

SUPERSOLVABLE LATTICES¹⁾

R. P. STANLEY

1. Introduction

We shall investigate a certain class of finite lattices which we call *supersolvable lattices* (for a reason to be made clear shortly). These lattices L have a number of interesting combinatorial properties connected with the counting of chains in L , which can be formulated in terms of Möbius functions. I am grateful to the referee for his helpful suggestions, which have led to more general results with simpler proofs.

1.1. DEFINITION. Let L be a finite lattice and Δ a maximal chain of L . If, for every chain K of L , the sublattice generated by K and Δ is distributive, then we call Δ an M -chain of L ; and we call (L, Δ) a *supersolvable lattice* (or *SS-lattice*).

Sometimes, by abuse of notation, we refer to L itself as an *SS-lattice*, the M -chain Δ being tacitly assumed.

A wide variety of examples of *SS-lattices* is given in the next section. In this section, we define two fundamental concepts associated with *SS-lattices*, viz., the *rank-selected Möbius invariant* and the *set of Jordan-Holder permutations*. We shall outline their connection with each other, together with some consequences. Proofs will be given in later sections.

If L is an *SS-lattice* whose M -chain Δ has length n (or cardinality $n+1$), then every maximal chain K of L has length n since all maximal chains of the distributive lattice generated by Δ and K have the same length. Hence if $\hat{0}$ denotes the bottom element and $\hat{1}$ the top element of L , then L has defined on it a unique *rank function* $r: L \rightarrow \{0, 1, 2, \dots, n\}$ satisfying $r(\hat{0})=0$, $r(\hat{1})=n$, $r(y)=r(x)+1$ if y covers x (i.e., $y > x$ and no $z \in L$ satisfies $y > z > x$). Let S be any subset of the set $\mathbf{n}-\mathbf{1}$, where we use the notation

$$\mathbf{k} = \{1, 2, \dots, k\}.$$

We will also write $S = \{m_1, m_2, \dots, m_s\}^<$ to signify that $m_1 < m_2 < \dots < m_s$. Define $\alpha(S)$ to be the number of chains

$$\hat{0} = y_0 < y_1 < \dots < y_s < \hat{1}$$

in L such that $r(y_i) = m_i$, $i = 1, 2, \dots, s$. In particular, if $S = \{m\}$, then $\alpha(S)$ is the number

¹⁾ The research was supported by the Air Force Office of Scientific Research, AF 44620-70-C-0079, at M.I.T.

of elements of L of rank m ; while if $S = \mathbf{n} - \mathbf{1}$, then $\alpha(S)$ is the number of maximal chains in L . Also, $\alpha(\phi) = 1$. Now define

$$\beta(S) = \sum_{T \subseteq S} (-1)^{|S-T|} \alpha(T),$$

so by the Principle of Inclusion-Exclusion,

$$\alpha(S) = \sum_{T \subseteq S} \beta(T).$$

Our main object is to investigate the numbers $\beta(S)$ when L is an SS -lattice. It will be seen that these numbers have many remarkable properties. First, we consider an alternative interpretation of $\beta(S)$.

If $S \subseteq \mathbf{n} - \mathbf{1}$, define $L(S)$ to be the sub-ordered set of L consisting of $\hat{0}$, $\hat{1}$, and all elements of L whose ranks belong to S . Thus, $L(\phi)$ is a two-element chain, and $L(\mathbf{n} - \mathbf{1}) = L$. It follows from a basic result on Möbius functions due to Philip Hall [11] (see also [15, p. 346]) that

$$\mu_S(\hat{0}, \hat{1}) = (-1)^{s+1} \beta(S), \quad (1)$$

where μ_S is the Möbius function of $L(S)$ and $s = |S|$. For this reason, we call $\beta(S)$ the *rank-selected Möbius invariant* of L .

Somewhat more generally, if $[x, y]$ is a segment in L of length m (i.e., $r(y) - r(x) = m$) and if $S \subseteq \mathbf{m} - \mathbf{1}$, then we denote by $\beta_{xy}(S)$ the rank-selected Möbius invariant of the segment $[x, y]$, considered as a lattice in its own right.

In order to define the second fundamental concept associated with SS -lattices, we first review some properties of finite distributive lattices. If P is a partially ordered set, then an *order ideal* of P is a subset I of P such that if $x \in I$ and $y \leq x$, then $y \in I$. Recall the structure theorem of Birkhoff [1, p. 59] that every finite distributive lattice L is isomorphic to the set of order ideals of some finite partially ordered set P , ordered by inclusion. This correspondence is denoted $L = J(P)$. If I is an element of L of rank m , then as an order ideal of P , I has cardinality m . Every maximal chain $\phi = I_0 < I_1 < \dots < I_n = P$ in L corresponds to an *order-compatible permutation* $\sigma = (x_1, x_2, \dots, x_n)$ of the elements x_i of P , i.e., if $x < y$ in P , then x appears before y in σ . This correspondence is determined by the condition

$$x_i \in I_{i+1} - I_i.$$

Now let $\Delta: \phi = I_0 < I_1 < \dots < I_n = P$ be any fixed maximal chain in L , and let J cover I in L (so $|J - I| = 1$). Then there is a unique integer $i \in \mathbf{n}$ such that the prime interval $[I, J]$ is projective to the prime interval $[I_{i-1}, I_i]$. We denote this integer i as $\gamma(I, J)$.

It is easily seen that i is determined by the condition

$$J - I = I_i - I_{i-1}.$$

This fact is essentially the well-known Jordan-Hölder correspondence for finite distributive lattices.

Suppose now that $I < J$ in L . Define the subset $\Gamma(I, J)$ of \mathfrak{n} by the condition

$$\Gamma(I, J) = \{i \mid x_i \in J - I\}.$$

Hence, $|\Gamma(I, J)| = |J - I|$. If $I = \phi$ (the bottom element of L), then $\Gamma(I, J)$ is denoted simply $\Gamma(J)$, so $\Gamma(I, J) = \Gamma(J) - \Gamma(I)$. Note that if J covers I , then $\gamma(I, J)$ is the unique element of $\Gamma(I, J)$.

Suppose that

$$K: I = I'_0 < I'_1 < \dots < I'_m = J$$

is an unrefinable chain between I and J . Define the *Jordan-Hölder permutation* (or *J-H permutation*) $\pi_K: \Gamma(I, J) \rightarrow \Gamma(I, J)$ associated with K (relative to Δ) by

$$\pi_K = (\gamma(I'_0, I'_1), \gamma(I'_1, I'_2), \dots, \gamma(I'_{m-1}, I'_m)).$$

Now let (L, Δ) be an SS-lattice, with $x < y$ in L . The set $\Gamma(x, y)$ is still defined, viz., $\Gamma(x, y)$ is computed in the distributive lattice generated by Δ and the chain $x < y$. Similarly, we still have the notion of $\gamma(x, y)$ (when y covers x) and of the *J-H permutation* $\pi_K: \Gamma(x, y) \rightarrow \Gamma(x, y)$, where K is an unrefinable chain between x and y . The set of all *J-H permutations* π_K , including repetitions, as K ranges over all unrefinable chains between x and y , is called the *J-H set* of $(L, \Delta; x, y)$ and is denoted $\mathcal{J}_{xy}(L, \Delta)$ (or \mathcal{J}_{xy} for short). If $x = \hat{0}$ and $y = \hat{1}$, then the corresponding *J-H set* is called the *J-H set* of (L, Δ) and is denoted simply $\mathcal{J}(L, \Delta)$ or just \mathcal{J} .

Figure 1, for example, shows an SS-lattice (L, Δ) (actually the lattice of subgroups

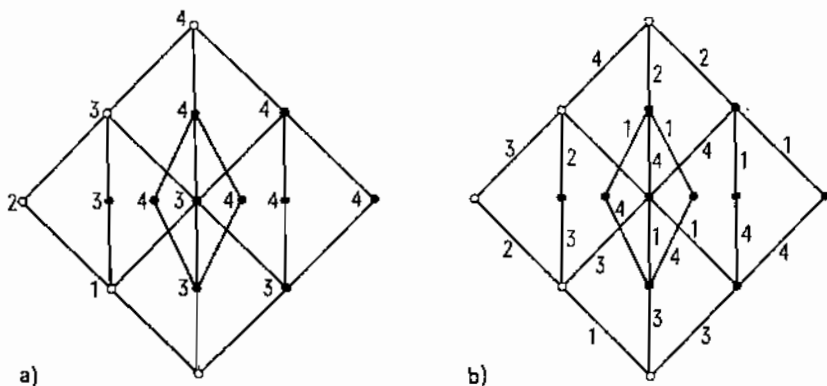


Figure 1.

of an abelian 2-group of type $(2,2)$, with the M -chain Δ indicated by open dots. In Figure 1(a), each element $x \in L$ is marked by the largest element of $\Gamma(x)$; in Figure 1(b), the numbers $\gamma(x, y)$ are indicated. From Figure 1(b), we read off the J - H set $\mathcal{J}(L, \Delta)$:

1	2	3	4
1	3	2	4
1	3	2	4
1	3	4	2
1	3	4	2
3	4	1	2
3	1	2	4
3	1	4	2
3	1	4	2
3	4	1	2
3	1	2	4
3	1	4	2
3	1	4	2
3	4	1	2
3	4	1	2

If $\pi = (i_1, i_2, \dots, i_m)$ is a permutation of some finite subset of the integers, then a pair $i_j > i_{j+1}$ is called a *descent* of π , and the set

$$D(\pi) = \{j : i_j > i_{j+1}\}$$

is called the *descent set* of π . The fundamental result connecting the J - H set $\mathcal{J}_{xy}(L, \Delta)$ with the rank-selected Möbius function $\beta_{xy}(S)$ of the segment $[x, y]$ is the following:

1.2 THEOREM. *Let (L, Δ) be an SS-lattice, and let $[x, y]$ be a segment of L of length m . If $S \subseteq \mathbf{m} - 1$, then the number of permutations π in the J - H set $\mathcal{J}_{xy}(L, \Delta)$ with descent set $D(\pi) = S$ is equal to $\beta_{xy}(S)$.*

The proof of Theorem 1.2 is given in Section 3. It was proved in [16, Thm 9.1] when L is a distributive lattice (under a different terminology). The present paper is a result of extending the lattice-theoretical portions of [16] as far as possible.

By way of illustration, we list the descent sets of the 15 elements of the J - H set $\mathcal{J}(L, \Delta)$ of the SS-lattice (L, Δ) in Figure 1.

π	$D(\pi)$
1 2 3 4	ϕ
1 3 2 4	2

1	3	2	4	2
1	3	4	2	3
1	3	4	2	3
3	4	1	2	2
3	1	2	4	1
3	1	4	2	1,3
3	1	4	2	1,3
3	4	1	2	2
3	1	2	4	1
3	1	4	2	1,3
3	1	4	2	1,3
3	4	1	2	2
3	4	1	2	2

Hence $\beta(\phi)=1$, $\beta(1)=2$, $\beta(2)=6$, $\beta(3)=2$, $\beta(1, 3)=4$, and all other $\beta(S)=0$.

Using the interpretation (1) of $\beta(S)$, we immediately get two interesting corollaries to Theorem 1.2.

1.3 COROLLARY. *Let (L, Δ) be an SS-lattice with $x < y$ in L . Then there is a unique unrefinable chain*

$$x = x'_0 < x'_1 < \dots < x'_m = y$$

between x and y such that

$$\gamma(x'_0, x'_1) < \gamma(x'_1, x'_2) < \dots < \gamma(x'_{m-1}, x'_m).$$

1.4 COROLLARY. *Let (L, Δ) be an SS-lattice with $x < y$ in L , with $r(y) - r(x) = m$. Then the number of unrefinable chains*

$$x = x'_0 < x'_1 < \dots < x'_m = y$$

between x and y satisfying

$$\gamma(x'_0, x'_1) > \gamma(x'_1, x'_2) > \dots > \gamma(x'_{m-1}, x'_m)$$

is equal to $(-1)^m \mu(x, y)$, where μ is the Möbius function of L . \square

Let Δ_{xy} denote the unique chain between x and y given by Corollary 1.3. It is not hard to see that Δ_{xy} is an M -chain of $[x, y]$ (this will be done in Section 3), so in fact $([x, y], \Delta_{xy})$ is an SS-lattice. Hence there is no loss of generality in restricting our attention to β rather than to β_{xy} .

From Theorem 1.2, we immediately see that

$$\beta_{xy}(S) \geq 0. \tag{2}$$

Using the Möbius-theoretic interpretation (1) of β , (2) may be restated as follows:

1.5 COROLLARY. *Let (L, Δ) be an SS -lattice of rank n , and let $S \subseteq \mathbf{n} - 1$. Then the Möbius function μ_S of the rank-selected subset $L(S)$ of L alternates in sign, i.e., if $[x, y]$ is a segment of $L(S)$ of length k , then*

$$(-1)^k \mu_S(x, y) \geq 0. \quad \square$$

Theorem 1.2 is a powerful tool for studying properties of $\beta(S)$, e.g., we trivially have (2). Observe also that the collection of descent sets (including repetitions) of the elements of $\mathcal{J}(L, \Delta)$ depend only on L and not on the M -chain Δ , since the same is obviously true of $\beta(S)$. A further result which will be given in Section 3 is:

(a) If $\beta(S) > 0$ and $T \subseteq S$, then $\beta(T) > 0$ (Proposition 3.3).

SS -lattices L which are also upper semimodular enjoy a number of properties not shared by general SS -lattices. Some of these are:

(b) When L is an upper semimodular SS -lattice (*USS-lattice*, for short), a necessary and sufficient condition for $\beta(S) > 0$ is given in terms of the existence of Loewy chains (i.e., chains $y_0 < y_1 < \dots < y_s$ for which every y_j , $1 \leq j \leq s$, is the join of atoms of the segment $[y_{j-1}, y_j]$) in L (Theorem 5.2).

(c) The *Birkhoff polynomial* (also called the *characteristic polynomial*) of a *USS*-lattice L has positive integral roots related to the structure of L (Theorem 4.1).

(d) For a special class of *USS*-lattices, $\beta(S)$ is divisible by a large power of an integer q (Section 6). This gives a lattice-theoretical generalization of some well-known results in the enumerative theory of p -groups.

In addition to the lattice-theoretical results mentioned above, our work also has applications to the combinatorial theory of permutations. The problem of analyzing permutations by their descents has received considerable attention (see, e.g., [9], [16]), and here we introduce a new and more general point of view.

2. Examples

The next proposition will make it easy to give a wide variety of examples of SS -lattices. First, we recall some lattice-theoretical results. These results were discovered mostly in the 1930s by Garrett Birkhoff, L. R. Wilcox, R. P. Dilworth, and others (see [1]). If x and y belong to a lattice L , we say that (x, y) is a *modular pair* (written xMy) if, for all $z \leq y$, we have $z \vee (x \wedge y) = (z \vee x) \wedge y$. In general, the relation of being a modular pair is *not* symmetric. In fact, Wilcox [18] showed that the relation of being a modular pair is symmetric if and only if L is upper semimodular. We say that x is a *modular element* of the lattice L if and only if xMy and yMx for all $y \in L$. If every element of L is modular, then L is a *modular lattice*.

2.1 PROPOSITION. *Let L be a finite lattice and Δ a maximal chain of L such that every element of Δ is modular. Then Δ is an M -chain of L .*

Proof. The proof is essentially the same as Birkhoff's proof of the less general result that a modular lattice generated by two chains is distributive (see [1, pp. 65-66]). We will merely point out why Birkhoff's proof applies to our more general result.

The only point of Birkhoff's proof which invokes modularity is in establishing the identities

$$(a_1 \wedge b_1) \vee \cdots \vee (a_r \wedge b_r) = a_1 \wedge (b_1 \vee a_2) \wedge \cdots \wedge (b_{r-1} \vee a_r) \wedge b_r; \quad (3)$$

$$(b_1 \vee a_1) \wedge \cdots \wedge (b_r \vee a_r) = b_1 \vee (a_1 \wedge b_2) \vee \cdots \vee (a_{r-1} \wedge b_r) \vee a_r, \quad (4)$$

when $a_i \geq a_{i+1}$ and $b_i \leq b_{i+1}$ in a modular lattice. We show that these identities still hold, however, if one only assumes that the a_i 's are modular, from which the proof of Proposition 2.1 follows.

We first prove (4) by induction on r . Set $A = (b_1 \vee a_1) \wedge \cdots \wedge (b_r \vee a_r)$. Now $b_1 \leq (b_2 \vee a_2) \wedge \cdots \wedge (b_r \vee a_r)$. Hence since $a_1 M (b_2 \vee a_2) \wedge \cdots \wedge (b_r \vee a_r)$, we have

$$A = b_1 \vee [a_1 \wedge (b_2 \vee a_2) \wedge \cdots \wedge (b_r \vee a_r)].$$

By induction,

$$A = b_1 \vee [a_1 \wedge \{b_2 \vee (a_2 \wedge b_3) \vee \cdots \vee (a_{r-1} \wedge b_r) \vee a_r\}].$$

Now $a_r \leq a_1$. Hence since $b_2 \vee (a_2 \wedge b_3) \vee \cdots \vee (a_{r-1} \wedge b_r) M a_1$, we have

$$A = b_1 \vee [a_1 \wedge \{b_2 \vee (a_2 \wedge b_3) \vee \cdots \vee (a_{r-1} \wedge b_r)\}] \vee a_r.$$

Now $(a_2 \wedge b_3) \vee \cdots \vee (a_{r-1} \wedge b_r) \leq a_1$. Hence since $b_2 M a_1$, we have

$$A = b_1 \vee (a_1 \wedge b_2) \vee (a_2 \wedge b_3) \vee \cdots \vee (a_{r-1} \wedge b_r) \vee a_r.$$

This proves (4).

We cannot just dualize (4) to prove (3), since the property of being a modular element is not self-dual. Instead, setting $B = (a_1 \wedge b_1) \vee \cdots \vee (a_r \wedge b_r)$, we have $(a_2 \vee b_2) \vee \cdots \vee (a_r \wedge b_r) \leq a_1$ and $b_1 M a_1$, so

$$B = a_1 \wedge [b_1 \vee (a_2 \wedge b_2) \vee \cdots \vee (a_r \wedge b_r)].$$

Now $b_1 \vee (a_2 \wedge b_2) \vee \cdots \vee (a_{r-1} \wedge b_{r-1}) \leq b_r$ and $a_r M b_r$, so

$$B = a_1 \wedge [b_1 \vee (a_2 \wedge b_2) \vee \cdots \vee (a_{r-1} \wedge b_{r-1}) \vee a_r] \wedge b_r.$$

By (4),

$$B = a_1 \wedge (b_1 \vee a_2) \wedge (b_2 \vee a_3) \wedge \cdots \wedge (b_{r-1} \vee a_r) \wedge b_r.$$

This proves (3), and with it, the proposition. \square

The converse to Proposition 2.1 is false in general. For instance, take L to be the lattice of subsets of $\{a, b, c\}$ ordered by inclusion except that the relation $\{a\} \subset \{a, b\}$ is excluded. Let Δ be the chain $\emptyset < \{c\} < \{b, c\} < \{a, b, c\}$. Then Δ is an M -chain, but $\{a\} M \{b, c\}$ is false. We have, however, the following partial converse.

2.2 PROPOSITION. *Let (L, Δ) be an SS-lattice. If $x \in \Delta$ and $y \in L$, then xMy .*

Proof. Let $z \leq y$. Since the sublattice generated by Δ , y , and z is distributive, *a fortiori* so is the sublattice generated by x , y , and z . Hence, xMy . \square

The converse to Proposition 2.2 is also false: take L to be the 5-element non-modular lattice and Δ to be the maximal chain of length 3.

Since the relation xMy is symmetric in an upper semimodular lattice, we deduce from Propositions 2.1 and 2.2, the following corollary.

2.3 COROLLARY. *Let L be a finite upper semimodular lattice, and let Δ be a maximal chain of L . Then Δ is an M -chain if and only if every element of Δ is modular.*

We are now in a position to give numerous examples of SS-lattices.

2.4 Example. If L is a finite modular lattice and Δ is any maximal chain of L , then trivially (L, Δ) is an SS-lattice.

2.5 Example. Let G be a supersolvable finite group and $L(G)$ its lattice of subgroups. Now every normal subgroup of any group G is a modular element of its lattice of subgroups [1, p. 172]. Hence since G is supersolvable, $L(G)$ contains a maximal chain of normal subgroups (corresponding to a chief series of G). Hence $L(G)$ is an SS-lattice, and every chief series of G is an M -chain (there may be other M -chains). Since it is the supersolvability of G which implies the existence of an M -chain in $L(G)$, this explains our terminology 'supersolvable lattice'.

Observe that from Corollary 1.5 (with $S = \mathbf{n} - \mathbf{1}$), we deduce the following interesting result: the Möbius function of the lattice of subgroups of a finite supersolvable group alternates in sign.

2.6 Example. Let Π_n denote the lattice of partitions of an n -set S [1, p. 95]. It is not difficult to see that a partition π of S is a modular element of Π_n if and only if at most one block of π has more than one element. From this it follows that Π_n is an SS-lattice with exactly $n!/2$ M -chains ($n > 1$). These M -chains are permuted among themselves transitively by the automorphisms of Π_n .

The next two examples generalize the previous example.

2.7 Example. A finite graph whose lattice of contractions [15, Section 9] is an

SS-lattice will be called an *SS-graph*. The next proposition (whose proof we omit) gives a characterization of SS-graphs. The case of complete graphs corresponds to the lattices Π_n of the previous example.

2.8 PROPOSITION. *Let G be a finite graph. Then G is an SS-graph if and only if the vertices of G can be labeled as v_1, v_2, \dots, v_n such that whenever $1 \leq i < j < k \leq n$ and v_k is connected by an edge to both v_i and v_j , then v_i and v_j are connected by an edge. If G is doubly-connected, then the number of M -chains in the lattice of contractions of G is equal to exactly half the number of such labelings (the labeling v_1, v_2, \dots, v_n being paired with the labeling obtained by interchanging v_1 and v_2). \square*

SS-graphs have been considered previously in different contexts under the name *triangulated graphs* or *rigid circuit graphs*. They are defined to be graphs for which every cycle of length at least four contains a chord.

2.9. Example. Let V be a projective space of rank n over $GF(q)$. Let L be the lattice of flats of the geometry (in the sense of Crapo-Rota [5]) determined by all the vectors in V with one or two nonzero entries. Then L is a geometric lattice of rank n . These interesting lattices were discovered by Dowling [8], who derived their basic properties (see also Doubilet-Rota-Stanley [7, Section 5 (c)]). In particular, when $q=2$, we get the partition lattices Π_{n+1} . For any q , the boolean algebra generated by the vectors in V which contain one nonzero entry consists of modular elements of L . (There will be additional modular elements only if $q=2$). Hence L is an SS-lattice, with $n!$ M -chains when $q > 2$.

2.10 Example. Let a_1, a_2, \dots, a_n be any sequence of positive integers with $a_1 = 1$. Let G be the geometry consisting of n independent points v_1, v_2, \dots, v_n , with an additional $a_i - 1$ points inserted on the line $v_i v_1$, $i > 1$. Then the lattice L of flats of G is an SS-lattice. L possesses an M -chain $\hat{0} = x_0 < x_1 < \dots < x_n = \hat{1}$ such that the number of points contained in x_i but not in x_{i-1} is a_i ($i = 1, 2, \dots, n$). The significance of this remark will become clear in Example 4.7.

2.11 Example. Let \mathfrak{R} denote the set of all partial orderings P on the set $\{1, 2, \dots, n\}$ satisfying $i < j$ in $P \Rightarrow i < j$ as integers. Define $P \leq Q$ in \mathfrak{R} if $i < j$ in $P \Rightarrow i < j$ in Q . Dean and Keller [6] showed that this order relation makes \mathfrak{R} into a lower semimodular lattice of rank $N = \binom{n}{2}$. Let Δ be the maximal chain $\hat{0} = P_0 < P_1 < \dots < P_N = \hat{1}$ of \mathfrak{R} where P_i is generated by the first i terms of the sequence $1 < n, 1 < n-1, 1 < n-2, \dots, 1 < 2, 2 < n, 2 < n-1, \dots, 2 < 3, 3 < n, 3 < n-1, \dots, 3 < 4, \dots, n-1 < n$. Then Δ is an M -chain of \mathfrak{R} , so (\mathfrak{R}, Δ) is an SS-lattice.

In all the above examples except for some cases of Example 1.3, either the lattice L or its dual L^* is upper semimodular. (It is clear that if (L, Δ) is an SS-lattice, then

so is (L^*, Δ^*) .) Some special properties of supersolvable semimodular lattices will be discussed in Sections 4–6, and additional properties will be given in a later paper.

3. Properties of SS-lattices

We begin by proving Theorem 1.2, viz., that the number of permutations π in the J - H set $\mathcal{J}_{xy} = \mathcal{J}_{xy}(L, \Delta)$ (where $[x, y]$ is a segment of length m in an SS-lattice (L, Δ)) with descent set $D(\pi) = S \subseteq \mathbf{m} - \mathbf{1}$ is equal to $\beta_{xy}(S)$. The proof is based on a simple lemma which is in fact a special case of Corollary 1.3.

3.1 LEMMA. *Let (L, Δ) be a distributive SS-lattice, and let $I < J$ in L . Then there is a unique unrefinable chain*

$$I = J_0 < J_1 < \cdots < J_m = J$$

in L between I and J such that

$$\gamma(J_0, J_1) < \gamma(J_1, J_2) < \cdots < \gamma(J_{m-1}, J_m). \quad (5)$$

Proof. Let $L = J(P)$. Suppose Δ is given by $\phi = I_0 < I_1 < \cdots < I_n = P$. Label the elements of P as x_1, x_2, \dots, x_m so that $x_i \in I_i - I_{i-1}$. Suppose $J - I = \{x_{i_1}, x_{i_2}, \dots, x_{i_m}\}$, where $i_1 < i_2 < \cdots < i_m$. Then condition (5) requires that $J_k = I \cup \{x_{i_1}, x_{i_2}, \dots, x_{i_k}\}$. Moreover, with this definition of J_k , we indeed have that $J_0 < J_1 < \cdots < J_m$ is an unrefinable chain between I and J , so the proof is complete. \square

Proof of Theorem 1.2. Let $\delta_{xy}(S)$ be the number of permutations $\pi \in \mathcal{J}_{xy}$ with descent set S . Thus we need to show that $\beta_{xy}(S) = \delta_{xy}(S)$ for all $S \subseteq \mathbf{m} - \mathbf{1}$.

Let K be a maximal chain of the segment $[x, y]$,

$$K: x = y_0 < y_1 < \cdots < y_m = y, \quad (6)$$

with associated J - H permutation π_K . If $S = \{m_1, m_2, \dots, m_s\} \subseteq \mathbf{m} - \mathbf{1}$, denote by K_S the chain

$$K_S: y_{m_1} < y_{m_2} < \cdots < y_{m_s}. \quad (7)$$

We shall show that the correspondence $K \rightarrow K_S$ is a bijection between maximal chains K of $[x, y]$ satisfying $D(\pi_K) \subseteq S$ and chains K_S of L satisfying

$$\{r(z) - r(x) \mid z \in K_S\} = S. \quad (8)$$

This will show that $\sum_{T \in S} \delta_{xy}(T)$ is equal to the number of chains satisfying (8), i.e.,

$$\sum_{T \in S} \delta_{xy}(T) = \alpha_{xy}(S). \quad (9)$$

But (9) uniquely determines the $\delta_{xy}(S)$'s and is also the recursion satisfied by the $\beta_{xy}(S)$'s. Hence it will follow that $\delta_{xy}(S) = \beta_{xy}(S)$.

We need to show that given a chain K' satisfying $\{r(z) - r(x) | z \in K'\} = S$, then there is a unique maximal chain K of $[x, y]$ satisfying (i) $D(\pi_K) \subseteq S$, and (ii) $K_S = K'$. Condition (ii) is equivalent to: K' is a subchain of K . Thus if K' is given by (7) and K by (6), then condition (i) is equivalent to the conditions

$$\begin{aligned} \gamma(y_0, y_1) &< \gamma(y_1, y_2) < \dots < \gamma(y_{m_1-1}, y_{m_1}), \\ \gamma(y_{m_1}, y_{m_1+1}) &< \gamma(y_{m_1+1}, y_{m_1+2}) < \dots < \gamma(y_{m_2-1}, y_{m_2}), \\ &\vdots \\ \gamma(y_{m_s}, y_{m_s+1}) &< \gamma(y_{m_s+1}, y_{m_s+2}) < \dots < \gamma(y_{m-1}, y_m). \end{aligned} \quad (10)$$

Let L' be the distributive lattice generated by $K' \cup \{x, y\}$ and Δ . Then by Lemma 3.1, there is a unique maximal chain K of L' satisfying (i) and (ii). K is also a maximal chain of $[x, y]$ since every maximal chain of L' has the same length as Δ . If K_1 were another maximal chain of L satisfying (i) and (ii), then since $K' \subseteq K_1$ the distributive lattice generated by $K_1 \cup \{x, y\}$ and Δ would contain the two chains K and K_1 satisfying (i) and (ii). This contradicts Lemma 3.1, so the theorem is proved. \square

We now clarify the relationship between the J - H sets $\mathcal{J}_{xy}(L, \Delta)$ (where $x \leq y$ in L) and $\mathcal{J}(L, \Delta)$.

3.2 PROPOSITION. *Let (L, Δ) be an SS-lattice, and let $x \leq y$ in L . Denote by L' the segment $[x, y]$, considered as a lattice in its own right. Let $\Delta' = \Delta_{xy}$ be the unique maximal chain in L' given by Corollary 1.3. Then*

(i) (L', Δ') is an SS-lattice.

(ii) *Suppose Δ is given by $\hat{0} = x_0 < x_1 < \dots < x_n = \hat{1}$ and Δ' by $x = y_0 < y_1 < \dots < y_m = y$. Let γ refer to (L, Δ) and γ' to (L', Δ') . Suppose y' covers x' , where x' and y' lie in L' . If $i = \gamma(x', y')$ and $j = \gamma'(x', y')$, then i and j satisfy*

$$\begin{aligned} i &= \gamma(x_{i-1}, x_i) = \gamma(y_{j-1}, y_j) \\ j &= \gamma'(y_{j-1}, y_j). \end{aligned}$$

(iii) *If y' covers x' and y'' covers x'' , where x', y', x'', y'' all lie in L' , then $\gamma(x', y') > \gamma(x'', y'')$ if and only if $\gamma'(x', y') > \gamma'(x'', y'')$.*

Proof. (i) Let K' be a chain in L' . We need to prove that Δ' and K' generate a distributive lattice. Now $K'' = K' \cup \{x, y\}$ is also a chain, so Δ and K'' generate a distributive lattice D . But Δ' is contained in the lattice generated by Δ and $\{x, y\}$. Hence $\Delta' \subseteq D$, so the lattice generated by Δ' and K' is distributive.

(ii) That $i = \gamma(x_{i-1}, x_i)$ and $j = \gamma'(y_{j-1}, y_j)$ is immediate from the definition of γ and γ' . Thus the prime intervals $[x', y']$ and $[y_{j-1}, y_j]$ are projective in L' ; hence they are projective in L . Since projectivity is transitive, $[y_{j-1}, y_j]$ and $[x_{i-1}, x_i]$ are projective. Thus $\gamma(y_{j-1}, y_j) = i$.

(iii) Follows immediately from (ii). \square

The significance of Proposition 3.2(iii) is that it allows one to compute the J - H set $\mathcal{J}(L', \Delta')$ once the 'relative' J - H set $\mathcal{J}_{xy}(L, \Delta)$ is known. For instance, a permutation $(4, 8, 2, 6, 3)$ in $\mathcal{J}_{xy}(L, \Delta)$ corresponds to a permutation $(3, 5, 1, 4, 2)$ in $\mathcal{J}(L', \Delta')$.

We turn to an interesting property of the numbers $\beta(S)$.

3.3 PROPOSITION. *Let (L, Δ) be an SS-lattice of rank n , and let $S \subseteq \mathbf{n}-1$. If $\beta(S) > 0$ and $T \subseteq S$, then $\beta(T) > 0$.*

Proof. Suppose $S = \{m_1, m_2, \dots, m_s\} <$ and $\beta(S) > 0$. Then there is a maximal chain

$$K: \hat{0} = y_0 < y_1 < \dots < y_n = \hat{1}$$

such that $D(\pi_K) = S$, where $D(\pi_K)$ is the descent set of the J - H permutation π_K . For any i satisfying $1 \leq i \leq s$, we have, by Corollary 1.3, a (unique) unrefinable chain

$$y_{m_{i-1}} = y'_0 < y'_1 < \dots < y'_r = y_{m_{i+1}}$$

between $y_{m_{i-1}}$ and $y_{m_{i+1}}$ (with the convention $m_0 = 0, m_{s+1} = n$) satisfying

$$\gamma(y'_0, y'_1) < \gamma(y'_1, y'_2) < \dots < \gamma(y'_{r-1}, y'_r).$$

Hence the chain K' given by

$$\hat{0} = y_0 < y_1 < \dots < y_{m_{i-1}} < y'_1 < y'_2 < \dots < y'_r < y_{m_{i+1}+1} < y_{m_{i+1}+2} < \dots < y_n = \hat{1}$$

satisfies $D(\pi_{K'}) = S - \{m_i\}$, so $\beta(S - \{m_i\}) > 0$. By a trivial inductive argument, $\beta(T) > 0$ for any $T \subseteq S$. \square

The numbers $\beta(S)$ provide a means of giving ' q -analogues' and ' Π -analogues' of certain well-known combinatorial numbers. For instance, let L be a direct product of chains of lengths n_1, n_2, \dots, n_r , so that L is a distributive lattice of rank $n = n_1 + n_2 + \dots + n_r$. If $S = \{m_1, m_2, \dots, m_s\} < \subseteq \mathbf{n}-1$, then MacMahon [13, Sections 167-168] has studied the relation between the numbers $\beta(S)$ and the theory of distribution of objects. He uses the notation $N(\mu)_\lambda = \beta(S)$, where λ is the partition of n into parts n_1, n_2, \dots, n_s , and where $S = \{\mu_1, \mu_1 + \mu_2, \mu_1 + \mu_2 + \mu_3, \dots, \mu_1 + \mu_2 + \dots + \mu_{r-1}\}$. The p -analog of the lattice L (at least when p is prime) is the lattice of subgroups of an abelian p -group of type (n_1, n_2, \dots, n_r) . Hence we get a p -analog of MacMahon's invariants $N(\mu)_\lambda$. Some properties of these numbers will be discussed in a subsequent paper.

As a further example, if L is a boolean algebra of rank n and $0 \leq s \leq n-1$, then $A_{ns} = \sum \beta(S)$ is an Eulerian number [14], where the sum is over all subsets of $\mathbf{n}-1$ of cardinality $n-s$ (see [16, Section 13]) Hence if L is the lattice of subspaces of a

projective geometry of dimension n over $GF(q)$, we get a q -analog of the Eulerian numbers. These q -Eulerian numbers differ from those of Carlitz [3]. In fact, Carlitz's q -Eulerian numbers $A_{ns}(q)$ can be defined as

$$A_{ns}(q) = \sum_S \beta(S) q^{2S},$$

where L is a boolean algebra of rank n , S ranges over all subsets of $\mathbf{n}-1$ of cardinality $n-s$, and $\sum S$ is the sum of the elements of S .

If we take $L = \Pi_{n+1}$ (cf. Example 2.6), then $\sum \beta(S)$, where S ranges over all subsets of $\mathbf{n}-1$ of cardinality $n-s$, is a ' H -Eulerian number'. These numbers seem never to have been considered before and may be of further interest.

4. The Birkhoff polynomial

In the remaining three sections of this paper, we will be largely concerned with upper-semimodular SS -lattices, or USS -lattices for short. Let L be a finite lattice with a rank function r , and let n be the rank of L . The *Birkhoff polynomial* $p(\lambda)$ (also called the *characteristic polynomial* [5] or *Poincaré polynomial* [4]) of L is defined by

$$p(\lambda) = \sum_{x \in L} \mu(\hat{0}, x) \lambda^{n-r(x)},$$

where μ denotes the Möbius function of L . This concept is due to G. D. Birkhoff [2], though usually it is only defined for more restrictive classes of lattices.

We shall show that the Birkhoff polynomial $p(\lambda)$ of a USS -lattice L of rank n has nonnegative integral roots $a_1 = 1, a_2, \dots, a_n$ connected with the structure of L . In particular, $\mu(\hat{0}, \hat{1}) = (-1)^n a_1 a_2 \dots a_n$. This fact can be proved in a purely lattice-theoretic way by applying the 'factorization theorem' of Stanley [17] (in fact, the following theorem led to the discovery of the factorization theorem), but in the supersolvable case we can gain more insight into the structure of $p(\lambda)$ by employing a different approach. Specifically, the coefficients of $p(\lambda)$ are symmetric functions in the a_i 's, and we shall attach a combinatorial meaning to each term of these symmetric functions.

4.1 THEOREM. *Let (L, Δ) be a USS -lattice of rank n with Δ given by $\hat{0} = x_0 < x_1 < \dots < x_n = \hat{1}$, and let a_i be the number of atoms x of L satisfying $\gamma(\hat{0}, x) = i$ (i.e., $x \leq x_i$ but $x \not\leq x_{i-1}$). Then*

$$p(\lambda) = (\lambda - a_1)(\lambda - a_2) \dots (\lambda - a_n).$$

In particular, $\mu(\hat{0}, \hat{1}) = (-1)^n a_1 a_2 \dots a_n$.

Proof. Let $x \in L$ with $r(x) = m$. By Corollary 1.4, $(-1)^m \mu(\hat{0}, x)$ is equal to the

number of chains $\hat{0} = y_0 < y_1 < \dots < y_m = x$ such that $i_1 > i_2 > \dots > i_m$, where $i_j = \gamma(y_{j-1}, y_j)$. Hence the coefficient of λ^{n-m} in $p(\lambda)$ is equal to $(-1)^m$ times the total number of chains $\hat{0} = y_0 < y_1 < \dots < y_m$ with $i_1 > i_2 > \dots > i_m$ (where $i_j = \gamma(y_{j-1}, y_j)$ as before).

Fix a sequence $n > i_1 > i_2 > \dots > i_m \geq 1$. We prove by induction on m that:

(A) The number of chains $\hat{0} = y_0 < y_1 < \dots < y_m$ satisfying $r(y_m) = m$ and $i_j = \gamma(y_{j-1}, y_j)$ ($j = 1, 2, \dots, m$) is $a_{i_1} a_{i_2} \dots a_{i_m}$.

Assertion (A) is clearly true for $m = 1$, by definition of a_i . Assume true for $m - 1$. We thus have $a_{i_1} a_{i_2} \dots a_{i_{m-1}}$ chains $\hat{0} = y_0 < y_1 < \dots < y_{m-1}$ with $i_j = \gamma(y_{j-1}, y_j)$ ($1 \leq j \leq m - 1$), and it suffices to prove that there are precisely a_{i_m} elements y_m covering y_{m-1} such that $i_m = \gamma(y_{m-1}, y_m)$. Suppose y_m covers y_{m-1} and $i_m = \gamma(y_{m-1}, y_m)$. Then i_m is the least element of the set $\Gamma(y_m)$. Applying Corollary 1.3 to the case $x = \hat{0}$, $y = y_m$, it follows that there is a unique atom $x' \in L$ satisfying $x' \leq y_m$ and $\gamma(\hat{0}, x') = i_m$. Conversely, given any atom x' satisfying $\gamma(\hat{0}, x') = i_m$, then we can take $y_m = x' \vee y_{m-1}$. (This is where the assumption of upper-semimodularity is needed.) Hence there is a one-to-one correspondence between the y_m 's and the atoms x' of L satisfying $\gamma(\hat{0}, x') = i_m$. Since there are a_{i_m} such atoms, the proof of (A) follows by induction.

Thus the coefficient of λ^{n-m} in $p(\lambda)$ is equal to $(-1)^m \sum a_{i_1} a_{i_2} \dots a_{i_m}$, the sum being over all sequences $n \geq i_1 > i_2 > \dots > i_m \geq 1$, so $p(\lambda) = (\lambda - a_1)(\lambda - a_2) \dots (\lambda - a_n)$. \square

Note that Theorem 4.1 shows that no matter what M -chain Δ we choose for L , the set of a_i 's is uniquely determined; on the other hand, easy examples show that their order can vary (though trivially, $a_1 = 1$).

We now give various examples which illustrate Theorem 4.1.

4.2 *Example.* If L is a boolean algebra of rank n , then each $a_i = 1$ so $p(\lambda) = (\lambda - 1)^n$.

4.3 *Example.* If L is a projective geometry of rank n over $GF(q)$, then $a_i = q^i$ so $p(\lambda) = (\lambda - 1)(\lambda - q) \dots (\lambda - q^{n-1})$.

4.4 *Example.* Let $L = H_{n+1}$ with the M -chain of Example 2.6. Then $a_i = i$ so $p(\lambda) = (\lambda - 1)(\lambda - 2) \dots (\lambda - n)$.

4.5 *Example.* Let L be Dowling's lattice of rank n over $GF(q)$ (cf. Example 2.9). Let $\hat{0} = x_0 < x_1 < \dots < x_n = \hat{1}$ be the M -chain in L such that x_i contains all the vectors v generating L whose nonzero entries appear among the first coordinates of v . Thus x_i contains i vectors with one nonzero entry and $\binom{i}{2} (q - 1)$ vectors with two nonzero entries. Hence

$$\begin{aligned} a_i &= \left[i + \binom{i}{2} (q - 1) \right] - \left[i - 1 + \binom{i - 1}{2} (q - 1) \right] \\ &= 1 + (i - 1)(q - 1). \end{aligned}$$

Therefore $p(\lambda) = (\lambda - 1)(\lambda - q)(\lambda - 2q + 1)(\lambda - 3q + 2) \cdots (\lambda - (n - 1)q + n - 2)$, a result proved by Dowling by other means.

4.6 Example. Let G be an SS -graph, as defined in Example 2.7. Let v_1, v_2, \dots, v_n be a labeling of the vertices of G in accordance with Proposition 2.8. Suppose v_i is connected to exactly a_{i-1} vertices v_j with $j < i$. Then by Proposition 2.8, these vertices form a clique (complete subgraph), from which it follows that the chromatic polynomial of G is given by $\lambda(\lambda - a_1)(\lambda - a_2) \cdots (\lambda - a_n)$. By [15, Section 9], the Birkhoff polynomial $p(\lambda)$ of the lattice of contractions of G is $(\lambda - a_1)(\lambda - a_2) \cdots (\lambda - a_n)$. Loosely speaking, an SS -graph is a graph whose chromatic polynomial can be 'trivially' calculated. Note that a polynomial $p(\lambda)$ is the Birkhoff polynomial of the lattice of contractions of some SS -graph if and only if the roots of $p(\lambda)$ are positive integers such that if $a > 1$ is a root, then $a - 1$ is a root.

4.7 Example. In Example 2.10, a geometric SS -lattice was constructed with an M -chain $\hat{0} = x_0 < x_1 < \cdots < x_n = \hat{1}$, such that exactly a_i atoms x satisfy $\gamma(\hat{0}, x) = i$, for any set a_1, a_2, \dots, a_n of positive integers with $a_1 = 1$. Hence $p(\lambda) = (\lambda - a_1)(\lambda - a_2) \cdots (\lambda - a_n)$. It follows that a polynomial $p(\lambda)$ is the Birkhoff polynomial of a geometric SS -lattice if and only if the roots of $p(\lambda)$ are positive integers, including the integer 1. Unfortunately, there exist finite geometric lattices which are *not* SS -lattices but whose Birkhoff polynomials have only positive integral roots. For instance, take a 5-point line and two others points in the same plane. The Birkhoff polynomial of the resulting geometric lattice L is $(\lambda - 1)(\lambda - 3)^2$, but L is not supersolvable.

5. Loewy chains

Following Zassenhaus [19, p. 215] (who, however, only considers modular lattices), we define a *Loewy chain* in a lattice L of finite length as a chain

$$\hat{0} = y_0 < y_1 < \cdots < y_r = \hat{1}$$

such that each y_i is the join of the atoms of the segment $[y_{i-1}, y_i]$. If L is upper-semimodular, this is equivalent to saying that each segment $[y_{i-1}, y_i]$ is complemented. This does not mean that each segment $[y_{i-1}, y_i]$ is relatively complemented, or that every element of $[y_{i-1}, y_i]$ is a join of atoms of $[y_{i-1}, y_i]$ (in other words, $[y_{i-1}, y_i]$ need not be a geometric lattice). Recall, however, that every complemented modular lattice is relatively complemented [1, p. 16].

A sufficient condition for a chain of an SS -lattice to be a Loewy chain is provided by the next lemma.

5.1 LEMMA. *Let (L, Δ) be an SS -lattice, and let K be a maximal chain*

in L ,

$$K: \hat{0} = y_0 < y_1 < \cdots < y_n = \hat{1}.$$

Let $0 < m_1 < m_2 < \cdots < m_r = n$. Then the subchain

$$\hat{0} = y_0 < y_{m_1} < y_{m_2} < \cdots < y_{m_r} = \hat{1}$$

is a Loewy chain if

$$\mathbf{n} - \mathbf{1} - D(\pi_K) \subseteq \{m_1, m_2, \dots, m_{r-1}\}.$$

Proof. We need to prove that if, for $1 \leq j < k \leq n$, we have $\gamma(y_j, y_{j+1}) > \gamma(y_{j+1}, y_{j+2}) > \cdots > \gamma(y_{k-1}, y_k)$, then y_k is the join of atoms of the segment $[y_j, y_k]$.

First method. If $\gamma(y_j, y_{j+1}) > \cdots > \gamma(y_{k-1}, y_k)$, then by Corollary 1.4, $\mu(y_j, y_k) \neq 0$. By a theorem of P. Hall [11, Thm. 2.3] (see also, Rota [15, p. 349]), y_k is the join of atoms of $[y_j, y_k]$.

Second method. Let Δ' be the M -chain of $[y_j, y_k]$ induced by Δ (via Proposition 3.2), say, $\Delta': y_j = x'_0 < x'_1 < \cdots < x'_m = y_k$ ($m = k - j$). Let $L' = J(P)$ be the distributive lattice generated by Δ' and the chain $y_j < y_{j+1} < \cdots < y_k$. Regarding each x'_i and y_i as an order ideal of P , and assuming $\gamma(y_j, y_{j+1}) > \cdots > \gamma(y_{k-1}, y_k)$, we see that $x_{i+1} - x_i = y_{m-i} - y_{m-i-1}$. It follows that P is an antichain, so L' is a boolean algebra. Thus y_k is the join of atoms of L' . Since every atom of L' is an atom of $[y_j, y_k]$, the proof follows. \square

We now come to a fundamental theorem telling us when $\beta(S) > 0$ in a USS-lattice.

5.2 THEOREM. Let (L, Δ) be a USS-lattice of rank n , and let $S = \{m_1, m_2, \dots, m_s\} \subset \mathbf{n} - \mathbf{1}$. There exists a chain C ,

$$C: \hat{0} = y_0 < y_1 < \cdots < y_s < y_{s+1} = \hat{1},$$

satisfying the two conditions

- (i) $r(y_i) = m_i$, $1 \leq i \leq s$;
- (ii) each y_i ($1 \leq i \leq s+1$) is the join of atoms of the segment $[y_{i-1}, y_i]$, i.e., C is a Loewy chain, if and only if $\beta(\mathbf{n} - \mathbf{1} - S) > 0$.

Proof. If $\beta(\mathbf{n} - \mathbf{1} - S) > 0$, then there exists a maximal chain K such that $D(\pi_K) = \mathbf{n} - \mathbf{1} - S$. By Lemma 5.1, the subchain $\hat{0} = y_0 < y_1 < \cdots < y_s < y_{s+1} = \hat{1}$ of K satisfying $r(y_i) = m_i$ ($1 \leq i \leq s$) is a Loewy chain.

Conversely, suppose we have a chain $C: \hat{0} = y_0 < y_1 < \cdots < y_s < y_{s+1} = \hat{1}$, satisfying (i) and (ii). Let k satisfy $1 \leq k \leq s+1$, and define $x = y_{k-1}$, $y = y_k$. Suppose $r(y) - r(x) = m$. We will establish the existence of a maximal chain K_k in $[x, y]$,

$$K_k: x = z_0 < z_1 < \cdots < z_m = y,$$

such that

$$\gamma(z_0, z_1) > \gamma(z_1, z_2) > \cdots > \gamma(z_{m-1}, z_m).$$

The proof is based on the following lemma:

(A) *If $[u, v]$ is a segment of an SS-lattice such that v is the join of atoms of $[u, v]$, then there is an atom w of $[u, v]$ such that $\gamma(u, w)$ is the largest element of $\Gamma(u, v)$.*

Proof of (A). Let v' be the element of the induced M -chain Δ_{uv} which is covered by v . Since v is a join of atoms, some atom w of $[u, v]$ satisfies $w \not\leq v'$. Hence $\gamma(u, w)$ is the largest element of $\Gamma(u, v)$, proving (A).

Now, since y is the join of atoms of $[x, y]$, by (A), we have an atom z_1 such that $\gamma(z_0, z_1)$ is the largest element of $\Gamma(x, y)$. Since L is upper-semimodular, for any $z \in [x, y]$, we have that y is the join of atoms of $[z, x]$. (This is where the assumption of upper-semimodularity is needed.) In particular, y is the join of atoms of $[z_1, y]$. Thus, by (A), there is an atom z_2 of $[z_1, y]$ such that $\gamma(z_1, z_2)$ is the largest element of $\Gamma(z_1, y)$. Continuing in this way, we get a maximal chain $K_k: x = z_0 < z_1 < \cdots < z_m = y$ such that $\gamma(z_{i-1}, z_i)$ is the largest element of $\Gamma(z_{i-1}, y)$, so

$$\gamma(z_0, z_1) > \gamma(z_1, z_2) > \cdots > \gamma(z_{m-1}, z_m).$$

The union of these chains K_k ($1 \leq k \leq s+1$) is then a maximal chain K of L (containing C), satisfying $\mathbf{n}-1-D(\pi_K) \subseteq S$. Then $\mathbf{n}-1-S \subseteq D(\pi_K)$, so by Proposition 3.3, $\beta(\mathbf{n}-1-S) > 0$. \square

Conjecture. Equation (2), Proposition 3.3, and Theorem 5.2 are valid for any finite upper-semimodular lattice L .

6. q -USS-lattices

Recall that the *degree* of a projective geometry V is one less than the number of points on a line. In particular, if V is coordinatized by the field $GF(q)$, then $\deg V = q$. If L is the lattice of subspaces of a projective geometry of degree q , then the integer q enters into many of the combinatorial properties of L . Our object in this section is to define a general class of upper-semimodular lattices L 'based on' the integer q , and, in the SS-case, to show how q enters into the global combinatorial properties of L .

6.1 DEFINITION. Let q be a fixed positive integer. A q -lattice is a lattice L of finite length with the property that every segment $[x, y]$ of L for which y is the join of atoms of $[x, y]$ is isomorphic to the lattice of subspaces of a projective geometry of degree q (or to a boolean algebra if $q=1$).

Observe that every q -lattice is necessarily upper-semimodular, since if y and z

cover x , then the segment $[x, y \vee z]$ is a projective geometry or boolean algebra, so $y \vee z$ covers y and z .

6.2 *Example.* Let $L^*(G)$ denote the dual of the lattice of subgroups of a finite p -group G . Since G is supersolvable, we know from Example 2.5 that $L^*(G)$ is an SS -lattice. In addition, $L^*(G)$ is a p -lattice. This fact is essentially well known, but for the sake of completeness we shall sketch a proof. If G is any finite p -group and if $\Phi(G)$ is the Frattini subgroup of G (intersection of all maximal subgroups), then the quotient group $G/\Phi(G)$ is an elementary abelian p -group [10, Thm. 12.2.1]. Hence, if $H \in L^*(G)$ and H' denotes the join of all elements in $L^*(G)$ covering H , then $H' = \Phi(H)$, and the segment $[H, H']$ is isomorphic to the dual of the lattice of subgroups of the elementary abelian p -group H/H' . Since this lattice is a projective geometry over $GF(p)$, $L^*(G)$ is a p -lattice. We therefore say that $L^*(G)$ is a p - SS -lattice.

6.3 *Example.* Let \mathfrak{R} denote the lattice of natural partial orders on the set \mathbf{n} , as defined in Example 2.11. It is easily seen that the dual \mathfrak{R}^* is a 1- SS -lattice. Indeed, if $[P, Q]$ is a segment of \mathfrak{R}^* such that y is a join of atoms of $[P, Q]$, then Q is obtained from P by removing a set S of relations of the form $i < j$ where j covers i in P ; and the general element of $[P, Q]$ is obtained by removing an arbitrary subset of the relations in S . Hence $[P, Q]$ is a boolean algebra.

The basic result on q - SS -lattices is the following.

6.4 LEMMA. Let (L, Δ) be a q - SS -lattice of rank n ; let σ be a permutation of $\{1, 2, \dots, n\}$ with $\mathbf{n}-1 - D(\sigma) = \{j_1, j_2, \dots, j_t\}$ (where $D(\sigma)$ is the descent set of σ); and let $j_0 = 0, j_t = n$. Then the number of maximal chains K of L satisfying $\sigma = \pi_K$ is equal to $q^k M$, where

$$k = \sum_{r=1}^t \binom{j_r - j_{r-1}}{2}, \quad (11)$$

and where M is the number of Loewy chains

$$C: \hat{0} = y_0 < y_1 < \dots < y_t = \hat{1} \quad (12)$$

such that $r(y_i) = j_i$ and $\Gamma(y_i) = \{\sigma(1), \sigma(2), \dots, \sigma(j_i)\}$, $0 \leq i \leq t$.

Proof. If K is a maximal chain of L , satisfying $\pi_K = \sigma$, then by Lemma 5.1, the subchain C of K consisting of all $x \in K$ such that $r(x) = j_i$ ($0 \leq i \leq t$) is a Loewy chain, while, by definition of π_K and Γ , we have $\Gamma(y_i) = \{\sigma(1), \sigma(2), \dots, \sigma(j_i)\}$. Hence it suffices to prove that if we have a Loewy chain (12) with $r(y_i) = j_i$ and $\Gamma(y_i) = \{\sigma(1), \sigma(2), \dots, \sigma(j_i)\}$, then the number of refinements of C to a maximal chain K , satisfying $\pi_K = \sigma$, is equal to q^k , where k is given by (11).

Assume we have such a Loewy chain C . Since L is a q -lattice, each segment

$[y_{r-1}, y_r]$ ($1 \leq r \leq t$) is a projective geometry of degree q . Hence $\mu(y_{r-1}, y_r) = (-1)^b q^{k_r}$, where $b = j_r - j_{r-1}$ and $k_r = \binom{j_r - j_{r-1}}{2}$. Now, by Corollary 1.4, the number of maximal chains $y_{r-1} = z_0 < z_1 < \dots < z_b = y_r$ of the segment $[y_{r-1}, y_r]$ such that

$$\gamma(z_0, z_1) > \gamma(z_1, z_2) > \dots > \gamma(z_{b-1}, z_b)$$

is just $(-1)^b \mu(y_{r-1}, y_r) = q^{k_r}$. Hence the total number of refinements of C to a maximal chain K , satisfying $\pi_K = \sigma$, is equal to $q^{k_1} q^{k_2} \dots q^{k_t} = q^k$, and the proof follows. \square

6.5 COROLLARY. Let (L, Δ) be a q -SS-lattice of rank n , and let $S \subseteq \mathbf{n-1}$. Set $\mathbf{n-1} - S = \{j_1, j_2, \dots, j_{t-1}\} <$, with $j_0 = 0, j_t = n$. Then $\beta(S)$ is divisible by q^k , where k is given by (11). \square

If n is a positive integer and $0 \leq s \leq n-1$, define

$$Q(n, s) = \frac{1}{2} \left[\frac{n}{n-s} \right] \left(n + s - (n-s) \left[\frac{n}{n-s} \right] \right)$$

(brackets denote the integer part).

6.6 THEOREM. Let (L, Δ) be a q -SS-lattice of rank n , and let $S \subseteq \mathbf{n-1}$ with $|S| = s$. Then $\beta(S)$ is divisible by $q^{Q(n, s)}$. This result is best possible in the sense that, given n and $0 \leq s \leq n-1$, there exists a q -SS-lattice of rank n and a set $S \subseteq \mathbf{n-1}$ of cardinality s such that $\beta(S) = q^{Q(n, s)}$.

Proof. Let K be a maximal chain of L with $D(\pi_K) = S$, and let $\mathbf{n-1} - S = \{j_1, j_2, \dots, j_{t-1}\} <$, so $s + t = n$. It follows from Corollary 6.5 that $\beta(S)$ is divisible by q^m , where

$$m = \min \sum_{r=1}^t \binom{j_r - j_{r-1}}{2},$$

the minimum being taken over all sequences $0 = j_0 < j_1 < \dots < j_t = n$. We shall show that this minimum is equal to $Q(n, s)$.

If $0 \leq a < b$, then it is easily verified that

$$\binom{a}{2} + \binom{b}{2} \geq \binom{a+1}{2} + \binom{b-1}{2}.$$

Hence the sum (11) is minimized when the differences $j_1 - j_0, j_2 - j_1, \dots, j_t - j_{t-1}$ are as nearly equal as possible. Given n and $t \geq 1$, it is easy to show that there is a unique partition $\lambda = \lambda(n, t)$ of n into t parts such that each part is one of two consecutive integers. In this partition λ , the part $[n/t] + 1$ appears $n - t[n/t]$ times and the part $[n/t]$ appears $t(1 + [n/t]) - n$ times. Hence the sum (11) is minimized when $n - t[n/t]$

of the differences $j_r - j_{r-1}$ are equal to $\lceil n/t \rceil + 1$ and $t(1 + \lceil n/t \rceil) - n$ of them are equal to $\lceil n/t \rceil$. Setting $C = \lceil n/t \rceil$ and using $t = n - s$, we get

$$\begin{aligned} m &= (n - tC) \binom{C+1}{2} + (t(1+C) - n) \binom{C}{2} \\ &= \frac{1}{2}C(2n - t - tC) \\ &= Q(n, s). \end{aligned}$$

To prove that this result is best possible given n and s , choose $0 = j_0 < j_1 < \dots < j_t = n$ so as to minimize the sum (11) (so this minimum value is $Q(n, s)$). For $1 \leq r \leq t$, let V_r be a projective geometry over $GF(q)$ of rank $j_r - j_{r-1}$. Let L be obtained by 'stacking' the V_r 's, i.e., by identifying the top element of V_{r-1} with the bottom element of V_r . Then L is a q -SS-lattice (in fact, a q -modular lattice), and it is clear (e.g., from Theorem 1.2) that if $S = \mathbf{n} - \mathbf{1} - \{j_1, j_2, \dots, j_{t-1}\}$, then $|S| = s$ and $\beta(S) = q^{Q(n, s)}$. \square

For fixed s , the function $Q(n, s)$ exhibits the following behavior:

$$\begin{aligned} \binom{s+1}{2} &= Q(s+1, s) > Q(s+2, s) > \dots > Q(2s-1, s) > Q(2s, s) \\ &= Q(2s+1, s) = \dots = s. \end{aligned}$$

Thus the sequence $Q(n, s)$ (for fixed s) becomes 'stable' at the value s when $n \geq 2s$.

6.7 COROLLARY. *Let L be a q -SS-lattice of rank n , and let $0 \leq m \leq n$. The number of elements of L of rank m is congruent to $1 \pmod{q}$.*

Proof. The number of such elements is $\alpha(m) = \beta(m) + 1$. Now $Q(n, 1) = 1$, so $\beta(m)$ is divisible by q . \square

As a special case of Corollary 6.7, we get the well-known result of P. Hall [12] that the number of subgroups of a given order in a finite p -group is congruent to $1 \pmod{p}$. Thus Theorem 6.6 gives a lattice-theoretical generalization of this result, which, even in the case of the lattice of subgroups of p -groups, appears to be new. We ask whether there are similar lattice-theoretic arguments for proving stronger results in the enumerative theory of p -groups, e.g., Kulakoff's theorem [19, p. 153].

Conjecture. Corollary 6.5 and Theorem 6.6 are valid for any finite q -lattice L .

REFERENCES

- [1] Garrett Birkhoff, *Lattice Theory* (third ed.), American Mathematical Society, Providence, R.I. (1967).
- [2] G. D. Birkhoff, *A determinant formula for the number of ways of coloring a map*, *Annals of Math.* 14 (1912), 42-46.

- [3] L. Carlitz, *q-Bernoulli and Eulerian numbers*, Trans. Amer. Math. Soc. 76 (1954), 332-350.
- [4] H. H. Crapo, *The Tutte polynomial*, Aequationes Math. 3 (1969), 211-229.
- [5] H. H. Crapo and G.-C. Rota, *On the Foundations of Combinatorial Theory: Combinatorial Geometries*, M.I.T. Press (1970).
- [6] R. A. Dean and G. Keller, *Natural partial orders*, Canad. J. Math. 20 (1968), 535-554.
- [7] P. Doubilet, G.-C. Rota, and R. P. Stanley, *On the foundations of combinatorial theory: The idea of generating function*, Sixth Berkeley Symposium on Mathematical Statistics and Probability (to appear).
- [8] T. A. Dowling, *A g-analog of the partition lattice*, Proc. International Symposium on Combinatorial Mathematics and Its Applications, Colorado State University, Fort Collins, Colorado, September 9-11 (1971) (to appear).
- [9] D. Foata and M. P. Schützenberger, *Théorie géométrique des polynômes Eulériens*, Lecture Notes in Math. 138, Springer-Verlag, Berlin (1970).
- [10] Marshall Hall, Jr., *The Theory of Groups*, Macmillan, New York (1959).
- [11] P. Hall, *The Eulerian functions of a group*, Quart. J. Math. 7 (1936), 134-151.
- [12] P. Hall, *A contribution to the theory of groups of prime-power orders*, Proc. London Math. Soc. (2) 36 (1933), 29-95.
- [13] P. A. MacMahon, *Combinatory Analysis*, Vols. 1-2, Cambridge (1916), reprinted by Chelsea (1960).
- [14] J. Riordan, *An Introduction to Combinatorial Analysis*, John Wiley & Sons, New York (1958).
- [15] G.-C. Rota, *On the foundations of combinatorial theory, I. Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie 2 (1964), 340-368.
- [16] R. P. Stanley, *Ordered structures and partitions*, Memoirs of the Amer. Math. Soc. 119 (1972).
- [17] R. P. Stanley, *Modular elements of geometric lattices*, Algebra Universalis 1 (1971), 214-217.
- [18] L. R. Wilcox, *Modularity in the theory of lattices*, Annals of Math. (2) 40 (1939), 490-505.
- [19] H. J. Zassenhaus, *The Theory of Groups* (second ed.), Chelsea, New York (1958).

*University of California
Berkeley, California
U.S.A.*