A PERMUTATION GROUP DETERMINED BY AN ORDERED SET

ANDERS CLAESSON, CHRIS D. GODSIL, AND DAVID G. WAGNER

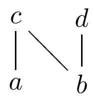
Abstract. Let P be a finite ordered set, and let $J(P)$ be the distributive lattice of order ideals of P. The covering relations of $J(P)$ are naturally associated with elements of P; in this way, each element of P defines an involution on the set $J(P)$. Let $\Gamma(P)$ be the permutation group generated by these involutions. We show that if P is connected then $\Gamma(P)$ is either the alternating or the symmetric group. We also address the computational complexity of determining which case occurs.

Let P be a finite ordered set, and let $J(P)$ be the distributive lattice of order ideals (also called down–sets) of P. For each $p \in P$, define a permutation σ_p on $J(P)$ as follows: for every $S \in J(P)$,

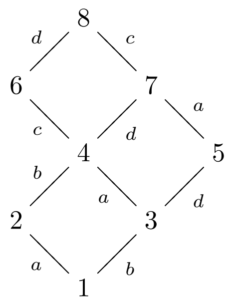
$$\sigma_p(S) := \begin{cases} S \cup \{p\} & \text{if } p \text{ is minimal in } P \smallsetminus S, \\ S \smallsetminus \{p\} & \text{if } p \text{ is maximal in } S, \\ S & \text{otherwise.} \end{cases}$$

Each of these permutations is an involution. We let $\Gamma(P)$ denote the subgroup of the symmetric group $\mathrm{Sym}(J(P))$ generated by all these involutions. Plain curiosity led us to wonder about the structure of these permutation groups. As we shall see, this can be determined quite precisely.

As an example, for

$P =$ 

we may number the down–sets $\{\varnothing, a, b, ab, bd, abc, abd, abcd\}$ of P by 1 through 8, and then

$J(P) =$ 

and

$$\begin{cases} \sigma_a = (1\,2)(3\,4)(5\,7) \\ \sigma_b = (1\,3)(2\,4) \\ \sigma_c = (4\,6)(7\,8) \\ \sigma_d = (3\,5)(4\,7)(6\,8) \end{cases}$$

Key words and phrases. ordered set, distributive lattice, permutation group.

Research supported by an operating grant from the Natural Sciences and Engineering Research Council of Canada.

in which we have labeled the edges of the Hasse diagram of $J(P)$ to indicate the action of each σ_p on $J(P)$. By using GAP [1] (or otherwise) one finds that $\Gamma(P)$ is the symmetric group $\mathrm{Sym}(J(P))$ in this case.

We use the following notation for ordered sets. The set of minimal elements of P is $P_{\min}$ and the set of maximal elements of P is $P_{\max}$. A covering relation in P is denoted by $a \lessdot b$. For $S \subseteq P$ we let $\downarrow S = \{p \in P : \ p \leq b \text{ for some } b \in S\}$ denote the down–set (order ideal) generated by S, we let $\uparrow S = \{p \in P : \ b \leq p \text{ for some } b \in S\}$ denote the up–set (dual order ideal) generated by S, and we let $\updownarrow \{p\} = \downarrow S \cup \uparrow S$ be the set of elements comparable with S. The set P with the opposite order is denoted by P^{op}. For more background on finite ordered sets and distributive lattices, see Chapter 3 of Stanley [2], for instance.

The first observation is completely elementary.

Lemma 1. *Let P and Q be disjoint finite ordered sets. Then*

$$\Gamma(P \cup Q) = \Gamma(P) \times \Gamma(Q).$$

Proof. Since $P \cup Q$ is the disjoint union of P and Q we may regard $J(P \cup Q)$ as $J(P) \times J(Q)$ via the bijection $S \leftrightarrow (S \cap P, S \cap Q)$. For such a down–set S of $P \cup Q$ we have $\sigma_p(S) = (\sigma_p(S \cap P), S \cap Q)$ for all $p \in P$, and $\sigma_q(S) = (S \cap P, \sigma_q(S \cap Q))$ for all $q \in Q$. This proves the result. $\square$

The problem is thus reduced to determining $\Gamma(P)$ for connected ordered sets P.

Theorem 2. *Let P be a finite connected ordered set. Then $\Gamma(P)$ is either the alternating group $\mathrm{Alt}(J(P))$ or the symmetric group $\mathrm{Sym}(J(P))$.*

This is, of course, something of a disappointment – we had hoped that some ordered sets would exhibit groups with more interesting structure. Our proof of Theorem 2 is by induction on $|J(P)|$. We begin with a few simple observations.

Lemma 3. *For any finite ordered set P, the permutation group $\Gamma(P)$ acts transitively on $J(P)$.*

Proof. This follows immediately from connectedness of the Hasse diagram of $J(P)$. $\square$

Lemma 4. *For any finite ordered set P, $\Gamma(P^{\mathrm{op}}) \simeq \Gamma(P)$.*

Proof. One checks that the bijection $S \mapsto P \smallsetminus S$ from $J(P)$ to $J(P^{\mathrm{op}})$ commutes with the actions of $\Gamma(P)$ on $J(P)$ and $\Gamma(P^{\mathrm{op}})$ on $J(P^{\mathrm{op}})$. $\square$

An element of an ordered set is *extremal* if it is either minimal or maximal.

Lemma 5. *Every finite connected ordered set P with at least two elements has an extremal element $p \in P$ such that $P \smallsetminus \{p\}$ is also connected.*

Proof. Form the bipartite graph G with bipartition $(P_{\min}, P_{\max})$ and with edges $a \sim b$ whenever $a < b$ in P. Then G has at least two elements, and P is connected if and only if G is connected. Let T be a spanning tree of G, and let p be a leaf of T. Then $G \smallsetminus \{p\}$ is connected, so that $P \smallsetminus \{p\}$ is connected. $\square$

Lemma 6. *Let P be a finite ordered set, and let $p \in P_{\max}$. Then*

$$\frac{1}{2}|J(P)| \leq |J(P \smallsetminus \{p\})| < |J(P)|.$$

Further, if P is connected and $|P| \geq 2$ then the first inequality is strict.

Proof. The second inequality is trivial. Let L be the set of down–sets of P which contain p, so that $J(P) = J(P \setminus \{p\}) \cup L$. The function from L to $J(P \setminus \{p\})$ given by $S \mapsto S \setminus \{p\}$ is injective, so that $|L| \leq |J(P \setminus \{p\})|$ and the first inequality follows. If equality holds then the above function is a bijection, so that $p \in P_{\min} \cap P_{\max}$. When $|P| \geq 2$ this implies that P is not connected. □

Lemma 7. *Let P be a finite ordered set, and let $p \in P$. Then $\Gamma(P \setminus \{p\})$ is a quotient of a subgroup of $\Gamma(P)$.*

Proof. The subgroup $H = \langle \sigma_a : \ a \in P \setminus \{p\} \rangle$ of $\Gamma(P)$ has two orbits on $J(P)$ – namely $J(P \setminus \{p\})$ and L, with the notation of the proof of Lemma 6. The homomorphism $\gamma \mapsto \gamma|_{J(P \setminus \{p\})}$ from H to $\Gamma(P \setminus \{p\})$ is surjective, and the result follows. □

Proposition 8. *Let P be a finite connected ordered set. Then $\Gamma(P)$ is 2–transitive (and hence primitive).*

Proof. Since $\Gamma(P)$ is transitive, by Lemma 3, it suffices to show that the stabilizer $\Gamma(P)_\varnothing$ of $\varnothing$ in $\Gamma(P)$ is transitive on $J(P) \setminus \{\varnothing\}$. We prove this by induction on $|P|$, the basis $|P| = 1$ being trivial.

For the induction step $|P| \geq 2$, so that by Lemma 5 there is an extremal element $p \in P$ such that $P \setminus \{p\}$ is connected. By Lemma 4, (replacing P by P^{op} if necessary) we may assume that p is maximal in P.

For each $A \subseteq P_{\min}$, let $J_A(P)$ be the set of down–sets $S \in J(P)$ such that $S \cap P_{\min} = A$. Each of these is a distributive lattice – in fact $J_A(P) \simeq J(P_A)$ in which P_A is obtained by deleting the up–set $\uparrow(P_{\min} \setminus A)$ from P, then deleting the set A of minimal elements of the result; see Figure 1 for an example. The covering relations of $J(P_A)$ correspond to elements of $P_A \subseteq P \setminus P_{\min}$. By Lemma 3, $\Gamma(P_A)$ acts transitively on $J(P_A)$. Therefore, the subgroup $D = \langle \sigma_v : \ v \in P \setminus P_{\min} \rangle$ of $\Gamma(P)$ acts transitively on each of the sets $J_A(P)$ separately, for all $A \subseteq P_{\min}$. In fact, these are the orbits of D acting on $J(P)$. The subgroup D is contained in the stabilizer $\Gamma(P)_\varnothing$.

Now, $P \setminus \{p\}$ is connected, so that $\Gamma(P \setminus \{p\})$ is 2–transitive on $J(P \setminus \{p\})$, by induction. Since $\Gamma(P \setminus \{p\})$ is a quotient of a subgroup of $\Gamma(P)$, it follows that $\Gamma(P)_\varnothing$ is transitive on $J(P \setminus \{p\}) \setminus \{\varnothing\}$ as well. Since $J(P_{\min}) \setminus \{\varnothing\} \subseteq J(P \setminus \{p\}) \setminus \{\varnothing\}$, it follows that $J(P_{\min}) \setminus \{\varnothing\}$ is contained in a single orbit of $\Gamma(P)_\varnothing$ acting on $J(P)$. Since $J(P) \setminus \{\varnothing\}$ is the union of the $J_A(P)$ for all $\varnothing \neq A \subseteq P_{\min}$, it follows that $\Gamma(P)_\varnothing$ acts transitively on $J(P) \setminus \{\varnothing\}$. This completes the induction step, and the proof. □

A well–known lemma ([3] Theorem 13.3) states that if a primitive permutation group of degree n contains a 3–cycle then it contains $\mathrm{Alt}(n)$. We can apply this in the following circumstance. A covering relation $a \lessdot b$ in P is *dominant* provided that every element of P is comparable with either a or b.

Proposition 9. *If a finite ordered set P has a dominant covering relation, then $\mathrm{Alt}(J(P)) \leq \Gamma(P)$.*

Proof. Notice that since P has a dominant covering relation $a \lessdot b$, it follows that P is connected. Proposition 8 thus implies that $\Gamma(P)$ is primitive. We claim that the element $\gamma = \sigma_b \sigma_a \sigma_b \sigma_a$ of $\Gamma(P)$ is a 3–cycle, which suffices to prove the result.

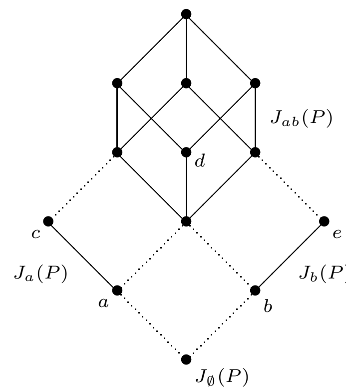


FIGURE 1. The partition of $J(P)$ for $P = {}^{c}\diagdown_{a}\diagup^{d}\diagdown_{b}\diagup^{e}$

Consider any down–set S of P on which both σ_a and σ_b act nontrivially. Then we have either $a \in S_{\max}$ or $a \in (P \smallsetminus S)_{\min}$, and either $b \in S_{\max}$ or $b \in (P \smallsetminus S)_{\min}$. Since $a < b$ and S is a down–set, the only consistent possibility is that $a \in S_{\max}$ and $b \in (P \smallsetminus S)_{\min}$. If $c \in S_{\max}$ and $c \neq a$, then a and c are incomparable – since $a \lessdot b$ is dominant it follows that $c < a$. Therefore, $S \subseteq \downarrow\{b\} \smallsetminus \{b\}$. Since $b \in (P \smallsetminus S)_{\min}$, it follows that $S = \downarrow\{b\} \smallsetminus \{b\}$. That is, this down–set $\downarrow\{b\} \smallsetminus \{b\}$ is the only element of $J(P)$ on which both σ_a and σ_b act nontrivially. From this and the fact that σ_a and σ_b are involutions, it follows that $\sigma_b\sigma_a$ consists of one 3–cycle and some 2–cycles and fixed points. Therefore $\gamma = (\sigma_b\sigma_a)^2$ is a 3–cycle, as claimed. □

The induction step for the proof of Theorem 2 is a consequence of the following lemma.

Lemma 10. *Let Γ be a primitive group of permutations on a set X with $|X| \geq 9$. Assume that Γ has a subgroup H which has exactly two orbits Y and $\overline{Y}$ on X, such that $|Y| > |\overline{Y}|$ and $\mathrm{Alt}(Y) \leq H|_Y$. Then $\mathrm{Alt}(X) \leq \Gamma$.*

Proof. Let K be the preimage of $\mathrm{Alt}(Y)$ under the quotient map $H \to H|_Y$. If the pointwise stabilizer $K_{\overline{Y}}$ is trivial then K acts faithfully on $\overline{Y}$, and therefore $\mathrm{Alt}(Y)$ acts faithfully on $\overline{Y}$. Since $|\overline{Y}| < |Y|$ this is not possible, so that $K_{\overline{Y}}$ is not trivial. Therefore, H contains a nontrivial element h fixing $\overline{Y}$ pointwise. The conjugates of h under H generate a normal subgroup G of H with nontrivial image in $H|_Y$. Since $\mathrm{Alt}(Y)$ is simple it follows that $\mathrm{Alt}(Y) \leq G$. In particular, G (and hence Γ) contains a three–cycle. Since Γ is primitive, it follows that $\mathrm{Alt}(X) \leq \Gamma$. □

Proof of Theorem 2. We prove Theorem 2 by induction on $|J(P)|$. If P is a connected ordered set of width at most two then P contains a dominant covering relation, so that $\mathrm{Alt}(J(P)) \leq \Gamma(P)$ by Proposition 9. If P is a connected ordered set of width at least three, then $|J(P)| \geq 9$. Thus, the basis of induction $|J(P)| \leq 8$ is established. For the induction step, let P be a connected ordered set with $|J(P)| \geq 9$. Replacing P by P^{op}, if necessary (by Lemma 4) we may assume that $p \in P_{\max}$ is such that $P \smallsetminus \{p\}$ is connected (by Lemma 5). Now Lemmas 6 and 7, Proposition 8, and the induction hypothesis imply that $\Gamma = \Gamma(P)$, $X = J(P)$,

$H = \langle \sigma_a : \ a \in P \smallsetminus \{p\} \rangle$, and $Y = J(P \smallsetminus \{p\})$ satisfy the hypotheses of Lemma 10. It follows that $\mathrm{Alt}(J(P)) \leq \Gamma(P)$, completing the induction step and the proof. $\square$

The only remaining issue is to determine, for each finite connected ordered set, which case of the conclusion of Theorem 2 holds. This seems to be difficult, but it is equivalent to a problem which appears superficially to be easier.

Proposition 11. *Let P be a finite connected ordered set. Then $\Gamma(P) = \mathrm{Alt}(J(P))$ if and only if for every $p \in P$, the cardinality of $J(P \smallsetminus \updownarrow\{p\})$ is even.*

Proof. The statement follows by observing that for each $p \in P$, the two–cycles of the involution σ_p correspond bijectively with the elements of $J(P \smallsetminus \updownarrow\{p\})$. Thus, the condition is equivalent to requiring that $\Gamma(P)$ is contained in $\mathrm{Alt}(J(P))$. $\square$

Proposition 11 suggests the following two decision problems.

The Group Problem:
Instance: A finite connected ordered set P.
Problem: Determine whether $\Gamma(P)$ equals $\mathrm{Alt}(J(P))$ or $\mathrm{Sym}(J(P))$.

The Parity Problem:
Instance: A finite ordered set P.
Problem: Determine whether $|J(P)|$ is even or odd.

A decision problem $\mathcal{A}$ is *polynomially reducible* to a decision problem $\mathcal{B}$ when the following holds: from any instance A of $\mathcal{A}$ of size n one can compute several instances $B_1, \ldots, B_m$ of $\mathcal{B}$ such that:
- the number of operations required to compute $\{B_i\}$ is bounded by a polynomial function of n; and
- given a solution to $\mathcal{B}$ for each B_i, a solution to $\mathcal{A}$ for A can be computed using a number of operations which is bounded by a polynomial function of n.

Two decision problems each of which is polynomially reducible to the other are said to be *polynomially equivalent*. [We are being rather informal with these issues of computational complexity. To be precise, the size of an instance is the number of bits required to represent it, and the operations discussed above are bit operations.]

Theorem 12. *The Group Problem and the Parity Problem are polynomially equivalent.*

Proof. First, we reduce the Parity Problem to the Group Problem. Given a finite ordered set P as an instance of the Parity Problem, let x, y, z be distinct new elements, and construct the ordered set Q with elements $P \cup \{x, y, z\}$ and order relations given by those of P together with $\{x, y\} \times (P \cup \{z\})$. Then Q is a finite connected ordered set. Assume that we have a solution to the Group Problem for Q. By Proposition 11, we know whether or not all of the $|J(Q \smallsetminus \updownarrow\{b\})|$ for $b \in Q$ are even. Now, if $b \in P$ then $Q \smallsetminus \updownarrow\{b\} = (P \smallsetminus \updownarrow\{b\}) \cup \{z\}$, so that $J(Q \smallsetminus \updownarrow\{b\}) = J(P \smallsetminus \updownarrow\{b\}) \times J(\{z\})$ has even cardinality since $|J(\{z\})| = 2$. Also, if $b \in \{x, y\}$ then $|Q \smallsetminus \updownarrow\{b\}| = 1$ so that $|J(Q \smallsetminus \updownarrow\{b\})| = 2$. Thus, $\Gamma(Q) = \mathrm{Alt}(J(Q))$ if and only if $|J(Q \smallsetminus \updownarrow\{z\})|$ is even. Since $Q \smallsetminus \updownarrow\{z\} = P$, this reduces the Parity Problem to the Group Problem. One checks easily that the computations can be made with only polynomially many operations.

Conversely, we reduce the Group Problem to the Parity Problem. Given a connected finite ordered set P as an instance of the Group Problem, consider the set

$\{P \smallsetminus \updownarrow \{p\} : \ p \in P\}$ of instances of the Parity Problem. This set can be computed from P using only polynomially many operations. Given a solution to the Parity Problem for each instance in this set, we check whether all these parities are even – Proposition 11 implies that if so, then $\Gamma(P) = \mathrm{Alt}(J(P))$; otherwise $\Gamma(P) = \mathrm{Sym}(J(P))$. This reduces the Group Problem to the Parity Problem, and completes the proof. □

References

[1] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.3; 2002, `(http://www.gap-system.org)`.

[2] R.P. Stanley, *Enumerative Combinatorics, Vol. 1*, Cambridge U.P., Cambridge, 1997.

[3] H. Wielandt, *Finite permutation groups* (translated by R. Bercov) Academic Press, New York/London, 1964.

Department of Mathematics, Chalmers University of Technology, S-412 96 Göteborg, Sweden

E-mail address: `claesson@math.chalmers.se`

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: `cgodsil@uwaterloo.ca`

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: `dgwagner@math.uwaterloo.ca`