

5 Group actions on boolean algebras.

Let us begin by reviewing some facts from group theory. Suppose that X is an n -element set and that G is a group. We say that G *acts on* the set X if for every element π of G we associate a permutation (also denoted π) of X , such that for all $x \in X$ and $\pi, \sigma \in G$ we have

$$\pi(\sigma(x)) = (\pi\sigma)(x).$$

Thus [why?] an action of G on X is the same as a homomorphism $\varphi : G \rightarrow \mathfrak{S}_X$, where \mathfrak{S}_X denotes the symmetric group of all permutations of X . We sometimes write $\pi \cdot x$ instead of $\pi(x)$.

5.1 Example. (a) Let the real number α act on the xy -plane by rotation counterclockwise around the origin by an angle of α radians. It is easy to check that this defines an action of the group \mathbb{R} of real numbers (under addition) on the xy -plane.

(b) Now let $\alpha \in \mathbb{R}$ act by translation by a distance α to the right (i.e., adding $(\alpha, 0)$). This yields a completely different action of \mathbb{R} on the xy -plane.

(c) Let $X = \{a, b, c, d\}$ and $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. Let G act as follows:

$$\begin{aligned} (0, 1) \cdot a &= b, & (0, 1) \cdot b &= a, & (0, 1) \cdot c &= c, & (0, 1) \cdot d &= d \\ (1, 0) \cdot a &= a, & (1, 0) \cdot b &= b, & (1, 0) \cdot c &= d, & (1, 0) \cdot d &= c. \end{aligned}$$

The reader should check that this does indeed define an action. In particular, since $(1, 0)$ and $(0, 1)$ generate G , we don't need to define the action of $(0, 0)$ and $(1, 1)$ — they are uniquely determined.

(d) Let X and G be as in (c), but now define the action by

$$\begin{aligned} (0, 1) \cdot a &= b, & (0, 1) \cdot b &= a, & (0, 1) \cdot c &= d, & (0, 1) \cdot d &= c \\ (1, 0) \cdot a &= c, & (1, 0) \cdot b &= d, & (1, 0) \cdot c &= a, & (1, 0) \cdot d &= b. \end{aligned}$$

Again one can check that we have an action of $\mathbb{Z}_2 \times \mathbb{Z}_2$ on $\{a, b, c, d\}$.

Recall what is meant by an *orbit* of the action of a group G on a set X . Namely, we say that two elements x, y of X are *G -equivalent* if $\pi(x) = y$ for some $\pi \in G$. The relation of G -equivalence is an equivalence relation, and the equivalence classes are called orbits. Thus x and y are in the same orbit if $\pi(x) = y$ for some $\pi \in G$. The orbits form a *partition* of X , i.e., they are pairwise-disjoint, nonempty subsets of X whose union is X . The orbit containing x is denoted Gx ; this is sensible notation since Gx consists of all elements $\pi(x)$ where $\pi \in G$. Thus $Gx = Gy$ if and only if x and y are G -equivalent (i.e., in the same G -orbit). The set of all G -orbits is denoted X/G .

5.2 Example. (a) In Example 5.1(a), the orbits are circles with center $(0, 0)$ (including the degenerate circle whose only point is $(0, 0)$).

(b) In Example 5.1(b), the orbits are horizontal lines. Note that although in (a) and (b) the same group G acts on the same set X , the orbits are different.

(c) In Example 5.1(c), the orbits are $\{a, b\}$ and $\{c, d\}$.

(d) In Example 5.1(d), there is only one orbit $\{a, b, c, d\}$. Again we have a situation in which a group G acts on a set X in two different ways, with different orbits.

We wish to consider the situation where $X = B_n$, the boolean algebra of rank n (so $|B_n| = 2^n$). We begin by defining an *automorphism* of a poset P to be an isomorphism $\varphi : P \rightarrow P$. (This definition is exactly analogous to the definition of an automorphism of a group, ring, etc.) The set of all automorphisms of P forms a group, denoted $\text{Aut}(P)$ and called the *automorphism group* of P , under the operation of composition of functions (just as is the case for groups, rings, etc.)

Now consider the case $P = B_n$. Any permutation π of $\{1, \dots, n\}$ acts on B_n as follows: If $x = \{i_1, i_2, \dots, i_k\} \in B_n$, then

$$\pi(x) = \{\pi(i_1), \pi(i_2), \dots, \pi(i_k)\}. \quad (24)$$

This action of π on B_n is an automorphism [why?]; in particular, if $|x| = i$, then also $|\pi(x)| = i$. Equation (24) defines an action of the symmetric group

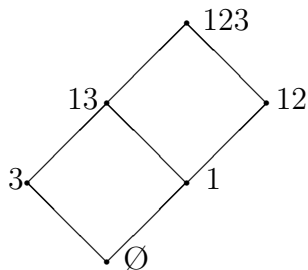
\mathfrak{S}_n of all permutations of $\{1, \dots, n\}$ on B_n [why?]. (In fact, it is not hard to show that *every* automorphism of B_n is of the form (24) for $\pi \in \mathfrak{S}_n$.) In particular, any subgroup G of \mathfrak{S}_n acts on B_n *via* (24) (where we restrict π to belong to G). In what follows this action is always meant.

5.3 Example. Let $n = 3$, and let G be the subgroup of \mathfrak{S}_3 with elements e and $(1, 2)$. Here e denotes the identity permutation, and (using disjoint cycle notation) $(1, 2)$ denotes the permutation which interchanges 1 and 2, and fixes 3. There are six orbits of G (acting on B_3). Writing e.g. 13 as short for $\{1, 3\}$, the six orbits are $\{\emptyset\}$, $\{1, 2\}$, $\{3\}$, $\{12\}$, $\{13, 23\}$, and $\{123\}$.

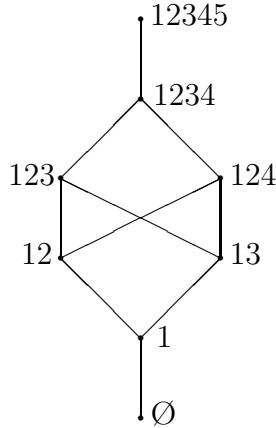
We now define the class of posets which will be of interest to us here. Later we will give some special cases of particular interest.

5.4 Definition. Let G be a subgroup of \mathfrak{S}_n . Define the *quotient poset* B_n/G as follows: The elements of B_n/G are the orbits of G . If \mathcal{O} and \mathcal{O}' are two orbits, then define $\mathcal{O} \leq \mathcal{O}'$ in B_n/G if there exist $x \in \mathcal{O}$ and $y \in \mathcal{O}'$ such that $x \leq y$ in B_n . (It's easy to check that this relation \leq is indeed a partial order.)

5.5 Example. (a) Let $n = 3$ and G be the group of order two generated by the cycle $(1, 2)$, as in Example 5.2. Then the Hasse diagram of B_3/G is shown below, where each element (orbit) is labeled by one of its elements.



(b) Let $n = 5$ and G be the group of order five generated by the cycle $(1, 2, 3, 4, 5)$. Then B_5/G has Hasse diagram



One simple property of a quotient poset B_n/G is the following.

5.6 Proposition. *The quotient poset B_n/G defined above is graded of rank n and rank-symmetric.*

Proof. We leave as an exercise the easy proof that B_n/G is graded of rank n , and that the rank of an element \mathcal{O} of B_n/G is just the rank in B_n of any of the elements x of \mathcal{O} . Thus the number of elements $p_i(B_n/G)$ of rank i is equal to the number of orbits $\mathcal{O} \in (B_n)_i/G$. If $x \in B_n$, then let \bar{x} denote the set-theoretic complement of x , i.e.,

$$\bar{x} = \{1, \dots, n\} - x = \{1 \leq i \leq n : i \notin x\}.$$

Then $\{x_1, \dots, x_j\}$ is an orbit of i -element subsets of $\{1, \dots, n\}$ if and only if $\{\bar{x}_1, \dots, \bar{x}_j\}$ is an orbit of $(n-i)$ -element subsets [why?]. Hence $|(B_n)_i/G| = |(B_n)_{n-i}/G|$, so B_n/G is rank-symmetric. \square

Let $\pi \in \mathfrak{S}_n$. We associate with π a linear transformation (still denoted π) $\pi : \mathbb{R}(B_n)_i \rightarrow \mathbb{R}(B_n)_i$ by the rule

$$\pi \left(\sum_{x \in (B_n)_i} c_x x \right) = \sum_{x \in (B_n)_i} c_x \pi(x),$$

where each c_x is a real number. (This defines an action of \mathfrak{S}_n , or of any subgroup G of \mathfrak{S}_n , on the vector space $\mathbb{R}(B_n)_i$.) The matrix of π with

respect to the basis $(B_n)_i$ is just a *permutation matrix*, i.e., a matrix with one 1 in every row and column, and 0's elsewhere. We will be interested in elements of $\mathbb{R}(B_n)_i$ which are fixed by every element of a subgroup G of \mathfrak{S}_n . The set of all such elements is denoted $\mathbb{R}(B_n)_i^G$, so

$$\mathbb{R}(B_n)_i^G = \{v \in \mathbb{R}(B_n)_i : \pi(v) = v \text{ for all } \pi \in G\}.$$

5.7 Lemma. *A basis for $\mathbb{R}(B_n)_i^G$ consists of the elements*

$$v_{\mathcal{O}} := \sum_{x \in \mathcal{O}} x,$$

where $\mathcal{O} \in (B_n)_i/G$, the set of G -orbits for the action of G on $(B_n)_i$.

Proof. First note that if \mathcal{O} is an orbit and $x \in \mathcal{O}$, then by definition of orbit we have $\pi(x) \in \mathcal{O}$ for all $\pi \in G$ (or all $\pi \in \mathfrak{S}_n$). Since π permutes the elements of $(B_n)_i$, it follows that π permutes the elements of \mathcal{O} . Thus $\pi(v_{\mathcal{O}}) = v_{\mathcal{O}}$, so $v_{\mathcal{O}} \in \mathbb{R}(B_n)_i^G$. It is clear that the $v_{\mathcal{O}}$'s are linearly independent since any $x \in (B_n)_i$ appears with nonzero coefficient in exactly one $v_{\mathcal{O}}$.

It remains to show that the $v_{\mathcal{O}}$'s span $\mathbb{R}(B_n)_i^G$, i.e., any $v = \sum_{x \in (B_n)_i} c_x x \in \mathbb{R}(B_n)_i^G$ can be written as a linear combination of $v_{\mathcal{O}}$'s. Given $x \in (B_n)_i$, let $G_x = \{\pi \in G : \pi(x) = x\}$, the *stabilizer* of x . We leave as an exercise the standard fact that $\pi(x) = \sigma(x)$ (where $\pi, \sigma \in G$) if and only if π and σ belong to the same left coset of G_x , i.e., $\pi G_x = \sigma G_x$. It follows that in the multiset of elements $\pi(x)$, where π ranges over all elements of G and x is fixed, every element y in the orbit Gx appears $|G_x|$ times, and no other elements appear. In other words,

$$\sum_{\pi \in G} \pi(x) = |G_x| \cdot v_{Gx}.$$

(Do not confuse the orbit Gx with the subgroup G_x !) Now apply π to v and sum on all $\pi \in G$. Since $\pi(v) = v$ (because $v \in \mathbb{R}(B_n)_i^G$), we get

$$\begin{aligned} |G| \cdot v &= \sum_{\pi \in G} \pi(v) \\ &= \sum_{\pi \in G} \left(\sum_{x \in (B_n)_i} c_x \pi(x) \right) \end{aligned}$$

$$\begin{aligned}
&= \sum_{x \in (B_n)_i} c_x \left(\sum_{\pi \in G} \pi(x) \right) \\
&= \sum_{x \in (B_n)_i} c_x \cdot |G_x| \cdot v_{Gx}.
\end{aligned}$$

Dividing by $|G|$ expresses v as a linear combination of the elements v_{Gx} (or $v_{\mathcal{O}}$), as desired. \square

Now let us consider the effect of applying the order-raising operator U_i to an element v of $\mathbb{R}(B_n)_i^G$.

5.8 Lemma. *If $v \in \mathbb{R}(B_n)_i^G$, then $U_i(v) \in \mathbb{R}(B_n)_{i+1}^G$.*

Proof. Note that since $\pi \in G$ is an automorphism of B_n , we have $x < y$ in B_n if and only if $\pi(x) < \pi(y)$ in B_n . It follows [why?] that if $x \in (B_n)_i$ then

$$U_i(\pi(x)) = \pi(U_i(x)).$$

Since U_i and π are linear transformations, it follows by linearity that $U_i\pi(u) = \pi U_i(u)$ for all $u \in \mathbb{R}(B_n)_i$. (In other words, $U_i\pi = \pi U_i$.) Then

$$\begin{aligned}
\pi(U_i(v)) &= U_i(\pi(v)) \\
&= U_i(v),
\end{aligned}$$

so $U_i(v) \in \mathbb{R}(B_n)_{i+1}^G$, as desired. \square

We come to the main result of this section, and indeed our main result on the Sperner property.

5.9 Theorem. *Let G be a subgroup of \mathfrak{S}_n . Then the quotient poset B_n/G is graded of rank n , rank-symmetric, rank-unimodal, and Sperner.*

Proof. Let $P = B_n/G$. We have already seen in Proposition 5.6 that P is graded of rank n and rank-symmetric. We want to define order-raising operators $\hat{U}_i : \mathbb{R}P_i \rightarrow \mathbb{R}P_{i+1}$ and order-lowering operators $\hat{D}_i : \mathbb{R}P_i \rightarrow \mathbb{R}P_{i-1}$. Let us first consider just \hat{U}_i . The idea is to identify the basis element $v_{\mathcal{O}}$ of $\mathbb{R}B_n^G$ with the basis element \mathcal{O} of $\mathbb{R}P$, and to let $\hat{U}_i : \mathbb{R}P_i \rightarrow \mathbb{R}P_{i+1}$ correspond to the usual order-raising operator $U_i : \mathbb{R}(B_n)_i \rightarrow \mathbb{R}(B_n)_{i+1}$. More precisely,

suppose that the order-raising operator U_i for B_n given by (18) satisfies

$$U_i(v_{\mathcal{O}}) = \sum_{\mathcal{O}' \in (B_n)_{i+1}/G} c_{\mathcal{O}, \mathcal{O}'} v_{\mathcal{O}'}, \quad (25)$$

where $\mathcal{O} \in (B_n)_i/G$. (Note that by Lemma 5.8, $U_i(v_{\mathcal{O}})$ does indeed have the form given by (25).) Then define the linear operator $\hat{U}_i : \mathbb{R}((B_n)_i/G) \rightarrow \mathbb{R}((B_n)_i/G)$ by

$$\hat{U}_i(\mathcal{O}) = \sum_{\mathcal{O}' \in (B_n)_{i+1}/G} c_{\mathcal{O}, \mathcal{O}'} \mathcal{O}'.$$

We claim that \hat{U}_i is order-raising. We need to show that if $c_{\mathcal{O}, \mathcal{O}'} \neq 0$, then $\mathcal{O}' > \mathcal{O}$ in B_n/G . Since $v_{\mathcal{O}'} = \sum_{x' \in \mathcal{O}'} x'$, the only way $c_{\mathcal{O}, \mathcal{O}'} \neq 0$ in (25) is for some $x' \in \mathcal{O}'$ to satisfy $x' > x$ for some $x \in \mathcal{O}$. But this is just what it means for $\mathcal{O}' > \mathcal{O}$, so \hat{U}_i is order-raising.

Now comes the heart of the argument. We want to show that \hat{U}_i is one-to-one for $i < n/2$. Now by Theorem 4.7, U_i is one-to-one for $i < n/2$. Thus the restriction of U_i to the subspace $\mathbb{R}(B_n)_i^G$ is one-to-one. (The restriction of a one-to-one function is always one-to-one.) But U_i and \hat{U}_i are exactly the same transformation, except for the names of the basis elements on which they act. Thus \hat{U}_i is also one-to-one for $i < n/2$.

An exactly analogous argument can be applied to D_i instead of U_i . We obtain one-to-one order-lowering operators $\hat{D}_i : \mathbb{R}(B_n)_i^G \rightarrow \mathbb{R}(B_n)_{i-1}^G$ for $i > n/2$. It follows from Proposition 4.4, Lemma 4.5, and (20) that B_n/G is rank-unimodal and Sperner, completing the proof. \square

We will consider two interesting applications of Theorem 5.9. For our first application, we let $n = \binom{m}{2}$ for some $m \geq 1$, and let $M = \{1, \dots, m\}$. Let $X = \binom{M}{2}$, the set of all two-element subsets of M . Think of the elements of X as (possible) edges of a graph with vertex set M . If B_X is the boolean algebra of all subsets of X (so B_X and B_n are isomorphic), then an element x of B_X is a collection of edges on the vertex set M , in other words, just a simple graph on M . Define a subgroup G of \mathfrak{S}_X as follows: Informally, G consists of all permutations of the edges $\binom{M}{2}$ that are induced from permutations of the vertices M . More precisely, if $\pi \in \mathfrak{S}_m$, then define $\hat{\pi} \in \mathfrak{S}_X$ by $\hat{\pi}(\{i, j\}) = \{\pi(i), \pi(j)\}$. Thus G is isomorphic to \mathfrak{S}_m .

When are two graphs $x, y \in B_X$ in the same orbit of the action of G on B_X ? Since the elements of G just permute vertices, we see that x and y are in the same orbit if we can obtain x from y by permuting vertices. This is just what it means for two simple graphs x and y to be *isomorphic* — they are the same graph except for the names of the vertices (thinking of edges as pairs of vertices). Thus the elements of B_X/G are *isomorphism classes* of simple graphs on the vertex set M . In particular, $\#(B_X/G)$ is the number of nonisomorphic m -vertex simple graphs, and $\#((B_X/G)_i)$ is the number of nonisomorphic such graphs with i edges. We have $x \leq y$ in B_X/G if there is some way of labelling the vertices of x and y so that every edge of x is an edge of y . Equivalently, some *spanning subgraph* of y (i.e., a subgraph of y with all the vertices of y) is isomorphic to x . Hence by Theorem 5.9 there follows the following result, which is by no means obvious and has no known non-algebraic proof.

5.10 Theorem. (a) *Fix $m \geq 1$. Let p_i be the number of nonisomorphic simple graphs with m vertices and i edges. Then the sequence $p_0, p_1, \dots, p_{\binom{m}{2}}$ is symmetric and unimodal.*

(b) *Let T be a collection of nonisomorphic simple graphs with m vertices such that no element of T is isomorphic to a subset of another element of T . Then $|T|$ is maximized by taking T to consist of all nonisomorphic simple graphs with $\lfloor \frac{1}{2} \binom{m}{2} \rfloor$ edges.*

Our second example of the use of Theorem 5.9 is somewhat more subtle and will be the topic of the next section.

Digression: edge reconstruction. Much work has been done on “reconstruction problems,” that is, trying to reconstruct a mathematical structure such as a graph from some of its substructures. The most famous of such problems is *vertex reconstruction*: given a simple graph G on n vertices v_1, \dots, v_p , let G_i be the subgraph obtained by deleting vertex v_i (and all incident edges). Given the multiset $\{G_1, \dots, G_p\}$ of vertex-deleted subgraphs, can G be uniquely reconstructed? It is important to realize that the vertices are *unlabelled*, so given G_i we don’t know for any j which vertex is v_j . The famous *vertex reconstruction conjecture* (still open) states that for $n \geq 3$ any graph G can be reconstructed from the multiset $\{G_1, \dots, G_p\}$.

Here we will be concerned with *edge* reconstruction, another famous open problem. Given a simple graph G with edges e_1, \dots, e_q , let $H_i = G - e_i$, the graph obtained from G by removing the edge e_i .

Edge Reconstruction Conjecture. A simple graph G can be uniquely reconstructed from its number of vertices and the multiset $\{H_1, \dots, H_q\}$ of edge-deleted subgraphs.

NOTE. As in the case of vertex-reconstruction, the subgraphs H_i are unlabelled. The reason for including the number of vertices is that for a graph with no edges, we have $\{H_1, \dots, H_q\} = \emptyset$, so we need to specify the number of vertices to obtain G .

NOTE. It can be shown that if G can be vertex-reconstructed, then G can be edge reconstructed. Hence the vertex-reconstruction conjecture implies the edge-reconstruction conjecture.

The techniques developed above to analyze group actions on boolean algebra can be used to prove a special case of the edge-reconstruction conjecture. Note that a simple graph with p vertices has at most $\binom{p}{2}$ edges.

5.11 Theorem. Let G be a simple graph with p vertices and $q > \frac{1}{2}\binom{p}{2}$ edges. Then G is edge-reconstructible.

Proof. Let P_i be the set of all simple graphs with i edges on the vertex set $[p]$, so $\#P_i = \binom{p}{i}$. Let $\mathbb{R}P_i$ denote the real vector space with basis P_i . Define a linear transformation $\psi_i : \mathbb{R}P_i \rightarrow \mathbb{R}P_{i-1}$ by

$$\psi_i(\Gamma) = \Gamma_1 + \dots + \Gamma_i,$$

where $\Gamma_1, \dots, \Gamma_i$ are the (labelled) graphs obtained from Γ by deleting a single edge. By Theorem 4.7, ψ_i is injective for $i > \frac{1}{2}\binom{p}{2}$. (Think of ψ_i as adding edges to the *complement* of Γ , i.e., the graph with vertex set $[p]$ and edge set $\binom{[p]}{2} - E(\Gamma)$.)

The symmetric group \mathfrak{S}_p acts on P_q by permuting the vertices, and hence acts on $\mathbb{R}P_q$, the real vector space with basis P_q . A basis for the fixed space $(\mathbb{R}P_q)^{\mathfrak{S}_p}$ consists of the distinct sums $\tilde{\Gamma} = \sum_{\pi \in \mathfrak{S}_p} \pi(\Gamma)$, where $\Gamma \in P_q$. We

may identify $\tilde{\Gamma}$ with the *unlabelled* graph isomorphic to Γ , since $\tilde{\Gamma} = \tilde{\Gamma}'$ if and only if Γ and Γ' are isomorphic. Just as in the proof of Theorem 5.9, when we restrict ψ_q to $(\mathbb{R}P_q)^{\mathfrak{S}_p}$ for $q > \frac{1}{2}\binom{p}{2}$ we obtain an injection $\psi_q : (\mathbb{R}P_q)^{\mathfrak{S}_p} \rightarrow (\mathbb{R}P_{q-1})^{\mathfrak{S}_p}$. In particular, for nonisomorphic unlabelled graphs $\tilde{\Gamma}, \tilde{\Gamma}'$ with p vertices, we have

$$\tilde{\Gamma}_1 + \cdots + \tilde{\Gamma}_q = \psi_q(\tilde{\Gamma}) \neq \psi_q(\tilde{\Gamma}') = \tilde{\Gamma}'_1 + \cdots + \tilde{\Gamma}'_q.$$

Hence the unlabelled graphs $\tilde{\Gamma}_1, \dots, \tilde{\Gamma}_q$ determine $\tilde{\Gamma}$, as desired. \square

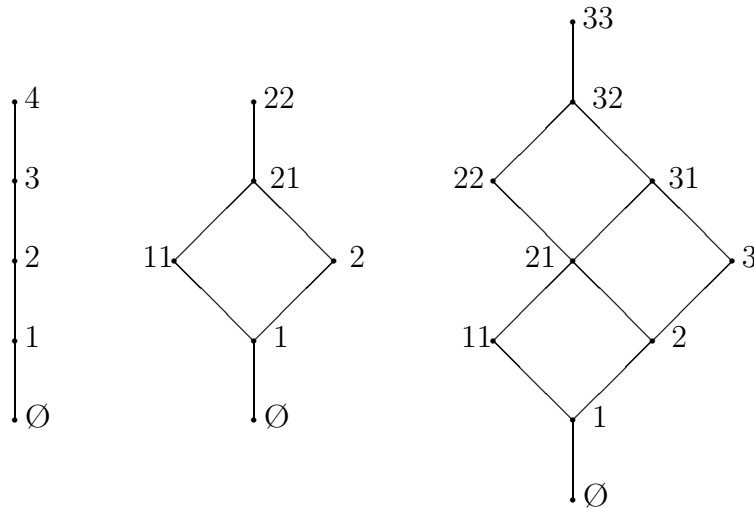
Theorem 5.11 was first proved by L. Lovász using the Principle of Inclusion-Exclusion. The proof given above is due to R. Stanley. W. Müller found an improvement of Lovász's argument, showing that a graph with p vertices and $q > p \log p$ edges is edge-reconstructible. I. Krasikov and Y. Roditty later found an improvement of our proof of Theorem 5.11 that gave another proof of Müller's result.

6 Young diagrams and q -binomial coefficients.

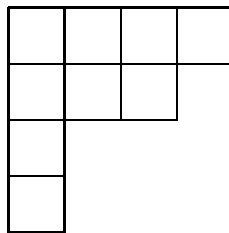
A *partition* λ of an integer $n \geq 0$ is a sequence $\lambda = (\lambda_1, \lambda_2, \dots)$ of integers $\lambda_i \geq 0$ satisfying $\lambda_1 \geq \lambda_2 \geq \dots$ and $\sum_{i \geq 1} \lambda_i = n$. Thus all but finitely many λ_i are equal to 0. Each $\lambda_i > 0$ is called a *part* of λ . We sometimes suppress 0's from the notation for λ , e.g., $(5, 2, 2, 1)$, $(5, 2, 2, 1, 0, 0, 0)$, and $(5, 2, 2, 1, 0, 0, \dots)$ all represent the same partition λ (of 10, with four parts). If λ is a partition of n , then we denote this by $\lambda \vdash n$ or $|\lambda| = n$.

6.1 Example. There are seven partitions of 5, namely (writing e.g. 221 as short for $(2, 2, 1)$): 5, 41, 32, 311, 221, 2111, and 11111.

The subject of partitions of integers has been extensively developed, and we will only be concerned here with a small part related to our previous discussion. Given positive integers m and n , let $L(m, n)$ denote the set of all partitions with at most m parts and with largest part at most n . For instance, $L(2, 3) = \{\emptyset, 1, 2, 3, 11, 21, 31, 22, 32, 33\}$. (Note that we are denoting by \emptyset the unique partition $(0, 0, \dots)$ with no parts.) If $\lambda = (\lambda_1, \lambda_2, \dots)$ and $\mu = (\mu_1, \mu_2, \dots)$ are partitions, then define $\lambda \leq \mu$ if $\lambda_i \leq \mu_i$ for all i . This makes the set of all partitions into a very interesting poset, denoted Y and called *Young's lattice* (named after the British mathematician Alfred Young, 1873–1940). (It is called “Young's lattice” rather than “Young's poset” because it turns out to have certain properties which define a *lattice*. However, these properties are irrelevant to us here, so we will not bother to define the notion of a lattice.) We will be looking at some properties of Y in Section 8. The partial ordering on Y , when restricted to $L(m, n)$, makes $L(m, n)$ into a poset which also has some fascinating properties. The diagrams below show $L(1, 4)$, $L(2, 2)$, and $L(2, 3)$.

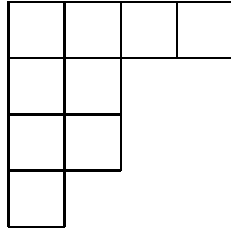


There is a nice geometric way of viewing partitions and the poset $L(m, n)$. The *Young diagram* (sometimes just called the *diagram*) of a partition λ is a left-justified array of squares, with λ_i squares in the i th row. For instance, the Young diagram of $(4, 3, 1, 1)$ looks like:



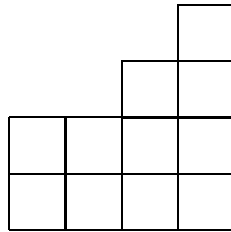
If dots are used instead of boxes, then the resulting diagram is called a *Ferrers diagram*. The advantage of Young diagrams over Ferrers diagrams is that we can put numbers in the boxes of a Young diagram, which we will do in Section 7. Observe that $L(m, n)$ is simply the set of Young diagrams D fitting in an $m \times n$ rectangle (where the upper-left (northwest) corner of D is the same as the northwest corner of the rectangle), ordered by inclusion. *We will always assume that when a Young diagram D is contained in a rectangle R , the northwest corners agree.* It is also clear from the Young diagram point of view that $L(m, n)$ and $L(n, m)$ are isomorphic partially ordered sets, the isomorphism being given by transposing the diagram (i.e., interchanging rows

and columns). If λ has Young diagram D , then the partition whose diagram is D^t (the transpose of D) is called the *conjugate* of λ and is denoted λ' . For instance, $(4, 3, 1, 1)' = (4, 2, 2, 1)$, with diagram



6.2 Proposition. $L(m, n)$ is graded of rank mn and rank-symmetric. The rank of a partition λ is just $|\lambda|$ (the sum of the parts of λ or the number of squares in its Young diagram).

Proof. As in the proof of Proposition 5.6, we leave to the reader everything except rank-symmetry. To show rank-symmetry, consider the complement $\bar{\lambda}$ of λ in an $m \times n$ rectangle R , i.e., all the squares of R except for λ . (Note that $\bar{\lambda}$ depends on m and n , and not just λ .) For instance, in $L(5, 4)$, the complement of $(4, 3, 1, 1)$ looks like



If we rotate the diagram of $\bar{\lambda}$ by 180° then we obtain the diagram of a partition $\tilde{\lambda} \in L(m, n)$ satisfying $|\lambda| + |\tilde{\lambda}| = mn$. This correspondence between λ and $\tilde{\lambda}$ shows that $L(m, n)$ is rank-symmetric. \square

Our main goal in this section is to show that $L(m, n)$ is rank-unimodal and Sperner. Let us write $p_i(m, n)$ as short for $p_i(L(m, n))$, the number of elements of $L(m, n)$ of rank i . Equivalently, $p_i(m, n)$ is the number of partitions of i with largest part at most n and with at most m parts, or, in

other words, the number of distinct Young diagrams with i squares which fit inside an $m \times n$ rectangle (with the same northwest corner, as explained previously). Though not really necessary for this goal, it is nonetheless interesting to obtain some information on these numbers $p_i(m, n)$. First let us consider the total number $|L(m, n)|$ of elements in $L(m, n)$.

6.3 Proposition. *We have $|L(m, n)| = \binom{m+n}{m}$.*

Proof. We will give an elegant combinatorial proof, based on the fact that $\binom{m+n}{m}$ is equal to the number of sequences a_1, a_2, \dots, a_{m+n} , where each a_j is either N or E , and there are m N 's (and hence n E 's) in all. We will associate a Young diagram D contained in an $m \times n$ rectangle R with such a sequence as follows. Begin at the lower left-hand corner of R , and trace out the southeast boundary of D , ending at the upper right-hand corner of R . This is done by taking a sequence of unit steps (where each square of R is one unit in length), each step either north or east. Record the sequence of steps, using N for a step to the north and E for a step to the east.

Example. Let $m = 5$, $n = 6$, $\lambda = (4, 3, 1, 1)$. Then R and D are given by:

×	×	×	×		
×	×	×			
×					
×					

The corresponding sequence of N 's and E 's is $NENNEENENEE$.

It is easy to see (left to the reader) that the above correspondence gives a bijection between Young diagrams D fitting in an $m \times n$ rectangle R , and sequences of m N 's and n E 's. Hence the number of diagrams is equal to $\binom{m+n}{m}$, the number of sequences. \square

We now consider how many elements of $L(m, n)$ have rank i . To this end,

let q be an indeterminate; and given $j \geq 1$ define $[j] = 1 + q + q^2 + \cdots + q^{j-1}$. Thus $[1] = 1$, $[2] = 1 + q$, $[3] = 1 + q + q^2$, etc. Note that $[j]$ is a polynomial in q whose value at $q = 1$ is just j (denoted $[j]_{q=1} = j$). Next define $[j]! = [1][2] \cdots [j]$ for $j \geq 1$, and set $[0]! = 1$. Thus $[1]! = 1$, $[2]! = 1 + q$, $[3]! = (1 + q)(1 + q + q^2) = 1 + 2q + 2q^2 + q^3$, etc., and $[j]!_{q=1} = j!$. Finally define for $k \geq j \geq 0$,

$$\begin{bmatrix} k \\ j \end{bmatrix} = \frac{[k]!}{[j]![k-j]!}.$$

The expression $\begin{bmatrix} k \\ j \end{bmatrix}$ is called a q -binomial coefficient (or *Gaussian coefficient*). Since $[r]!_{q=1} = r!$, it is clear that

$$\begin{bmatrix} k \\ j \end{bmatrix}_{q=1} = \binom{k}{j}.$$

One sometimes says that $\begin{bmatrix} k \\ j \end{bmatrix}$ is a “ q -analogue” of the binomial coefficient $\binom{k}{j}$.

6.4 Example. We have $\begin{bmatrix} k \\ j \end{bmatrix} = \begin{bmatrix} k \\ k-j \end{bmatrix}$ [why?]. Moreover,

$$\begin{bmatrix} k \\ 0 \end{bmatrix} = \begin{bmatrix} k \\ k \end{bmatrix} = 1$$

$$\begin{bmatrix} k \\ 1 \end{bmatrix} = \begin{bmatrix} k \\ k-1 \end{bmatrix} = [k] = 1 + q + q^2 + \cdots + q^{k-1}$$

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix} = \frac{[4][3][2][1]}{[2][1][2][1]} = 1 + q + 2q^2 + q^3 + q^4$$

$$\begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 3 \end{bmatrix} = 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6.$$

In the above example, $\begin{bmatrix} k \\ j \end{bmatrix}$ was always a polynomial in q (and with non-negative integer coefficients). It is not obvious that this is always the case, but it will follow easily from the following lemma.

6.5 Lemma. *We have*

$$\begin{bmatrix} k \\ j \end{bmatrix} = \begin{bmatrix} k-1 \\ j \end{bmatrix} + q^{k-j} \begin{bmatrix} k-1 \\ j-1 \end{bmatrix}, \quad (26)$$

whenever $k \geq 1$, with the “initial conditions” $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$, $\begin{bmatrix} k \\ j \end{bmatrix} = 0$ if $j < 0$ or $j > k$ (the same initial conditions satisfied by the binomial coefficients $\binom{k}{j}$).

Proof. This is a straightforward computation. Specifically, we have

$$\begin{aligned}
\begin{bmatrix} k-1 \\ j \end{bmatrix} + q^{k-j} \begin{bmatrix} k-1 \\ j-1 \end{bmatrix} &= \frac{[k-1]!}{[j]![k-1-j]!} + q^{k-j} \frac{[k-1]!}{[j-1]![k-j]!} \\
&= \frac{[k-1]!}{[j-1]![k-1-j]!} \left(\frac{1}{[j]} + \frac{q^{k-j}}{[k-j]} \right) \\
&= \frac{[k-1]!}{[j-1]![k-1-j]!} \frac{[k-j] + q^{k-j}[j]}{[j][k-j]} \\
&= \frac{[k-1]!}{[j-1]![k-1-j]!} \frac{[k]}{[j][k-j]} \\
&= \begin{bmatrix} k \\ j \end{bmatrix}. \quad \square
\end{aligned}$$

Note that if we put $q = 1$ in (26) we obtain the well-known formula

$$\binom{k}{j} = \binom{k-1}{j} + \binom{k-1}{j-1},$$

which is just the recurrence defining Pascal’s triangle. Thus equation (26) may be regarded as a q -analogue of the Pascal triangle recurrence.

We can regard equation (26) as a recurrence relation for the q -binomial coefficients. Given the initial conditions of Lemma 6.5, we can use (26) inductively to compute $\begin{bmatrix} k \\ j \end{bmatrix}$ for any k and j . From this it is obvious by induction that the q -binomial coefficient $\begin{bmatrix} k \\ j \end{bmatrix}$ is a polynomial in q with nonnegative integer coefficients. The following theorem gives an even stronger result, namely, an explicit combinatorial interpretation of the coefficients.

6.6 Theorem. *Let $p_i(m, n)$ denote the number of elements of $L(m, n)$ of rank i . Then*

$$\sum_{i \geq 0} p_i(m, n) q^i = \begin{bmatrix} m+n \\ m \end{bmatrix}. \quad (27)$$

(NOTE. The sum on the left-hand side is really a *finite* sum, since $p_i(m, n) = 0$ if $i > mn$.)

Proof. Let $P(m, n)$ denote the left-hand side of (27). We will show that

$$P(0, 0) = 1, \text{ and } P(m, n) = 0 \text{ if } m < 0 \text{ or } n < 0 \quad (28)$$

$$P(m, n) = P(m, n - 1) + q^n P(m - 1, n). \quad (29)$$

Note that equations (28) and (29) completely determine $P(m, n)$. On the other hand, substituting $k = m + n$ and $j = m$ in (26) shows that $\left[\begin{smallmatrix} m+n \\ m \end{smallmatrix} \right]$ also satisfies (29). Moreover, the initial conditions of Lemma 6.5 show that $\left[\begin{smallmatrix} m+n \\ m \end{smallmatrix} \right]$ also satisfies (28). Hence (28) and (29) imply that $P(m, n) = \left[\begin{smallmatrix} m+n \\ m \end{smallmatrix} \right]$, so to complete the proof we need only establish (28) and (29).

Equation (28) is clear, since $L(0, n)$ consists of a single point (the empty partition \emptyset), so $\sum_{i \geq 0} p_i(0, n)q^i = 1$; while $L(m, n)$ is empty (or undefined, if you prefer) if $m < 0$ or $n < 0$,

The crux of the proof is to show (29). Taking the coefficient of q^i of both sides of (29), we see [why?] that (29) is equivalent to

$$p_i(m, n) = p_i(m, n - 1) + p_{i-n}(m - 1, n). \quad (30)$$

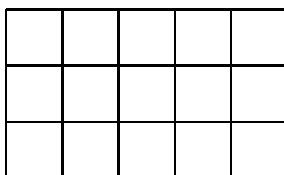
Consider a partition $\lambda \vdash i$ whose Young diagram D fits in an $m \times n$ rectangle R . If D does not contain the upper right-hand corner of R , then D fits in an $m \times (n - 1)$ rectangle, so there are $p_i(m, n - 1)$ such partitions λ . If on the other hand D does contain the upper right-hand corner of R , then D contains the whole first row of R . When we remove the first row of R , we have left a Young diagram of size $i - n$ which fits in an $(m - 1) \times n$ rectangle. Hence there are $p_{i-n}(m - 1, n)$ such λ , and the proof follows [why?]. \square

Note that if we set $q = 1$ in (27), then the left-hand side becomes $|L(m, n)|$ and the right-hand side $\binom{m+n}{m}$, agreeing with Proposition 6.3.

NOTE: There is another well-known interpretation of $\left[\begin{smallmatrix} k \\ j \end{smallmatrix} \right]$, this time not of its coefficients (regarded as a polynomial in q), but rather at its *values* for certain q . Namely, suppose q is the power of a prime. Recall that there is a field \mathbb{F}_q (unique up to isomorphism) with q elements. Then one can show

that $\begin{bmatrix} k \\ j \end{bmatrix}$ is equal to the number of j -dimensional subspaces of a k -dimensional vector space over the field \mathbb{F}_q . We will not discuss the proof here since it is not relevant for our purposes.

As the reader may have guessed by now, the poset $L(m, n)$ is isomorphic to a quotient poset B_s/G for a suitable integer $s > 0$ and finite group G acting on B_s . Actually, it is clear that we must have $s = mn$ since $L(m, n)$ has rank mn and in general B_s/G has rank s . What is not so clear is the right choice of G . To this end, let $R = R_{mn}$ denote an $m \times n$ rectangle of squares. For instance, R_{35} is given by the 15 squares of the diagram



We now define the group $G = G_{mn}$ as follows. It is a subgroup of the group \mathfrak{S}_R of all permutations of the squares of R . A permutation π in G is allowed to permute the elements in each row of R in any way, and then to permute the rows themselves of R in any way. The elements of each row can be permuted in $n!$ ways, so since there are m rows there are a total of $n!^m$ permutations preserving the rows. Then the m rows can be permuted in $m!$ ways, so it follows that the order of G_{mn} is given by $m!n!^m$. (The group G_{mn} is called the *wreath product* of \mathfrak{S}_n and \mathfrak{S}_m , denoted $\mathfrak{S}_n \wr \mathfrak{S}_m$ or $\mathfrak{S}_n \text{ wr } \mathfrak{S}_m$. However, we will not discuss the general theory of wreath products here.)

6.7 Example. Suppose $m = 4$ and $n = 5$, with the boxes of X labelled as follows.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

Then a typical permutation π in $G(4, 5)$ looks like

16	20	17	19	18
4	1	5	2	3
12	13	15	14	11
7	9	6	10	8

i.e., $\pi(16) = 1$, $\pi(20) = 2$, etc.

We have just defined a group G_{mn} of permutations of the set R_{mn} of squares of an $m \times n$ rectangle. Hence G_{mn} acts on the boolean algebra B_R of all subsets of the set R . The next lemma describes the orbits of this action.

6.8 Lemma. *Every orbit \mathcal{O} of the action of G_{mn} on B_R contains exactly one Young diagram D (i.e., exactly one subset $D \subseteq R$ such that D is left-justified, and if λ_i is the number of elements of D in row i of R , then $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_m$).*

Proof. Let S be a subset of R , and suppose that S has α_i elements in row i . If $\pi \in G_{mn}$ and $\pi \cdot S$ has β_i elements in row i , then β_1, \dots, β_m is just some permutation of $\alpha_1, \dots, \alpha_m$ [why?]. There is a unique permutation $\lambda_1, \dots, \lambda_m$ of $\alpha_1, \dots, \alpha_m$ satisfying $\lambda_1 \geq \dots \geq \lambda_m$, so the only possible Young diagram D in the orbit $\pi \cdot S$ is the one of shape $\lambda = (\lambda_1, \dots, \lambda_m)$. It's easy to see that the Young diagram D_λ of shape λ is indeed in the orbit $\pi \cdot S$. For by permuting the elements in the rows of R we can left-justify the rows of S , and then by permuting the rows of R themselves we can arrange the row sizes of S to be in weakly decreasing order. Thus we obtain the Young diagram D_λ as claimed. \square

We are now ready for the main result of this section.

6.9 Theorem. *The quotient poset $B_{R_{mn}}/G_{mn}$ is isomorphic to $L(m, n)$.*

Proof. Each element of B_R/G_{mn} contains a unique Young diagram D_λ by Lemma 6.8. Moreover, two different orbits cannot contain the same Young diagram D since orbits are disjoint. Thus the map $\varphi : B_R/G_{mn} \rightarrow L(m, n)$

defined by $\varphi(D_\lambda) = \lambda$ is a bijection (one-to-one and onto). We claim that in fact φ is an isomorphism of partially ordered sets. We need to show the following: Let \mathcal{O} and \mathcal{O}^* be orbits of G_{mn} (i.e., elements of B_R/G_{mn}). Let D_λ and D_{λ^*} be the unique Young diagrams in \mathcal{O} and \mathcal{O}^* , respectively. Then there exist $D \in \mathcal{O}$ and $D^* \in \mathcal{O}^*$ satisfying $D \subseteq D^*$ if and only if $\lambda \leq \lambda^*$ in $L(m, n)$.

The “if” part of the previous sentence is clear, for if $\lambda \leq \lambda^*$ then $D_\lambda \subseteq D_{\lambda^*}$. So assume there exist $D \in \mathcal{O}$ and $D^* \in \mathcal{O}^*$ satisfying $D \subseteq D^*$. The lengths of the rows of D , written in decreasing order, are $\lambda_1, \dots, \lambda_m$, and similarly for D^* . Since each row of D is contained in a row of D^* , it follows that for each $1 \leq j \leq m$, D^* has at least j rows of size at least λ_j . Thus the length λ_j^* of the j th largest row of D^* is at least as large as λ_j . In other words, $\lambda_j \leq \lambda_j^*$, as was to be proved. \square

Combining the previous theorem with Theorem 5.9 yields:

6.10 Corollary. *The posets $L(m, n)$ are rank-symmetric, rank-unimodal, and Sperner.*

Note that the rank-symmetry and rank-unimodality of $L(m, n)$ can be rephrased as follows: The q -binomial coefficient $\begin{bmatrix} m+n \\ m \end{bmatrix}$ has symmetric and unimodal coefficients. While rank-symmetry is easy to prove (see Proposition 6.2), the unimodality of the coefficients of $\begin{bmatrix} m+n \\ m \end{bmatrix}$ is by no means apparent. It was first proved by J. Sylvester in 1878 by a proof similar to the one above, though stated in the language of the invariant theory of binary forms. For a long time it was an open problem to find a combinatorial proof that the coefficients of $\begin{bmatrix} m+n \\ m \end{bmatrix}$ are unimodal. Such a proof would give an explicit injection (one-to-one function) $\mu : L(m, n)_i \rightarrow L(m, n)_{i+1}$ for $i < \frac{1}{2}mn$. (One difficulty in finding such maps μ is to make use of the hypothesis that $i < \frac{1}{2}mn$.) Finally around 1989 such a proof was found by Kathy O’Hara. However, O’Hara’s proof has the defect that the maps μ are not order-matchings. Thus her proof does not prove that $L(m, n)$ is Sperner, but only that it’s rank-unimodal. It is an outstanding open problem in algebraic combinatorics to find an explicit order-matching $\mu : L(m, n)_i \rightarrow L(m, n)_{i+1}$ for $i < \frac{1}{2}mn$.

Note that the Sperner property of $L(m, n)$ (together with the fact that the

largest level is in the middle) can be stated in the following simple terms: The largest possible collection \mathcal{C} of Young diagrams fitting in an $m \times n$ rectangle such that no diagram in \mathcal{C} is contained in another diagram in \mathcal{C} is obtained by taking all the diagrams of size $\frac{1}{2}mn$. Although the statement of this fact requires almost no mathematics to understand, there is no known proof that doesn't use algebraic machinery. (The several known algebraic proofs are all closely related, and the one we have given is the simplest.) Corollary 6.10 is a good example of the efficacy of algebraic combinatorics.

An application to number theory. There is an interesting application of Corollary 6.10 to a number-theoretic problem. Fix a positive integer k . For a finite subset S of $\mathbb{R}^+ = \{\alpha \in \mathbb{R} : \alpha > 0\}$, and for a real number $\alpha > 0$, define

$$f_k(S, \alpha) = \# \left\{ T \in \binom{S}{k} : \sum_{t \in T} t = \alpha \right\}$$

In other words, $f_k(S, \alpha)$ is the number of k -element subsets of S whose elements sum to α . For instance, $f_3(\{1, 3, 4, 6, 7\}, 11) = 2$, since $1 + 3 + 7 = 1 + 4 + 6 = 11$.

Given positive integers $k < n$, our object is to maximize $f_k(S, \alpha)$ subject to the condition that $\#S = n$. We are free to choose both S and α , but k and n are fixed. Call this maximum value $h_k(n)$. Thus

$$h_k(n) = \max_{\substack{\alpha \in \mathbb{R}^+ \\ S \subset \mathbb{R}^+ \\ \#S = n}} f_k(S, \alpha).$$

What sort of behavior can we expect of the maximizing set S ? If the elements of S are “spread out,” say $S = \{1, 2, 4, 8, \dots, 2^{n-1}\}$, then all the subset sums of S are distinct. Hence for any $\alpha \in \mathbb{R}^+$ we have $f_k(S, \alpha) = 0$ or 1. Similarly, if the elements of S are “unrelated” (e.g., linearly independent over the rationals, such as $S = \{1, \sqrt{2}, \sqrt{3}, e, \pi\}$), then again all subset sums are distinct and $f_k(S, \alpha) = 0$ or 1. These considerations make it plausible that we should take $S = [n] = \{1, 2, \dots, n\}$ and then choose α appropriately. In other words, we are led to the conjecture that for any $S \in \binom{\mathbb{R}^+}{n}$ and $\alpha \in \mathbb{R}^+$, we have

$$f_k(S, \alpha) \leq f_k([n], \beta), \tag{31}$$

for some $\beta \in \mathbb{R}^+$ to be determined.

First let us evaluate $f_k([n], \alpha)$ for any α . This will enable us to determine the value of β in (31). Let $S = \{i_1, \dots, i_k\} \subseteq [n]$ with

$$1 \leq i_1 < i_2 < \dots < i_k \leq n, \quad i_1 + \dots + i_k = \alpha. \quad (32)$$

Let $j_r = i_r - r$. Then (since $1 + 2 + \dots + k = \binom{k+1}{2}$)

$$n - k \geq j_k \geq j_{k-1} \geq \dots \geq j_1 \geq 0, \quad j_1 + \dots + j_k = \alpha - \binom{k+1}{2}. \quad (33)$$

Conversely, given j_1, \dots, j_k satisfying (33) we can recover i_1, \dots, i_k satisfying (32). Hence $f_k([n], \alpha)$ is equal to the number of sequences j_1, \dots, j_k satisfying (33). Now let

$$\lambda(S) = (j_k, j_{k-1}, \dots, j_1).$$

Note that $\lambda(S)$ is a partition of the integer $\alpha - \binom{k+1}{2}$ with at most k parts and with largest part at most $n - k$. Thus

$$f_k([n], \alpha) = p_{\alpha - \binom{k+1}{2}}(k, n - k), \quad (34)$$

or equivalently,

$$\sum_{\alpha \geq \binom{k+1}{2}} f_k([n], \alpha) q^{\alpha - \binom{k+1}{2}} = \begin{bmatrix} n \\ k \end{bmatrix}.$$

By the rank-unimodality (and rank-symmetry) of $L(n-k, k)$ (Corollary 6.10), the largest coefficient of $\begin{bmatrix} n \\ k \end{bmatrix}$ is the middle one, that is, the coefficient of $\lfloor k(n-k)/2 \rfloor$. It follows that for fixed k and n , $f_k([n], \alpha)$ is maximized for $\alpha = \lfloor k(n-k)/2 \rfloor + \binom{k+1}{2} = \lfloor k(n+1)/2 \rfloor$. Hence the following result is plausible.

6.11 Theorem. *Let $S \in \binom{\mathbb{R}^+}{n}$, $\alpha \in \mathbb{R}^+$, and $k \in \mathbb{P}$. Then*

$$f_k(S, \alpha) \leq f_k([n], \lfloor k(n+1)/2 \rfloor).$$

Proof. Let $S = \{a_1, \dots, a_n\}$ with $0 < a_1 < \dots < a_n$. Let T and U be distinct k -element subsets of S with the same element sums, say $T = \{a_{i_1}, \dots, a_{i_k}\}$ and $U = \{a_{j_1}, \dots, a_{j_k}\}$ with $i_1 < i_2 < \dots < i_k$ and $j_1 < j_2 < \dots < j_k$. Define $T^* = \{i_1, \dots, i_k\}$ and $U^* = \{j_1, \dots, j_k\}$, so $T^*, U^* \in \binom{[n]}{k}$. The crucial observation is the following:

Claim. The elements $\lambda(T^*)$ and $\lambda(U^*)$ are incomparable in $L(k, n - k)$, i.e., neither $\lambda(T^*) \leq \lambda(U^*)$ nor $\lambda(U^*) \leq \lambda(T^*)$.

Proof of claim. Suppose not, say $\lambda(T^*) \leq \lambda(U^*)$ to be definite. Thus by definition of $L(k, n - k)$ we have $i_r - r \leq j_r - r$ for $1 \leq r \leq k$. Hence $i_r \leq j_r$ for $1 \leq r \leq k$, so also $a_{i_r} \leq a_{j_r}$ (since $a_1 < \dots < a_n$). But $a_{i_1} + \dots + a_{i_k} = a_{j_1} + \dots + a_{j_k}$ by assumption, so $a_{i_r} = a_{j_r}$ for all r . This contradicts the assumption that T and U are distinct and proves the claim.

It is now easy to complete the proof of Theorem 6.11. Suppose that S_1, \dots, S_r are distinct k -element subsets of S with the same element sums. By the claim, $\{\lambda(S_1^*), \dots, \lambda(S_r^*)\}$ is an antichain in $L(k, n - k)$. Hence r cannot exceed the size of the largest antichain in $L(k, n - k)$. By Theorem 6.6 and Corollary 6.10, the size of the largest antichain in $L(k, n - k)$ is given by $p_{\lfloor k(n-k)/2 \rfloor}(k, n - k)$. By equation (34) this number is equal to $f_k([n], \lfloor k(n+1)/2 \rfloor)$. In other words,

$$r \leq f_k([n], \lfloor k(n+1)/2 \rfloor),$$

which is what we wanted to prove. \square

Note that an equivalent statement of Theorem 6.11 is that $h_k(n)$ is equal to the coefficient of $q^{\lfloor k(n-k)/2 \rfloor}$ in $\begin{bmatrix} n \\ k \end{bmatrix}$ [why?].

Variation on a theme. Suppose that in Theorem 6.11 we do not want to specify the cardinality of the subsets of S . In other words, for any $\alpha \in \mathbb{R}$ and any finite subset $S \subset \mathbb{R}^+$, define

$$f(S, \alpha) = \#\{T \subseteq S : \sum_{t \in T} t = \alpha\}.$$

How large can $f(S, \alpha)$ be if we require $\#S = n$? Call this maximum value $h(n)$. Thus

$$h(n) = \max_{\substack{\alpha \in \mathbb{R}^+ \\ S \subset \mathbb{R}^+ \\ \#S = n}} f(S, \alpha). \quad (35)$$

For instance, if $S = \{1, 2, 3\}$ then $f(S, 3) = 2$ (coming from the subsets $\{1, 2\}$ and $\{3\}$). This is easily seen to be best possible, i.e., $h(3) = 2$.

We will find $h(n)$ in a manner analogous to the proof of Theorem 6.11. The big difference is that the relevant poset $M(n)$ is *not* of the form B_n/G ,

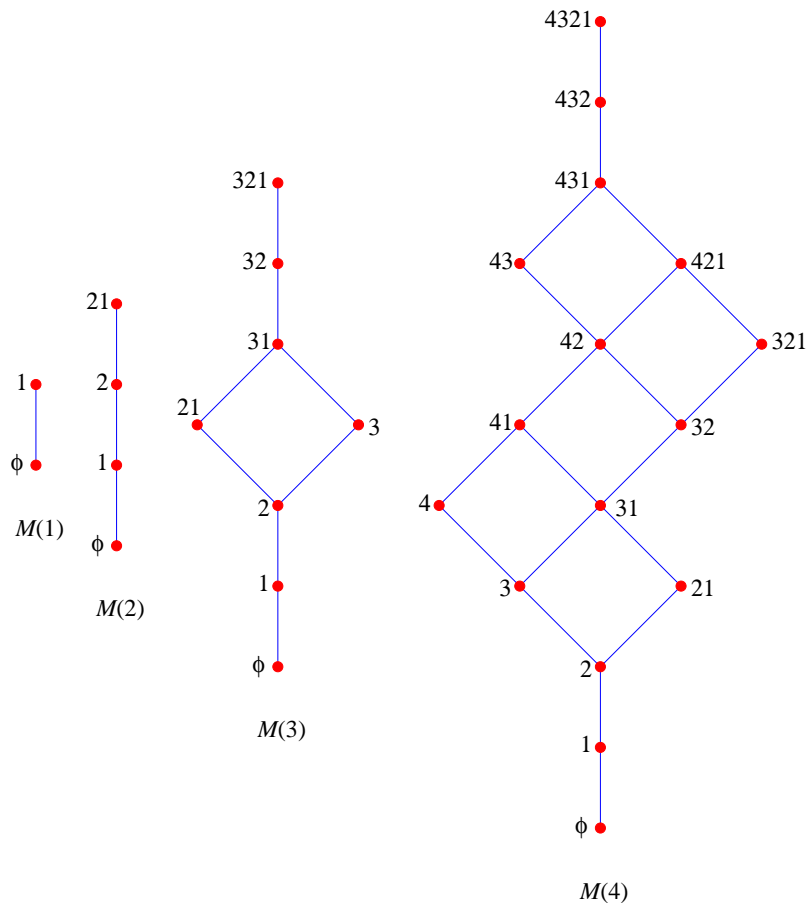


Figure 1: The posets $M(1)$, $M(2)$, $M(3)$ and $M(4)$

so we will have to prove the injectivity of the order-raising operator U_i from scratch. Our proofs will be somewhat sketchy; it shouldn't be difficult for the reader who has come this far to fill in the details.

Let $M(n)$ be the set of all subsets of $[n]$, with the ordering $A \leq B$ if the elements of A are $a_1 > a_2 > \dots > a_j$ and the elements of B are $b_1 > b_2 > \dots > b_k$, where $j \leq k$ and $a_i \leq b_i$ for $1 \leq i \leq j$. (The empty set \emptyset is the bottom element of $M(n)$.) Figure 1 shows $M(1)$, $M(2)$, $M(3)$, and $M(4)$.

It is easy to see that $M(n)$ is graded of rank $\binom{n+1}{2}$. The rank of the subset

$$T = \{a_1, \dots, a_k\} \text{ is} \quad \text{rank}(T) = a_1 + \dots + a_k. \quad (36)$$

It follows [why?] that the rank-generating function of $M(n)$ is given by

$$F(M(n), q) = \sum_{i=0}^{\binom{n+1}{2}} (\#M(n)_i) q^i = (1+q)(1+q^2) \cdots (1+q^n).$$

Define linear transformations

$$U_i : \mathbb{R}M(n)_i \rightarrow \mathbb{R}M(n)_{i+1}, \quad D_i : \mathbb{R}M(n)_i \rightarrow \mathbb{R}M(n)_{i-1}$$

by

$$U_i(x) = \sum_{\substack{y \in M(n)_{i+1} \\ x < y}} y, \quad x \in M(n)_i$$

$$D_i(x) = \sum_{\substack{v \in M(n)_{i-1} \\ v < x}} c(v, x)v, \quad x \in M(n)_i,$$

where the coefficient $c(v, x)$ is defined as follows. Let the elements of v be $a_1 > \dots > a_j > 0$ and the elements of x be $b_1 > \dots > b_k > 0$. Since x covers v , there is a unique r for which $a_r = b_r - 1$ (and $a_k = b_k$ for all other k). In the case $b_r = 1$ we set $a_r = 0$. (E.g., if x is given by $5 > 4 > 1$ and v by $5 > 4$, then $r = 3$ and $a_3 = 0$.) Set

$$c(v, x) = \begin{cases} \binom{n+1}{2}, & \text{if } a_r = 0 \\ (n - a_r)(n + a_r + 1), & \text{if } a_r > 0. \end{cases}$$

It is a straightforward computation (proof omitted) to obtain the commutation relation

$$D_{i+1}U_i - U_{i-1}D_i = \left(\binom{n+1}{2} - 2i \right) I_i, \quad (37)$$

where I_i denotes the identity linear transformation on $\mathbb{R}M(n)_i$. Clearly by definition U_i is order-raising. We want to show that U_i is injective (one-to-one) for $i < \frac{1}{2}\binom{n+1}{2}$. We can't argue as in the proof of Lemma 4.6 that $U_{i-1}D_i$

is semidefinite since the matrices of U_{i-1} and D_i are no longer transposes of one another. Instead we use the following result from linear algebra. For two proofs, see pp. 331-333 of *Selected Papers on Algebra* (S. Montgomery, *et al.*, eds.), Mathematical Association of America, 1977.

6.12 Lemma. Let V and W be finite-dimensional vector spaces over a field. Let $A : V \rightarrow W$ and $B : W \rightarrow V$ be linear transformations. Then

$$x^{\dim V} \det(AB - xI) = x^{\dim W} \det(BA - xI).$$

In other words, AB and BA have the same nonzero eigenvalues.

We can now prove the key linear algebraic result.

6.13 Lemma. The linear transformation U_i is injective for $i < \frac{1}{2}\binom{n+1}{2}$ and surjective (onto) for $i \geq \frac{1}{2}\binom{n+1}{2}$.

Proof. We prove by induction on i that $D_{i+1}U_i$ has positive real eigenvalues for $i < \frac{1}{2}\binom{n+1}{2}$. For $i = 0$ this is easy to check since $\dim \mathbb{R}M(n)_0 = 1$. Assume for $i - 1 < \frac{1}{2}\binom{n+1}{2} - 1$, i.e., assume that D_iU_{i-1} has positive eigenvalues. By Lemma 6.12, $U_{i-1}D_i$ has nonnegative eigenvalues. By (37), we have

$$D_{i+1}U_i = U_{i-1}D_i + \left(\binom{n+1}{2} - 2i \right) I_i.$$

Thus the eigenvalues of $D_{i+1}U_i$ are $\binom{n+1}{2} - 2i$ more than those of $U_{i-1}D_i$. Since $\binom{n+1}{2} - 2i > 0$, it follows that $D_{i+1}U_i$ has positive eigenvalues. Hence it is invertible, so U_i is injective. Similarly (or by ‘‘symmetry’’) U_i is surjective for $i \geq \frac{1}{2}\binom{n+1}{2}$. \square

The main result on the posets $M(n)$ now follows by a familiar argument.

6.14 Theorem. The poset $M(n)$ is graded of rank $\binom{n+1}{2}$, rank-symmetric, rank-unimodal, and Sperner.

Proof. We have already seen that $M(n)$ is graded of rank $\binom{n+1}{2}$ and rank-symmetric. By the previous lemma, U_i is injective for $i < \frac{1}{2}\binom{n+1}{2}$ and surjective for $i \geq \frac{1}{2}\binom{n+1}{2}$. The proof follows from Proposition 4.4 and Lemma 4.5. \square

NOTE. As a consequence of Theorem 6.14, the polynomial $F(M(n), q) = (1 + q)(1 + q^2) \cdots (1 + q^n)$ has unimodal coefficients. No combinatorial proof of this fact is known, unlike the situation for $L(m, n)$ (where we mentioned the proof of O'Hara above).

We can now determine $h(n)$ (as defined by equation (35)) by an argument analogous to the proof of Theorem 6.11.

6.15 Theorem. *Let $S \in \binom{\mathbb{R}^+}{n}$ and $\alpha \in \mathbb{R}^+$. Then*

$$f(S, \alpha) \leq f\left([n], \left\lfloor \frac{1}{2} \binom{n+1}{2} \right\rfloor\right) = h(n).$$

Proof. Let $S = \{a_1, \dots, a_n\}$ with $0 < a_1 < \cdots < a_n$. Let T and U be distinct subsets of S with the same element sums, say $T = \{a_{r_1}, \dots, a_{r_j}\}$ and $U = \{a_{s_1}, \dots, a_{s_k}\}$ with $r_1 < r_2 < \cdots < r_j$ and $s_1 < s_2 < \cdots < s_k$. Define $T^* = \{r_1, \dots, r_j\}$ and $U^* = \{s_1, \dots, s_k\}$, so $T^*, U^* \in M(n)$. The following fact is proved exactly in the same way as the analogous fact for $L(m, n)$ (the claim in the proof of Theorem 6.11) and will be omitted here.

Fact. The elements T^* and U^* are incomparable in $M(n)$, i.e., neither $T^* \leq U^*$ nor $U^* \leq T^*$.

It is now easy to complete the proof of Theorem 6.15. Suppose that S_1, \dots, S_t are distinct subsets of S with the same element sums. By the above fact, $\{S_1^*, \dots, S_t^*\}$ is an antichain in $M(n)$. Hence t cannot exceed the size of the largest antichain in $M(n)$. By Theorem 6.14, the size of the largest antichain in $M(n)$ is the size $p_{\lfloor \frac{1}{2} \binom{n+1}{2} \rfloor}$ of the middle rank. By equation (36) this number is equal to $f([n], \lfloor \frac{1}{2} \binom{n+1}{2} \rfloor)$. In other words,

$$t \leq f\left([n], \left\lfloor \frac{1}{2} \binom{n+1}{2} \right\rfloor\right),$$

which is what we wanted to prove. \square

NOTE. Theorem 6.15 is known as the *weak Erdős-Moser conjecture*. The original (strong) Erdős-Moser conjecture deals with the case $S \subset \mathbb{R}$ rather

than $S \subset \mathbb{R}^+$. There is a difference between these two cases; for instance, $h(3) = 2$ (corresponding to $S = \{1, 2, 3\}$ and $\alpha = 3$), while the set $\{-1, 0, 1\}$ has *four* subsets whose elements sum to 0 (including the empty set). (Can you see where the proof of Theorem 6.15 breaks down if we allow $S \subset \mathbb{R}$?) The original Erdős-Moser conjecture asserts that if $\#S = 2m + 1$, then

$$f(S, \alpha) \leq f(\{-m, -m + 1, \dots, m\}, 0).$$

This result can be proved by a somewhat tricky modification of the proof given above for the weak case. No proof of the Erdős-Moser conjecture (weak or strong) is known other than the one indicated here (sometimes given in a more sophisticated context, as explained in the next Note).

NOTE. The key to the proof of Theorem 6.15 is the definition of U_i and D_i which gives the commutation relation (37). The reader may be wondering how anyone managed to discover these definitions (especially that of D_i). In fact, the original proof of Theorem 6.15 was based on the representation theory of the orthogonal Lie algebra $\mathfrak{o}(2n, \mathbb{C})$. In this context, the definitions of U_i and D_i are built into the theory of the “principal subalgebras” of $\mathfrak{o}(2n, \mathbb{C})$. Robert Proctor was the first to remove the representation theory from the proof and present it solely in terms of linear algebra. See his paper in *Amer. Math. Monthly* **89** (1982), 721–634.