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 $\varphi : G \to \mathfrak{S}_X$, 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:

$$(0,1) \cdot a = b, \quad (0,1) \cdot b = a, \quad (0,1) \cdot c = c, \quad (0,1) \cdot d = d$$

$$(1,0) \cdot a = a, \quad (1,0) \cdot b = b, \quad (1,0) \cdot c = d, \quad (1,0) \cdot d = c.$$

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

$$(0,1) \cdot a = b, \quad (0,1) \cdot b = a, \quad (0,1) \cdot c = d, \quad (0,1) \cdot d = c$$

$$(1,0) \cdot a = c, \quad (1,0) \cdot b = d, \quad (1,0) \cdot c = a, \quad (1,0) \cdot d = b.$$

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 $\varphi : P \to P$. (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 $\mathrm{Aut}(P)$ 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 $\{1, \ldots, n\}$ acts on B_n as follows: If $x = \{i_1, i_2, \ldots, i_k\} \in B_n$, then

$$\pi(x) = \{\pi(i_1), \pi(i_2), \ldots, \pi(i_k)\}. \qquad (24)$$

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

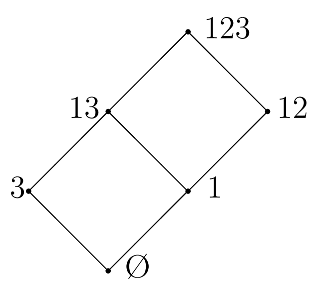
$\mathfrak{S}_n$ of all permutations of $\{1,\ldots,n\}$ on B_n [why?]. (In fact, it is not hard to show that *every* automorphism of B_n is of the form (24) for $\pi \in \mathfrak{S}_n$.) In particular, any subgroup G of $\mathfrak{S}_n$ acts on B_n *via* (24) (where we restrict π to belong to G). In 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 $\{123\}$.

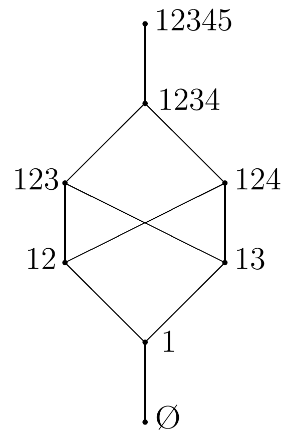
We now define the class of posets which will be of interest to us here. Later we will give some special cases of particular interest.

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 $\mathcal{O} \le \mathcal{O}'$ in B_n/G if there exist $x \in \mathcal{O}$ and $y \in \mathcal{O}'$ such that $x \le y$ in B_n. (It's easy to check that this relation $\le$ 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.,

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

Then $\{x_1, \ldots, x_j\}$ is an orbit of i-element subsets of $\{1, \ldots, n\}$ if and only if $\{\bar{x}_1, \ldots, \bar{x}_j\}$ 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. □

Let $\pi \in \mathfrak{S}_n$. We associate with π a linear transformation (still denoted π)
$\pi : \mathbb{R}(B_n)_i \to \mathbb{R}(B_n)_i$ 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 $\pi \in G$. 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. Now a vector $v \in \mathbb{R}(B_n)_i$ will belong to $\mathbb{R}(B_n)_i^G$ if and only if its coefficients are constant on G-orbits and hence if and only if it is a linear combination of $v_{\mathcal{O}}$'s for the various G-orbits $\mathcal{O}$.

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

$$\pi(U_i(v)) \;=\; U_i(\pi(v))$$

$$= \quad U_i(v),$$

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 $\hat{U}_i : \mathbb{R}P_i \to \mathbb{R}P_{i+1}$ and order-lowering operators $\hat{D}_i : \mathbb{R}P_i \to \mathbb{R}P_{i-1}$. 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 $\hat{U}_i : \mathbb{R}P_i \to \mathbb{R}P_{i+1}$ correspond to the usual order-raising operator $U_i : \mathbb{R}(B_n)_i \to \mathbb{R}(B_n)_{i+1}$. More precisely, suppose that the order-raising operator U_i for B_n given by (18) satisfies

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

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 $\hat{U}_i : \mathbb{R}((B_n)_i/G) \to \mathbb{R}((B_n)_i/G)$ 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 $\hat{D}_i : \mathbb{R}(B_n)_i^G \to \mathbb{R}(B_n)_{i-1}^G$ 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. □

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 $M = \{1, \ldots, m\}$. 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 $p_0, p_1, \ldots, p_{\binom{m}{2}}$ 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.