thus

$$\Pi(z \vee (s_i \wedge y)) = \gcd(\Pi(z), \Pi(s_i \wedge y))$$

and so $z \vee (s_i \wedge y) = z \mathbf{V}_L (s_i \wedge y)$ by Lemma 9(C). We now show that $z \vee (s_i \wedge y) \leqq (s_i \vee z) \wedge y$ which will imply equality since we know

$$\rho(z \vee (s_i \wedge y)) = \rho((s_i \vee z) \wedge y)$$

and

$$\Pi(z \vee (s_i \wedge y)) = \Pi((s_i \vee z) \wedge y) .$$

Suppose u and v are in the same block of $z \vee (s_i \wedge y)$. Since $z \vee (s_i \wedge y) = z \mathbf{V}_L (s_i \wedge y)$ there exists a sequence $u = u_0, u_1, \cdots, u_n = v$ such that u_l, u_{l+1} are in the same block of either z or $(s_i \wedge y)$. Since $z \leqq y$ we see that u_l, u_{l+1} are in the same block of y so u and v are in the same block of y. Also u_l, u_{l+1} are in the same block of either z or s_i so u and v are in the same block of $z \mathbf{V}_L s_i$ hence of

$z \vee s_i$. Thus u and v are in the same block of $(z \vee s_i) \wedge y$ so $(z \vee y) \leqq (s_i \vee z) \wedge y$. This completes the proof of (A).

The proof of (B) is the same with a minor exception. As in (A) we show that

$$\rho(z \vee (s_i \wedge y)) = \rho((z \vee y) \wedge s_i)$$

and

$$\Pi(z \vee (s_i \wedge y)) = \Pi(y \vee z) = \Pi((z \vee y) \wedge s_i) .$$

Let $d = \Pi(z \vee y)$, and suppose that u and v are in the same block of $z \vee (s_i \wedge y)$. Then there exists a sequence $u = u_0, u_1, \cdots, u_n$ such that

(1) u_l, u_{l+1} are in the same block of either z or $(s_i \wedge y)$

(2) $u_n \equiv v \pmod{d}$.

Note that u_l, u_{l+1} are in the same block of $(z \vee y) \wedge s_i$ and $\Pi((z \vee y) \wedge s_i) = d$ so u and v are in the same block of $(z \vee y) \wedge s_i$. This completes the proof of (B).

Lemma 11 tells us that each s_i is a modular element of $\mathscr{M}$. Combining Lemma 10, Lemma 11 and Proposition 2.1 from Stanley [4, pg. 203] gives the following theorem.

THEOREM 1. *$\mathscr{M}$ is a supersolvable lattice with M-chain*

$$0 = t_0 < t_1 < \cdots < t_r = h = s_{m-1} < s_{m-2} < \cdots < s_0 = 1 .$$

At this point a rough sketch of $\mathscr{M}$ is helpful.

4. The geometric properties of $\mathscr{M}$. Figure 4 suggests that $\mathscr{M}$ might be geometric; in fact $\mathscr{M}$ is geometric iff j is prime. However $\mathscr{M}$ does give rise to a pregeometry (in the language of Crapo and Rota [1]) which we will show in this section. To do so

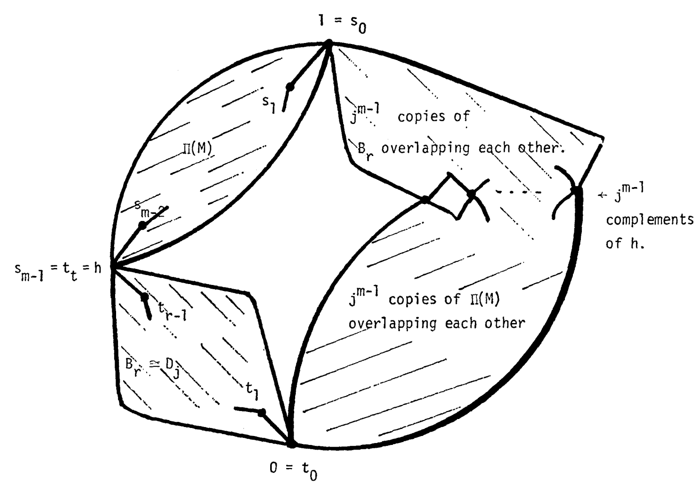


FIGURE 4

we need notation for certain elements of $\mathscr{M}$. Some of this notation has already been established; for completeness it is listed below again.

(1) For $d|j$, $\tau(d)$ denotes the unique element of $\mathscr{M}$ with $\rho(\tau(d)) = 0$ and $\Pi(\tau(d)) = d$. $\tau(d)$ sits in the interval $[0, h]$.

(2) For a partition $\beta \in \Pi(\mathscr{M})$, $\sigma(\beta)$ denotes the unique element of $\mathscr{M}$ with $\rho(\sigma(\beta)) = \beta$ and $\Pi(\sigma(\beta)) = 1$. $\sigma(\beta)$ sits in the interval $[h, 1]$.

(3) Let F be the set of functions mapping $\{1, 2, \cdots, m-1\}$ into the set $\{1, 2, \cdots, j\}$. For $f \in F$, $c(f)$ denotes the complement of h given by f as in the proof of Lemma 6. *Note*: for notational convenience in what follows we will extend f to a function from $\{1, 2, \cdots, m\}$ into $\{1, 2, \cdots, j\}$ by defining $f(m) = 1$.

(4) Let p and q be integers between 1 and m with $p < q$ and let r be an integer between 0 and $j - 1$. Then $\alpha(p, q, r)$ denotes the following partition in $\mathscr{M}$ which has exactly j blocks of size 2 and all other blocks of size 1. Each block of size 2 consists of one element from C_p and one from C_q according to $u \in C_p$ and $v \in C_q$ are in the same block iff $u \equiv v - r \pmod{j}$.

EXAMPLE 3. Let $j = m = 3$ so $\sigma = (1, 2, 3)(4, 5, 6)(7, 8, 9)$. Let $p = 1$, $q = 3$ and $r = 2$. Then

$$\alpha(1, 3, 2) = 19/27/38/4/5/6 \,.$$

It is worth noting that $\Pi(\alpha(p, q, r)) = j$ and that $\rho(\alpha(p, q, r))$ is the atom in $\Pi(\mathscr{M})$ having the block $\{p, q\}$ of size 2 and all other blocks of size 1.

LEMMA 12. *$\mathscr{M}$ has exactly $r + j\binom{m}{2}$ atoms. Of these, r atoms lie in the interval $[0, h]$; these are of the form $\tau(j/p)$ for p a prime dividing j. (These r atoms will be called type* a *atoms.) The remaining $j\binom{m}{2}$ atoms lie outside the interval $[0, h]$. These are of the form $\alpha(p, q, r)$ and will be called type* b *atoms.*

Proof. Let x be an atom. It is clear that $\rho(x)$ is either 0 or an atom in $\Pi(\mathscr{M})$ and that $\Pi(x)$ is either j or (j/p) for p a prime dividing j. We consider the four possibilities.

If $\rho(x) = 0$ and $\Pi(x) = j$ then $x = 0$ which is impossible. If $\rho(x) = 0$ and $\Pi(x)$ is j/p then $x = \tau(j/p)$. If $\rho(x)$ is an atom and $\Pi(x)$ is j/p then we have $0 < \tau(j/p) < x$ which is impossible.

Lastly suppose $\Pi(x) = j$ and $\rho(x)$ is the atom in $\Pi(\mathscr{M})$ which has exactly one block of size 2 containing p and q with $p < q$. Consider $(p-1)j + 1 \in C_p$. It is in a block of size 2 with a unique element of C_q, say $(q-1)j+(r+1)$ for $0 \leqq r \leqq j-1$. It is now clear that $x = \alpha(p, q, r)$.

For the remainder of this paper, A denotes the set of type a atoms and B denotes the set of type b atoms. Let $\beta \in \Pi(M)$ and let $f \in F$. Then $B(\beta)$ denotes the set of type b atoms x satisfying $x \leqq \sigma(\beta)$ and $B(f)$ denotes the set of type b atoms satisfying $x \leqq c(f)$. $B(\beta; f)$ denotes the intersection of $B(\beta)$ and $B(f)$. Note that $\alpha(p, q, r)$ is in $B(\beta)$ iff p and q are in the same block of β and $\alpha(p, q, r)$ is in $B(f)$ iff $r \equiv f(q) - f(p) \pmod{j}$.

Let $\mathscr{B}$ denonte the lattice of subsets of $A \cup B$.

DEFINITION 2. Define closure operator $^-$ on $\mathscr{B}$ as follows; let $S \in \mathscr{B}$ and write $S = S_A \cup S_B$ with $S_A \subseteqq A$ and $S_B \subseteqq B$. Let $\beta = \bigvee_{x \in S_B} \rho(x) \in \Pi(M)$. Then

Case 1. $\bar{\phi} = \varnothing$

Case 2. If $S_A = \varnothing \neq S_B$ and if there exists $f \in F$ such that $x \leqq c(f)$ for all $x \in S_B$ let $\bar{S} = B(\beta; f)$.

Case 3. Let $\bar{S} = A \cup B(\beta)$ otherwise.

We need to show that $^-$ is well-defined in Case 2. Suppose $S_A = \varnothing \neq S_B$ and let $f, g \in F$ satisfy $x \leqq c(f)$ and $x \leqq c(g)$ for all $x \in S_B$. We need to show that $B(\beta; f) = B(\beta; g)$. By the symmetry of f and g it suffices to prove that $B(\beta; f) \subseteqq B(\beta; g)$.

Assume that $\alpha(p, q, r) \in B(\beta, f)$ so $r \equiv f(q) - f(p) \bmod j$. Choose a sequence $\alpha(p_0, p_1, r_1), \alpha(p_1, p_2, r_2), \cdots, \alpha(p_{n-1}, p_n, r_n) \in S_B$ such that $p = p_0$ and $q = p_n$. This can be done by definition of β. As $x \leqq c(f)$ for all $x \in S_B$ we know

$$f(p_l) - f(p_{l-1}) \equiv r_l \pmod{j} .$$

In particular

$$r \equiv f(q) - f(p) \equiv f(p_n) - f(p_0) \equiv \sum_{l=1}^{n} (f(p_l) - f(p_{l-1})) \pmod{j} .$$

Hence $r \equiv \sum_{l=1}^{n} r_l \pmod{j}$. Since $x \leqq c(g)$ for all $x \in S_B$ we also have $r_l \equiv g(p_l) - g(p_{l-1}) \pmod{j}$. The same telescoping sum shows that

$$r \equiv g(p_n) - g(p_0) \equiv g(q) - g(p) \pmod{j}$$

and so $\alpha(p, q, r) \in B(\beta; g)$ as desired.

It is easy to show that $^-$ is a closure operator—the verification is left to the reader. The next lemma shows that $^-$ also satisfies the exchange condition thus making $(\beta, ^-)$ into a pregeometry. We first need the following technical lemma.

LEMMA 13. *Let $S_B \subseteqq B$ and let $y \in B$. Let $\beta = \bigvee_{z \in S_B} \rho(z)$ and suppose that $\bar{S}_B$ is of the form $B(\beta; f)$ whereas $\overline{S_B \cup \{y\}}$ is of the form $A \cup B(\gamma)$ for some $\gamma \geqq \beta$. Then $\rho(y) \leqq \beta$ and so $\gamma = \beta$.*

Proof. Suppose $\rho(y) \nleqq \beta$. We will construct a function $g \in F$ with $y \leqq c(g)$ and $z \leqq c(g)$ for all $z \in S_B$. Let $y = \alpha(p, q, r)$. As $\rho(y) \nleqq \beta$ we know that p and q lie in distinct blocks of β. Write

$$\beta = B_1/B_2/\cdots/B_k \quad \text{with} \quad p \in B_1 \quad \text{and} \quad q \in B_2 \ .$$

Case 1. $m \notin B_1$. Define $g(l) = f(l)$ for $l \notin B_1$.
For $l \in B_1$ define

$$g(l) \equiv (f(q) - f(p)) - r + f(l) \pmod{j} \ .$$

Note that $g(p) \equiv f(q) - r = g(q) - r \pmod{j}$. Thus $g(q) - g(p) \equiv r \pmod{j}$ and so $y \leqq c(g)$. Suppose $z \in S_B$, $z = \alpha(p_1, q_1, r_1)$. If $p_1, q_1 \in B_i$ for $i \neq 1$ then $g(q_1) - g(p_1) \equiv f(q_1) - f(p_1) \equiv r_1 \pmod{j}$ and so $z < c(g)$. If $p_1, q_1 \in B_1$ then

$$\begin{aligned} g(q_1) - g(p_1) &\equiv (f(q) - f(p) - r + f(q_1)) - (f(q) - f(p) - r + f(p_1)) \\ &\equiv f(q_1) - f(p_1) \equiv r_1 \pmod{j} \ . \end{aligned}$$

So $z \leqq c(g)$ as was to be shown.

Case 2. $m \in B_1$. Define $g(l) = f(l)$ for $l \notin B_2$. For $l \in B_2$ define

$$g(l) \equiv f(l) + (f(p) - f(q)) + r \pmod{j} \ .$$

As before, $g(q) \equiv f(p) + r = g(p) + r \pmod{j}$ so $y \leqq c(g)$. For $z \in S_B$, $z \leqq c(g)$ as in Case 1.

THEOREM 2. *$(\mathscr{B}, \bar{\ })$ is a pregeometry.*

Proof. We need to show that $\bar{\ }$ satisfies the following exchange property (*):

$$(*) \qquad \begin{array}{l} \text{Let } x, y \in A \cup B \text{ and let } S \subseteqq A \cup B. \text{ If } x \notin \bar{S} \text{ and} \\ x \in \overline{S \cup \{y\}} \text{ then } y \in \overline{S \cup \{x\}} \ . \end{array}$$

The verification of (*) proceeds in several cases. Let $\beta = \bigvee_{z \in S_B} \rho(z)$.

Case 1. $x \in A$.
Since $x \notin \bar{S}$ we know $S = S_B \subseteqq B$. If $y \in A$ then obviously $y \in \overline{S \cup \{x\}} = A \cup B(\beta)$, so assume that $y \in B$.

Since $x \notin \bar{S}_B$, we have $\bar{S}_B = B(\beta; f)$ for some $f \in F$. As $x \in \overline{S_B \cup \{y\}}$ we know $\overline{S_B \cup \{y\}} = B(\gamma) \cup A$ for some $\gamma \geqq \beta$. Applying Lemma 13 we have $\rho(y) < \beta$ so $y \in B(\beta)$. So $y \in \overline{S_B \cup \{x\}} = B(\beta) \cup A$.

Case 2. $x \in B$, $y \in A$.
If $y \in \bar{S}$ then

$$\bar{S} \subseteqq \overline{S \cup \{y\}} \subseteqq \overline{\bar{S} \cup \{y\}} = \bar{\bar{S}} = \bar{S}$$

which is impossible since $x \in \overline{S \cup \{y\}} - \bar{S}$.

So $y \notin \bar{S}$; i.e., $\bar{S} = B(\beta; f)$ for some $f \in F$. Thus $S \cup \{y\} = A \cup B(\beta)$ and so $\rho(x) \leqq \beta$.

Since $x \notin \bar{S}$ there is no function $f \in F$ with $x \leqq c(f)$ and with $z \leqq c(f)$ for all $z \in S$. So $\overline{S \cup \{x\}} = B(\beta) \cup A$ which gives $y \in \overline{S \cup \{x\}}$.

Case 3. $x, y \in B$ and $\rho(y) \leqq \beta$.
Since $\bar{S}$ is properly contained in $\overline{S \cup \{y\}}$ we see that $\bar{S}$ has the form $B(\beta; f)$ for some $f \in F$ and that $\overline{S \cup \{y\}} = B(\beta) \cup A$. As $x \in \overline{S \cup \{y\}}$, $\rho(x) \leqq \beta$.

Since $x \notin \bar{S}$ there is no function $f \in F$ with $x \leqq c(f)$ and $z \leqq c(f)$ for all $z \in S$. Thus $S \cup \{x\} = B(\beta) \cup A$ and so $y \in \{x\}$.

Case 4. $x, y \in B$, $\rho(y) \nleqq \beta$ and $\bar{S} = A \cup B(\beta)$.
Here we have $\overline{S \cup \{y\}} = A \cup B(\gamma)$ for $\gamma = \beta \vee \rho(y) > \beta$. Since $x \notin \bar{S}$ we know $\rho(x) \nleqq \beta$ but $\rho(x) \leqq \beta \vee \rho(y)$. Hence we know $\rho(y) \leqq \beta \vee \rho(x)$ because $\Pi(M)$ is a geometric lattice.

Case 5. $x, y \in B$, $\rho(y) \nleqq \beta$ and $S = B(\beta; f)$ for $f \in F$.
In this case we have $\overline{S \cup \{y\}} = B(\gamma; g)$ for $\gamma = \beta \vee \rho(y)$ and for some $g \in F$ (see the proof of Lemma 13). Suppose $\rho(x) \leqq \beta$. Since $x \in \overline{S \cup \{y\}}$, we know $x \leqq c(g)$ and so

$$x \in B(\beta; g) = B(\beta; f) = \bar{S} \quad \rightarrow\leftarrow .$$

Thus $\rho(x) \nleqq \beta$ and $\rho(x) \leqq \beta \vee \rho(y)$ so $\rho(y) \leqq \beta \vee \rho(x)$ again because $\Pi(\mathscr{M})$ is geometric. Hence $y \in B(\gamma; g) = \overline{S \cup \{x\}}$ and this finishes the proof of Theorem 2.

Let G be the subset of $\mathscr{M}$ consisting of all elements of period 1 together with all elements of period j. It is clear that if $x, y \in G$ then $x \wedge y \in G$ so G is closed under meets.

Given any element x of $\mathscr{M}$, there is a unique smallest element of period 1 which is greater than or equal to x, this being $\sigma(\rho(x))$. In particular this is true of $x = y \vee z$ for $y, z \in G$. Thus G has a join operation $\bigvee_G$ defined as follows; for $y, z \in G$

$$y \bigvee_G z = \begin{cases} y \vee z & \text{if} \quad \Pi(y \vee z) = j \\ \sigma(\rho(y \vee z)) & \text{if} \quad \Pi(y \vee z) < j . \end{cases}$$

G is a meet sublattice of $\mathscr{M}$ hence of L and so of $\Pi(\{1, 2, \cdots, mj\})$. For the remainder of the paper we continue to let $\vee$, $\wedge$ denote the join and meet of $\mathscr{M}$ and $\bigvee_G$, $\bigwedge_G$ denote the join and meet of G.

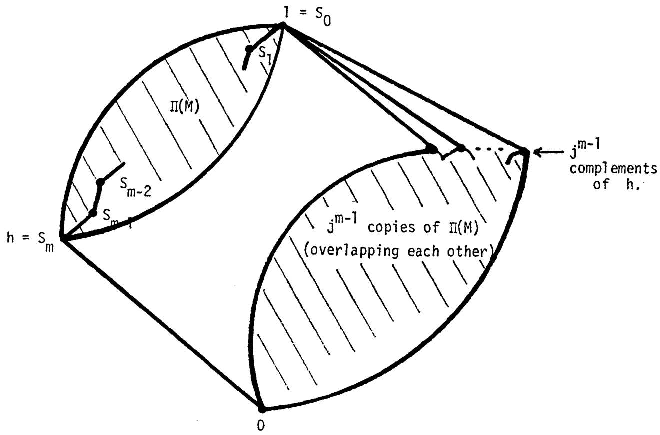


FIGURE 5

Let $\tilde{G}$ denote the lattice of flats of the pregeometry $(\mathscr{B}, \bar{\ })$. We know that $\tilde{G}$ is a geometric lattice. Define $\varphi: \tilde{G} \to G$ as follow;

(1) $\varphi(\phi) = 0$

(2) $\varphi(B(\beta; f)) = V_G B(\beta; f)$

(3) $\varphi(A \cup B(\beta)) = h \bigvee_G (V_G B(\beta)) = \sigma(\beta)$.

THEOREM 3. *φ is a lattice isomorphism and so G is a geometric lattice. Some elemetary properties of the matroid given by G are listed below*:

A. *Bases*: *If I is a basis containing h then $I - \{h\} \leqq B(f)$ for a unique function f. The set of $\rho(x)$ for $x \in I - \{h\}$ constitute a basis for $\Pi(M)$.*

If I is a basis not containing h then I contains an element y (not necessary unique) such that the set of $\rho(x)$ for $x \in I - \{y\}$ constitute a basis for $\Pi(M)$ and such that $V_G(I - \{y\}) = c(f)$ for some function f.

B. *Circuits*: *If C is a circuit containing h then the set of $\rho(x)$ such that $x \in C - \{h\}$ constitute a circuit in $\Pi(M)$. There is no function f such that $x \leqq c(f)$ for all $x \in C - \{h\}$.*

If C is a circuit not containing h then the set of $\rho(x)$ such that $x \in C$ constitute a circuit in $\Pi(M)$. There is a function f such that $x \leqq c(f)$ for all $x \in C$.

C. *Rank function*: *Let λ_G denote the rank function of G and let λ denote the rank function of $\Pi(M)$. Let S be a subset of $B \cup \{h\}$; write $S = S_A \cup S_B$ where $S_B \subseteqq B$ and $S_A = \varnothing$ or $\{h\}$. Let*

$$\beta = \bigvee_{x \in S_B} \rho(x) .$$

Then

$$\lambda_G(S) = \begin{cases} 0 & \textit{if} \quad S = \varnothing \\ \lambda(\beta) & \textit{if} \quad S_A = \varnothing \quad \textit{and} \\ & \qquad S_B \subseteqq B(f) \quad \textit{for some} \quad f \in F(S_B \neq \varnothing) \\ 1 + \lambda(\beta) & \textit{otherwise} . \end{cases}$$

Proof. It is easy to verify that φ is one-to-one, and onto. φ is obviously order-preserving hence φ is a lattice isomorphism. The matroid properties given in A, B and C are clear; proofs are left to the reader.

COROLLARY 1. *$\mathscr{M}$ is geometric* iff *j is prime, or $m = 1$.*

Proof. If j is prime then $\mathscr{M} = G$ and so the result follows from the last theorem. If $m = 1$ then $\mathscr{M}$ is isomorphic to the Boolean algebra B_r (i.e., lattice of divisors of j), and so $\mathscr{M}$ is geometric.

Conversely, suppose j is not prime and $m > 1$. We show that $\mathscr{M}$ is not geometric.

Consider the join of the two atoms $\alpha(1, 2, 1)$ and $\alpha(1, 2, 2)$. It is clear that these two do not both sit below $c(f)$ for some f hence

$$\alpha(1, 2, 1) V_{\mathscr{M}} \alpha(1, 2, 2) = \sigma(\beta) > h$$

where $\beta = \{1, 2\}/\{3\}/ \cdots /\{m\}$. But since j is not prime and $[0, h] \cong B_r$ we see that the rank of h is at least 2 so the rank of $\sigma(\beta)$ is at least 3. So $\mathscr{M}$ is not geometric.

Return to Figure 3, where $j = 2$ and $m = 3$. Corollary 1 tells us that $\mathscr{M}$ is geometric in this case. In fact, its easy to check that this particular $\mathscr{M}$ is the projective plane of order 2.

5. The Birkhoff polynomial of $\mathscr{M}$. The purpose of this section is to determine the Birkhoff polynomial of $\mathscr{M}$. Some results in this section will be proved in a more general framework and then specialized to $\mathscr{M}$. We begin with some well-known facts about closure operators on lattices.

Let K be a finite lattice with join and meet operations $\bigvee_K$ and $\bigwedge_K$. Let $x \rightarrow \bar{x}$ be a closure operator and let $\bar{K}$ denote the set of closed elements of K. Then $\bar{K}$ is a lattice with join $\bigvee_{\bar{K}}$ and meet $\bigwedge_{\bar{K}}$ given by

$$x \bigvee_{\bar{K}} y = \overline{x \bigvee_K y}$$
$$x \bigwedge_{\bar{K}} y = x \bigwedge_K y .$$

Let $h \in K$. Define $G(h)$ to be the set of elements of K whose meet with h is either 0 or h. Define a map $x \to \bar{x}$ from K to K by

$$\bar{x} = \begin{cases} x & \text{if } \ x \in G(h) \\ x \vee h & \text{if } \ x \notin G(h) . \end{cases}$$

It is clear that $\bar{x} \geqq x$. Also $^-$ maps K onto $G(h)$ so $\bar{\bar{x}} = \bar{x}$, and it is easy to check that if $x \geqq y$ then $\bar{x} \geqq \bar{y}$. Thus $^-$ is a closure on K and the lattice of closed elements is $G(h)$. We sometimes write $G(h) = G_0 \cup G_h$ where

$$G_0 = \{x \in K \colon x \wedge h = 0\}$$
$$G_h = \{x \in K \colon x \wedge h = h\} .$$

LEMMA 14. *Suppose that K is supersolvable with M-chain C, suppose $h \in C$ and let $C' = C \cap G(h)$. Then $G(h)$ is supersolvable with M-chain C'.*

Proof. Let $\mathscr{D}$ be a chain in $G(h)$, and let T be the sublattice of $G(h)$ generated by $\mathscr{D}$ and C. Note that T is contained in the sublattice of K generated by C and $\mathscr{D}$ since $h \in C$. Also observe that T is closed under joins in K, if $x, y \in T$ with $x \wedge h = y \wedge h = 0$ then

$$(x \bigvee_K y) \wedge h = (x \wedge h) \bigvee_K (y \wedge h) = 0 \bigvee 0 = 0 .$$

The first equality follows by the fact that C is an M-chain for K.

Let a, b and $c \in T$. Then

$$\begin{aligned}(a \bigvee_G b) \wedge c = (a \bigvee_K b) \wedge c &= (a \wedge c) \bigvee_K (b \wedge c) \\ &= (a \wedge c) \bigvee_G (b \wedge c)\end{aligned}$$

and

$$\begin{aligned}((a \wedge b) \bigvee_G c) = (a \wedge b) \bigvee_K c &= (a \bigvee_K c) \wedge (b \bigvee_K c) \\ &= (a \bigvee_G c) \wedge (b \bigvee_G c) .\end{aligned}$$

This proves the lemma.

Apply the last result to $\mathscr{M}$ with h as in §§ 3 and 4. Note that $G = G(h)$ and so we see that G is a supersolvable geometric lattice with M-chain

$$0 < h = s_{m-1} < s_{m-2} < \cdots < s_1 < s_0 = 1 .$$

We now use methods of Stanley to evaluate the Birkhoff polynomial of $\mathscr{M}$.

THEOREM 4. *Let $B_{\mathscr{M}}(\lambda)$ denote the Birkhoff polynomial of $\mathscr{M}$. Then*

$$B_{\mathscr{M}}(\lambda) = (\lambda - 1)^r (\lambda - j)(\lambda - 2j) \cdots (\lambda - (m-1)j) .$$

In particular $\mu_m(0, 1) = \mu(j)((-1)^{m-1}(m-1)!)j^{m-1}$ *where* $\mu(j)$ *denotes the number theoretic Möbius function.*

Proof. Let $B_h(\lambda)$ denote the Birkhoff polynomial of the interval $[0, h]$. We first observe that

$$B_{\mathscr{M}}(\lambda) = B_h(\lambda)(\sum_{b \in G_0} \mu(0, b)\lambda^{m-r(b)})$$

where $r(b)$ denotes the rank of b. The proof is exactly the same as the proof of Theorem 2 given in Stanley [3]. In this proof Stanley assumes that the lattice L under consideration is geometric whereas $\mathscr{M}$ is not in general geometric. However he only uses that L is geometic to prove his Lemmas 1 and 2. Lemma 1 still holds since we've shown h is modular in $\mathscr{M}$ (see Lemma 10). We now prove his Lemma 2; i.e., we show that for any $y \in \mathscr{M}$, $h \wedge y$ is a modular element of $[0, y]$.

Suppose $a \in [0, y]$ and $b \leqq a$. Then

$$\begin{aligned}(b \vee (y \wedge h)) \wedge a &= ((b \vee h) \wedge y) \wedge a \quad \text{by modularity of} \quad h \\ &= ((b \vee h) \wedge a) = b \vee (h \wedge a) \\ &= b \vee (h \wedge (y \wedge a)) = b \vee ((h \wedge y) \wedge a) .\end{aligned}$$

This part of the proof comes directly from Stanley [3, pg. 216]. Next suppose $b \leqq h \wedge y$ and $a \in [0, y]$. Then

$$\begin{aligned}b \vee ((h \wedge y) \wedge a) &= b \vee (h \wedge a) \\ &= h \wedge (b \vee a) \\ &= h \wedge (y \wedge (b \vee a)) \quad \text{since} \quad b \vee a \leqq y \\ &= (h \wedge y) \wedge (b \vee a) .\end{aligned}$$

My thanks to Prof. R. P. Dilworth for suggesting this half of the proof.

This shows that

$$B_{\mathscr{M}}(\lambda) = B_h(\lambda)(\sum_{b \in G_0} \mu(0, b)\lambda^{m-r(b)}) .$$

Next consider the supersolvable geometric lattice G. As h is a modular element of G we can apply the same result again to G. This time the interval $[0, h]$ is isomorphic to a chain of length 1 so we have

$$B_G(\lambda) = (\lambda - 1)(\sum_{b \in G_0} \mu(0, b)\lambda^{m-r(b)}) .$$

Combining this with the previous equation yields

$$B_M(\lambda) = (\lambda - 1)^{-1} B_h(\lambda) B_G(\lambda) .$$

Also the interval $[0, h]$ in M is isomorphic to the Boolean algebra B_r so $B_h(\lambda) = (\lambda - 1)^r$. Thus we have

$$B_M(\lambda) = (\lambda - 1)^{r-1} B_G(\lambda) . \tag{5.1}$$

Recall that an M-chain for G is $0 < s_m < s_{m-1} < \cdots < s_0 = 1$. For $i = 0$ to $m - 1$, let a_i denote the number of atoms of G which are less than or equal to s_i but not less than or equal to s_{i+1}. By Theorem 4.1 of Stanley [4, pg. 209] we know

$$\begin{aligned} B_G(\lambda) &= (\lambda - a_{m-1})(\lambda - a_{m-2}) \cdots (\lambda - a_0) \\ &= (\lambda - 1)(\lambda - a_{m-2}) \cdots (\lambda - a_0) . \end{aligned}$$

We next show that $a_{m-i} = (i - 1)j$ for $i = 2, \cdots, m$. The atoms of G are h together with all type b atoms $\mathscr{M}$. A type b atom a is less than or equal to s_{m-i} iff $\rho(a) < \rho(s_{m-i})$. Now $\rho(s_{m-i})$ has one block of size i together with $m - i$ blocks of size 1; the block of size i consists of $\{m, m - 1, \cdots, m - i + 1\}$.

Let $\alpha(p, q, r)$ be a type b atom with $\alpha(p, q, r) \leqq s_{m-i}$ and $\alpha(p, q, r) \nleqq s_{m-i-1}$. Since $\alpha(p, q, r) \leqq s_{m-i}$ we know $p, q \in \{m, m-1, \cdots, m - i + 1\}$. Since $\alpha(p, q, r) \nleqq s_{m-i-1}$ we know that p and q are not both members of $\{m, m - 1, \cdots, m - i + 2\}$. As $p < q$ we see

$$\begin{aligned} &p = m - i + 1 \\ &q \in \{m, m - 1, \cdots, m - i + 2\} . \end{aligned}$$

Furthermore any choice of $q \in \{m, m - 1, \cdots, m - i + 2\}$ and $r \in \{1, 2, \cdots, j\}$ give a type b atom $\alpha(m - i + 1, q, r) = a$ with $a \leqq s_{m-i}$ and $a \nleqq s_{m-i-1}$. So $a_{m-i} = j(i - 1)$. Thus

$$B_G(\lambda) = (\lambda - 1)(\lambda - j)(\lambda - 2j) \cdots (\lambda - (m - 1)j)$$

which together with equation (5.1) completes the proof of Theorem 4.

Return now to Figure 3. Here $j = 2$ and $m = 3$ so we have

$$B_M(\lambda) = (\lambda - 1)(\lambda - 2)(\lambda - 4) = \lambda^3 - 7\lambda^2 + 15\lambda - 8 .$$

The interested reader can verify from Figure 3 that this is the correct Birkhoff polynomial for $\mathscr{M}$.

In Theorem 4 we obtained, for a nongeometric supersolvable lattice, factorization results similar to those which Stanley obtained for supersolvable geometric lattices. We can restate Theorem 4 in the following more general form.

THEOREM 4A. *Let (K, C) be a supersolvale lattice and let h be an element of C. Suppose that $G(h)$ is a geometric lattice and that for each $y \in G_0$ the map from $[0, h]$ to $[y, y \vee h]$ given by $z \to z \vee y$ is one-to-one. Let $C' = C \cap G(h)$ be*

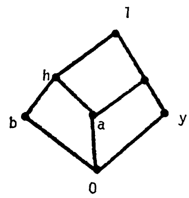
$$0 < h = s_0 < s_1 < \cdots < s_n = 1 .$$

Then

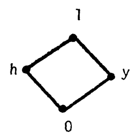
$$B_{\mathscr{M}}(\lambda) = B_h(\lambda)(\lambda - a_1)(\lambda - a_2) \cdots (\lambda - a_n)$$

where a_i is the number of atoms a of $\mathscr{M}$ which satisfy $a \leqq s_i$, $a \nleqq s_{i-1}$.

The assumption that the map $z \to z \vee y$ is one-to-one is necessary. Consider for example

$M =$ 

It is easy to check that $0 < a < h < 1$ is an M-chain for this lattice; note that the map from $[0, h]$ to $[y, y \vee h]$ given by $z \to z \vee h$ is not one-to-one (h and b have the same image).

$G(h) =$ 

so $G(h)$ is geometric. It is easy to check that $a_1 = 1$ and $B_h(\lambda) = (\lambda - 1)^2$ so

$$B_h(\lambda)(\lambda - a_1) = (\lambda - 1)^3 .$$

However one can check that $B_M(\lambda) = \lambda(\lambda - 1)(\lambda - 2)$ and so Theorem 4A does not hold.

References

1. H. H. Crapo and G. C. Rota, *On the Foundations of Combinatorial Theory: Combinatorial Geometries*, M.I.T. Press, 1970.
2. P. Crawley and R. P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, 1973.
3. R. P. Stanley, *Modular elements of geometric lattices*, Algebra Universalis, VI (1971), 214–217.
4. ———, *Supersolvable lattices*, Algebra Universalis, II (1972), 197–217.

Received July 16, 1980.

California Institute of Technology
Pasadena, CA 91125