Reprinted from

mathematical *social* *sciences*

Mathematical Social Sciences 27 (1994) 59–72
0165-4896/94/$07.00

Permutation lattices revisited

George Markowsky

Computer Science Department, University of Maine, Orono, ME 04469, USA

Communicated by M.F. Janowitz
Received 1 September 1992
Revised 2 August 1993

Mathematical Social Sciences 27 (1994) 59–72
0165-4896/94/$07.00 © 1994 – Elsevier Science B.V. All rights reserved

Permutation lattices revisited

George Markowsky

Computer Science Department, University of Maine, Orono, ME 04469, USA

Communicated by M.F. Janowitz
Received 1 September 1992
Revised 2 August 1993

Abstract

This paper shows how to compute efficiently meets and joins of permutations. The algorithms presented here have a worst case time of $O(N^2)$ and a space requirement of $O(N)$. The paper discusses how to adapt these algorithms for computing the meets and joins in the Newman commutativity lattices of Bennett and Birkhoff (1990).

Every element in the lattice of n-element permutations, S_n, has a complement; see, for example, Bennett and Birkhoff (1990). Since S_n is semidistributive (Duquenne and Cherfouh, 1991), it is also pseudocomplemented. As shown by Chameni-Nembua and Monjardet (1992, 1993) the complements of an element, x, in a complemented and pseudocomplemented lattice form an interval with the top element being the meet-pseudocomplement of x, x^*, while the bottom element is the join-pseudo-complement of x, $x^{\dagger}$. This paper describes how to compute x^* and $x^{\dagger}$.

The material developed in this paper is used to prove a result of Björner that the automorphism group of S_n for $n \geq 3$ consists of exactly 2 elements. The group of automorphisms and dual automorphisms of S_n is the Klein, 4-group. Finally, the poset of irreducibles for S_n is characterized.

Key words: Permutation; lattice; Meet-semidistributive; Join-pseudocomplement

1. Basic concepts

The group of all permutations of an n-element set is an example of a Coxeter group. Coxeter groups are commonly ordered using three orderings: (strong) Bruhat ordering, left weak Bruhat ordering and right weak Bruhat ordering (see Björner, 1984; Björner and Wachs, 1988; and Humphreys, 1990, for details). The weak Bruhat orderings are of particular interest because they produce isomorphic lattices when the Coxeter groups are finite (Björner, 1984; Le Conte de Poly-Barbut, 1992). Since this paper focuses on permutation groups, we will use the ordering used in Guilbaud and Rosenstiehl (1963) and Yanagimoto and Okamoto (1969) which is equivalent to the weak Bruhat orderings but can be defined without reference to Coxeter groups.

Throughout this paper, $\mathbf{n}$ represents the set $\{1, \ldots, n\}$, and S_n represents the symmetric group of all permutations on $\mathbf{n}$. Unless otherwise stated, n is an arbitrary positive integer.

SSDI 0165-4896(93)00731-9

Notation 1. We will represent members of S_n by strings of integers. Let $\sigma \in S_n$ and $i \in \boldsymbol{n}$, then index(σ, i) is the position of i in σ, when σ is written as a string. For example, if $\sigma = 4312$, index$(\sigma, 2) = 4$. When discussing permutations represented by strings, the terms prefix and suffix shall have their usual meaning. □

Definition 1. Let $\sigma, \pi \in S_n$. We say that $\sigma \le \pi$ if for all $i, j \in \boldsymbol{n}$, $(i<j)$ and (index$(\sigma, i) >$ index(σ, j)) imply that (index$(\pi, i) >$ index(π, j)). Given $\sigma \in S_n$, an ordered pair (i, j) is called an *inversion in* σ if $i<j$ and index$(\sigma, i) >$ index(σ, j). □

Remark 1. It is easy to see that $\le$ is a partial order. Permutations can also be thought of as functions, in which case the permutation $\sigma = 4312$ is the function having $\sigma(1) = 4$, $\sigma(2) = 3$, etc. This interpretation permits a different partial ordering. If $\sigma, \pi \in S_n$, we can define $\sigma \le \pi$ if for all $i, j \in \boldsymbol{n}$, $(i<j)$ and $(\sigma(i) > \sigma(j))$ imply $(\pi(i) > \pi(j))$. This ordering and the one defined in Definition 1 are the two kinds of weak Bruhat ordering and give isomorphic posets, with the isomorphism being given by the map $\sigma \to \sigma^{-1}$. Figure 2 in Bennett and Birkhoff (1990) illustrates the different orderings for S_3. Since there is no need to discuss both partial orders, only the ordering introduced in Definition 1 will be discussed in the remainder of this paper. □

Remark 2. Bennett and Birkhoff (1990) show how the partial order on S_n can be derived from the covering relation $\sigma \lessdot \pi$, meaning that a pair of adjacent elements, a and b with $a<b$, in the string representation of σ, are swapped. We will call such a pair of elements an *increasing adjacent pair*. For example, $3142 \lessdot 3412$ because the pair 14 was swapped. Throughout this paper we assume $n \ge 3$ since the cases $n<3$ are trivial: S_1 is the one-element lattice and S_2 is the two-element lattice.

Notation 2. For $\sigma \in S_n$, let $\text{Inv}(\sigma) = \{(i, j) \mid i<j, \text{ and index}(\sigma, i) > \text{index}(\sigma, j)\}$, $\text{Agr}(\sigma) = \{(i, j) \mid i<j, \text{ and index}(\sigma, i) < \text{index}(\sigma, j)\}$. Also let $\Omega(n)$ be the set $\{(i, j) \mid i, j \in \boldsymbol{n} \text{ and } i<j\}$. Thus, Inv$(\sigma)$ is the set of all inversions in σ, Agr(σ) the set of all pairs whose natural ordering *agrees* with their ordering in σ, and $\text{Inv}(\sigma) \cup \text{Agr}(\sigma) = \Omega(\sigma)$.

For example, $\text{Inv}(4312) = \{(1,3), (1,4), (2,3), (2,4), (3,4)\}$, and $\text{Inv}(n(n-1)(n-2)\ldots321) = \Omega(n)$. It is easy to see that for $\sigma, \pi \in S_n$, $\sigma \le \pi$ if and only if $\text{Inv}(\sigma) \subseteq \text{Inv}(\pi)$. □

Remark 3. That $(S_n, \le)$ is a lattice appears to have been first proved by Guilbaud and Rosenstiehl (1963), but has been discovered by other authors as well. In particular, in their proof, Yanagimoto and Okamoto (1969) ordered permutations by inclusion on the sets of pairs (i, j) such that $i<j$ and index $(\sigma, i) <$ index(σ, j), and characterized the sets of pairs which are associated with a permutation. This characterization can be used to show that S_n is a lattice, but does not immediately translate into an efficient algorithm for calculating meets and joins. The next section provides a short proof that S_n is a lattice which also provides efficient algorithms for computing joins and meets.

Definition 2. Let $\sigma \in S_n$. The *reversal* of σ, denoted by $\sigma^{\perp}$, is the permutation written in reverse order. □

Remark 4. For example, $4312^{\perp} = 2134$. We use $^{\perp}$ for reversal since $\sigma^{\perp}$ is the orthocomplement of σ. Note that $\text{Inv}(\sigma^{\perp}) = \Omega(n) - \text{Inv}(\sigma) = \text{Agr}(\sigma)$, where $\sigma \in S_n$.

2. Calculating meets and joins efficiently

Definition 3. For a permutation $\alpha = \alpha_1 \ldots \alpha_k n \alpha_{k+2} \ldots \alpha_n$ of $\boldsymbol{n}$ define the *n-cut* of α to be the pair $(A, A^{\#})$, where A is the string $\alpha_1 \ldots a_k$ and $A^{\#}$ is the string $\alpha_{k+2} \ldots \alpha_n$. □

Remark 5. In the n-cut of α, either A or $A^{\#}$ can be empty. Given the n-cut of α, α can be written as $AnA^{\#}$. Furthermore, if $\alpha\ (= AnA^{\#}) \le \beta\ (= BnB^{\#})$, then $A^{\#} \subseteq B^{\#}$ since any inversion (n, i) in α must be in β. For notational convenience we will treat strings as if they are also sets of integers. Thus, $A \subseteq B$ between strings means that every character appearing in A appears somewhere in B although it could be in a different position.

If $\alpha = AnA^{\#}$, let $\alpha\hat{}$ denote the permutation corresponding to $AA^{\#}$, so that $\alpha\hat{}$ is a permutation of $\boldsymbol{n-1}$. If $\alpha \le \beta$, then $\alpha\hat{} \le \beta\hat{}$.

Theorem 1 gives a short proof that S_n is a lattice and provides an approach for efficiently calculating meets and joins. The proof developed out of a series of exchanges between M.K. Bennett, Garrett Birkhoff and myself. An early version of these results appeared in Markowsky (1990a). □

Theorem 1. (a) *S_n is a lattice. Given α and β in S_n, $\alpha \vee \beta$ and $\alpha \wedge \beta$ are computed recursively as follows. Let $\pi = \alpha\hat{} \vee \beta\hat{}$, $\delta = \alpha\hat{} \wedge \beta\hat{}$, $(A, A^{\#})$ be the n-cut of α, and $(B, B^{\#})$ be the n-cut of β. Then $\alpha \vee \beta = CnC^{\#}$, where $C^{\#}$ is the smallest suffix of π which contains $A^{\#} \cup B^{\#}$ and $\pi = CC^{\#}$. Similarly, $\alpha \wedge \beta = DnD^{\#}$, where D is the smallest prefix of δ which contains $A \cup B$ and $\delta = DD^{\#}$.*

(b) $\text{Inv}(\alpha \vee \beta) = (\text{Inv}(\alpha) \cup \text{Inv}(\beta))^{\text{tc}}$ *and* $\text{Agr}(\alpha \wedge \beta) = (\text{Agr}(\alpha) \cup \text{Agr}(\beta))^{\text{tc}}$, *where W^{tc} denotes the transitive closure of $W \subseteq \Omega(n)$, in the sense that if (i, j), $(j, k) \in W$, then $(i, k) \in W$.*

(c) *For every n, S_n is an orthocomplemented, graded lattice.*

Proof. (a) and (b). If $(i, j), (j, k) \in \text{Inv}(\pi)$, then it is easy to see that $(i, k) \in \text{Inv}(\pi)$. Thus, $(\text{Inv}(\alpha) \cup \text{Inv}(\beta))^{\text{tc}} \subseteq \text{Inv}(\alpha \vee \beta)$. Similarly, $(\text{Agr}(\alpha) \cup \text{Agr}(\beta))^{\text{tc}} \subseteq \text{Agr}(\alpha \wedge \beta)$. Thus, we will only be concerned with proving the reverse inclusions.

The proof is by induction on n and is given only for $\alpha \vee \beta$. S_1 is clearly a lattice. Let $\pi^+ = CnC^\#$. Since $\alpha\hat{} \leq \pi$, $\mathrm{Inv}(\alpha\hat{}) \subseteq \mathrm{Inv}(\pi^+)$. Since $C^\#$ contains $A^\#$ it follows that $\mathrm{Inv}(\alpha) \subseteq \mathrm{Inv}(\pi^+)$. Thus, $\alpha \leq \pi^+$. Similarly, $\beta \leq \pi^+$. By the induction hypothesis, $\mathrm{Inv}(\pi) = (\mathrm{Inv}(\alpha\hat{}) \cup \mathrm{Inv}(\beta\hat{}))^{tc}$.

Now suppose that $\alpha, \beta \leq \sigma$. Since $\alpha\hat{}, \beta\hat{} \leq \sigma\hat{}$, it follows from the induction hypothesis that $\pi \leq \sigma\hat{}$. Thus, every inversion in π^+ not involving n is contained in σ. If $q \in A^\# \cup B^\#$, then (q, n) is an inversion in α or β and so must be an inversion in σ. Suppose that $q \in C^\# - A^\# \cup B^\#$. Since $C^\#$ is not empty, let t be the first element in $C^\#$. By the minimality of $C^\#$, t must be in either $A^\#$ or $B^\#$. We may assume that $t \in A^\#$. Thus, the inversion (t, n) is in α and hence in σ. If $t > q$, then (q, t) is an inversion in π^+ not involving n and must be an inversion in σ. Thus in σ, n is to the left of t and t is to the left of q, so n is to the left of q. This means that (q, n) is an inversion in σ. On the other hand, if $q > t$, then (t, q) must be an inversion in α since $q \not\in A^\#$ and $t \in A^\#$. If (t, q) is an inversion in α it must be an inversion in π^+, which contradicts the fact that t precedes q in π^+. Thus, we have shown that if $(q, n) \in \mathrm{Inv}(\pi^+)$, then $(q, n) \in \mathrm{Inv}(\sigma)$, so $\pi^+ \leq \sigma$.

To show that (b) holds, we need only consider pairs of the form (q, n) since (b) holds for π. The preceding paragraph proves that if $(q, n) \in \mathrm{Inv}(\pi^+)$ and $q \in C^\# - A^\# \cup B^\#$, then $t > q$. Since $t \in A^\#$, $(t, n) \in \mathrm{Inv}(\alpha)$. Since $(q, t) \in \mathrm{Inv}(\pi)$, by the induction hypothesis there is a chain $q = p_1 < p_2 < \cdots < p_{r-1} = t$ such that $(p_k, p_{k+1}) \in \mathrm{Inv}(\alpha\hat{}) \cup \mathrm{Inv}(\beta\hat{})$ for $i = 1, \ldots, r-2$. If we let $n = p_r$, then (b) holds.

(c) The orthogonal complement of $\alpha \in S_n$, $\alpha^\perp$, is its reversal. S_n is graded because if α covers β, α has one more inversion than β derived from swapping two elements that are adjacent in β. □

Theorem 1 can be used as a basis for a reasonably efficient algorithm for computing meets and joins in S_n that is described in detail in Theorem 2. Theorem 1 also shows that the map $\alpha \to \alpha\hat{}$ is a lattice epimorphism.

Theorem 2. *Let $\alpha, \beta \in S_n$. Then $\alpha \vee \beta$ ($\alpha \wedge \beta$) can be calculated as follows. Let π_1 (δ_1) be the string 1. Given the string π_i (δ_i) which consists of the integers in i, create the string $\pi_{i+1}(\delta_{i+1})$ by placing $i+1$ immediately to the left (right) of the leftmost (rightmost) element of $\pi_i(\delta_i)$ that follows (precedes) $i+1$ in either α or β, and to the right (left) of π_i (δ_i) if there does not exist such an element. The string $\pi_n = \alpha \vee \beta$ ($\delta_n = \alpha \wedge \beta$) and for each i, $\mathrm{Inv}(\pi_i) = \mathrm{Inv}(\alpha \vee \beta) \cap \Omega(i)$ ($\mathrm{Inv}(\delta_i) = \mathrm{Inv}(\alpha \wedge \beta) \cap \Omega(i)$).*

Proof. We will do the proof only for $\vee$, since the proof for $\wedge$ is similar. The following is clear from the proof of Theorem 1: when n is added to the string it must be to the left of all elements in $A^\# \cup B^\#$. At the same time, its immediate neighbor to the right in π_n must be an element of $A^\# \cup B^\#$. Thus, the algorithm for inserting n is to start at the left and let n drift to the right until it encounters the first element that must be to the right of it. □

Example 1. Let $\alpha = 3174652$ and $\beta = 4732651$. To compute $\alpha \vee \beta$ using the algorithm of Theorem 2 proceed as follows.

Step 1: π_1 is 1.
Step 2: $\pi_2 = 21$ since 2 comes before 1 in β.
Step 3: Since 3 comes before both 1 and 2 in both α and β, $\pi_3 = 321$.
Step 4: Since 4 precedes 3 in β, $\pi_4 = 4321$.
Step 5: Since 5 follows 3 and 4 in both α and β, but precedes 2 in α, $\pi_5 = 43521$.
Step 6: Since 6 follows 3 and 4 in both α and β, but precedes 5 in α, $\pi_6 = 436521$.
Step 7: Since 7 precedes 4 in α, π_7 is 7436521.

The algorithms presented in Theorem 2 takes time $O(n^2)$ and space $O(n)$. Theorem 2 can be extended to permutations on sets of the form $a, a+1, \ldots, b$ rather than just $1 \ldots i$. The statement and proof of this result are left as exercises for the reader. □

Definition 4. A lattice, L, is *meet-semidistributive* if and only for all $x, a, b \in L$, $x \wedge a = x \wedge b$ implies that $x \wedge (a \vee b) = x \wedge a$. *Join-semidistributivity* is defined dually, and a lattice is said to be *semidistributive* if it is both meet- and join-semidistributive.

Definition 5. In a lattice with a least element, a meet-pseudocomplement for an element, x, is an element y such that $x \wedge z = 0$ iff $z \leq y$. A join-pseudocomplement is defined dually. □

Remark 6. It is easy to see that if a finite lattice is semidistributive it is also pseudocomplemented. Furthermore, in a complemented lattice, a meet-pseudocomplement or a join-pseudocomplement must be a complement. □

Theorem 2 can be used to give a short, direct proof of the result of Duquenne and Cherfouh (1991) that S_n is semidistributive. In view of Remark 6, this also shows that it is pseudocomplemented, a result that Chameni–Nembua and Monjardet (1992) credit to personal communications from C. Le Conte de Poly-Barbut. Recently, Le Conte de Poly-Barbut (1992) has generalized the Duquenne and Cherfouh result and show that all finite Coxeter lattices are semidistributive.

In cases where α and β have certain structures it is possible to see that certain contiguous blocks of integers will pass unchanged into the meet or join of α and τ. This is illustrated in Theorem 3.

Theorem 3. *Suppose that $\alpha, \beta \in S_n$ are represented as strings of integers. Further, suppose that the representations have the forms $\alpha = L1\ M\ R1$ and $\beta = L2\ M\ R2$, where L1 and L2 contain exactly the same integers, but are not necessarily the same strings. Let $\delta = \alpha \wedge \beta$ and $\pi = \alpha \vee \beta$. Then $\delta = L3\ M\ R3$ and $\pi = L4\ M\ R4$, where*

L3 and L4 contain the same integers as L1 and L2, and R3 and R4 contain the same integers as R1 and R2.

Proof. The proof is by induction on n with the case $n = 1$ being trivial. We will just give the proof for $\alpha \wedge \beta$. First note that $\alpha\hat{} = P1\ Q\ T1$ and $\beta\hat{} = P2\ Q\ T2$, where $P1$ and $P2$, and $T1$ and $T2$ contain the same integers. By the inductive hypothesis it follows that $\alpha\hat{} \wedge \beta\hat{} = P3\ Q\ T3$, where $P3$ contains the same integers as $P1$ and $P2$, while $T3$ contains the same integers as $T1$ and $T2$. To construct $\alpha \wedge \beta$ it is necessary to insert n into the correct place in $\alpha\hat{} \wedge \beta\hat{}$. It is easy to see that n goes into $P3$ if $n \in L1 \cap L2$, n goes into Q if $n \in M$ and n goes into $T3$ if $n \in R1 \cap R2$. Thus δ has the structure $L3\ M\ R3$. □

Example 2. If $\alpha = 3274651$ and $\beta = 4732651$, we can apply Theorem 3 to see that the last three characters of δ must be 651. We need only calculate the meet of 3274 and 4732 which we can treat like 2143 and 3421 in S_4. After computing the meet in S_4 to get 2134 we convert back using the relations $1 \to 2$, $2 \to 3$, $3 \to 4$, and $4 \to 7$ to get 3247, so the final answer is 3247651. □

3. Calculating meets and joins in the Newman lattices

Bennett and Birkhoff (1990) describe a generalization of the positional ordering on permutations to *multi-permutations*, which are like permutations except that elements can be repeated. 12213 is an example of a multi-permutation. The algorithm of Section 2 can be used to compute the meets and joins of multi-permutations by converting the multi-permutations into permutations, using the algorithms and converting back. Converting between multi-permutations and permutations is used by Bennett and Birkhoff (1990) to prove that multi-permutations are sublattices of the permutation lattices.

The conversions can be done in linear time and space. For example, 12213 can be represented by the permutation 13425, where 1 and 2 represent the two 1's, 3 and 4 represent the two 2's and 5 represents the only 3. In fact, the lattice of all multi-permutations having two 1's, two 2's and one 3 is isomorphic to the interval (sublattice) [12345, 53412] of S_5. As long as the first 1 always comes before the second 1, etc. there is no ambiguity in converting between multi-permutations and permutations. Bennet and Birkhoff (1990) use the integers $m_1, m_2, \ldots, m_k$ to indicate the number of times $1, 2, \ldots, k$ appear in the multi-permutation.

4. Complements

Chameni-Nembua and Monjardet (1992, 1993) make some interesting observations about the structure of finite pseudocomplemented lattices and in particular about lattices that are also complemented. They show that in all such lattices, the

Glivenko congruence 'to have the same meet pseudocomplement' is the same as 'to have the same join pseudocomplement' is the same as 'to have the same complements'. The classes of this congruence are the 2^n intervals $[\vee A(x), \wedge C(x)]$, where $A(x) = \{\text{atoms } a \mid a \le x\}$ and $C(x) = \{\text{coatoms } c \mid c \ge x\}$, where n is the number of atoms or coatoms of L. In particular, it follows that the complements of an element form an interval with the top element being the meet pseudocomplement of x, x^*, while the bottom element is the join pseudocomplement of x, $x^\dagger$.

To apply these results to S_n requires showing that S_n is complemented and pseudocomplemented. It is easy to see that S_n is complemented. That S_n is pseudocomplemented follows from the fact, stated in Section 2, that S_n is semidistributive.

This section briefly sketches an alternative method for proving that S_n is pseudocomplemented, and gives some insight into the Glivenko interval structure of S_n and the process of computing pseudocomplements. The fact that the complements of an element in S_n form an interval was independently discovered by Markowsky (1990b).

Definition 6. An element, x, of a lattice, L, is said to be *coprime* (*prime*) if for all $y, z \in L$, $x \le y \vee z$ ($x \ge y \wedge z$) implies that $x \le y$ or $x \le z$ ($x \ge y$ or $x \ge z$). □

Theorem 5 of Markowsky (1992) states that a finite lattice is pseudocomplemented if and only if each atom is coprime and each coatom is prime.

Theorem 4. *Each atom of S_n is coprime and each coatom of S_n is prime. Furthermore, in S_n, I is the join of the atoms and O is the meet of the coatoms. Consequently, S_n is pseudocomplemented.*

Proof. The atoms of S_n are exactly the permutations of the form $12\ldots(q+1)\ q\ldots n$ which have exactly one inversion. The coatoms are reversals of the atoms. It is easy to see that the atoms are coprime since a pair $(q, q+1)$ can be in the transitive closure of a set of inversions if and only if it is in the original set. Similarly, the coatoms are prime. It follows easily from Theorem 2 that I is the join of the atoms and O the meet of the coatoms. □

The following material helps us describe how to compute the meet-pseudocomplement, σ^*, and the join-pseudocomplement, $\sigma^\dagger$, of an arbitrary permutation, σ.

Notation 3. Let $\sigma \in S_n$. Then $Comp(\sigma) = \{\tau \in S_n \mid \tau \wedge \sigma = O \text{ and } \tau \vee \sigma = I\}$. Also, $CInv(\sigma) = \{(i, i+1) \mid (i, i+1) \in \mathrm{Inv}(\sigma)\}$. CInv is shorthand for *consecutive inversions*. The symbol $C\Omega(n)$ will denote the set $\{(i, i+1) \mid i \in \boldsymbol{n-1}\}$. □

Theorem 5. *Let σ and τ belong to S_n, then* $\mathrm{CInv}(\sigma) \cap \mathrm{CInv}(\tau) = \mathrm{CInv}(\sigma \wedge \tau)$ *and*

$\mathrm{CInv}(\sigma) \cup \mathrm{CInv}(\tau) = \mathrm{CInv}(\sigma \vee \tau)$. *Thus,* $\tau \in \mathrm{Comp}(\sigma)$ *if and only if* $\mathrm{CInv}(\tau) = \mathrm{C}\Omega(n) - \mathrm{CInv}(\sigma)$.

Proof. Since no element can interpose between i and $i+1$, it follows from Theorem 1 that $(i, i+1) \in \mathrm{CInv}(\sigma \vee \tau)$ iff $(i, i+1) \in \mathrm{CInv}(\sigma) \cup \mathrm{CInv}(\tau)$. The result for $\wedge$ is dual. If $\tau \in \mathrm{Comp}(\sigma)$, then $\mathrm{CInv}(\sigma) \cup \mathrm{CInv}(\tau) = \mathrm{CInv}(n(n-1)\ldots 1) = \mathrm{C}\Omega(n)$ and $\mathrm{CInv}(\sigma) \cap \mathrm{CInv}(\tau) = \mathrm{CInv}(12\ldots(n-1)n) = \emptyset$, so $\mathrm{CInv}(\tau) = \mathrm{C}\Omega(n) - \mathrm{CInv}(\sigma)$. On the other hand, if $\mathrm{CInv}(\tau) = \mathrm{C}\Omega(n) - \mathrm{CInv}(\sigma)$, then $\mathrm{CInv}(\sigma \wedge \tau) = \emptyset$, so $\sigma \wedge \tau = 12\ldots(n-1)n$. Similarly, $\sigma \vee \tau = n(n-1)\ldots 21$. □

Corollary. *For all* $\sigma \in S_n$, $\mathrm{Comp}(\sigma)$ *is closed under meet and join. Thus,* $\mathrm{Comp}(\sigma)$ *is a sublattice of* S_n. *In fact,* $\mathrm{Comp}(\sigma) = [\sigma^*, \sigma^\dagger]$.

Proof. We will prove that $\mathrm{Comp}(\sigma)$ is closed under meet. The result for join is dual. Suppose $\alpha, \beta \in \mathrm{Comp}(\sigma)$. This means that $\mathrm{CInv}(\alpha) = \mathrm{CInv}(\beta) = \mathrm{C}\Omega(n) - \mathrm{CInv}(\sigma)$. From Theorem 5, it follows that $\mathrm{CInv}(\alpha \vee \beta) = \mathrm{CInv}(\alpha \wedge \beta) = \mathrm{C}\Omega(n) - \mathrm{CInv}(\sigma)$. Applying Theorem 5 again we see that $\alpha \vee \beta$, $\alpha \wedge \beta \in \mathrm{Comp}(\sigma)$.

Since $\mathrm{Comp}(\sigma)$ is a finite lattice it follows that it has a least element, $\sigma^\dagger$, and a greatest element, σ^*. It is routine to show that $\mathrm{Comp}(\sigma) = [\sigma^\dagger, \sigma^*]$, and that $\sigma^\dagger$ is join-pseudocomplement and σ^* the meet-pseudocomplement of σ. □

Remark 7. Theorem 5 gives the essential ideas needed for calculating $\sigma^\dagger$ and σ^*. It is enough to focus on calculating $\sigma^\dagger$ since $\sigma^* = \sigma^{\perp\dagger\perp}$. It is easy to see that $\sigma^\perp \in \mathrm{Comp}(\sigma)$. In general $\sigma^\dagger \le \sigma^\perp \le \sigma^*$, and all three complements are distinct.

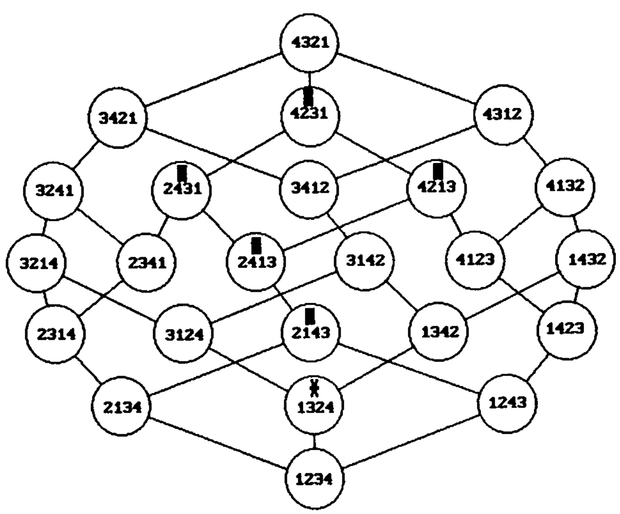

Fig. 1. The lattice S_4 showing the complements of 1324.

For example, $5376214^\perp = 4126735$, $5376214^\dagger = 1243657$ and $5376214^* = 6745123$.

$\sigma^\dagger$ is computed by starting with the identity permutation and making the smallest number of reversals that will yield a permutation π such that $\mathrm{CInv}(\pi) = \mathrm{C}\Omega(n) - \mathrm{CInv}(\sigma)$. To illustrate the algorithm let us consider finding $\sigma^\dagger$ and σ^* for $\sigma = 5376214$. $\mathrm{CInv}(\sigma) = \{(2,1), (3,2), (5,4), (7,6)\}$ so for any complement π, $\mathrm{CInv}(\pi) = \{(4,3), (6,5)\}$. To have the fewest reversed pairs we take 1234567 and reverse only what needs to be reversed. In this case just the pairs 34 and 56 must be reversed to yield 1243657. If $\mathrm{CInv}(\pi)$ was the set $\{(4,3), (5,4), (6,5)\}$ we would have to get a decreasing chain 654 since 6 comes before 5 and 5 comes before 4. In this case the least complement would be 1236547.

To compute σ^*, first compute $\alpha = \sigma^\perp = 4126735$. $\mathrm{CInv}(\alpha) = \{(4,3), (6,5)\}$ so for all $\beta \in \mathrm{Comp}(\alpha)$, $\mathrm{CInv}(\beta) = \{(2,1), (3,2), (5,4), (7,6)\}$. This means that $\alpha^\dagger = 3215476$, so $\sigma^* = \alpha^{\dagger\perp} = 6745123$. Fig. 1 shows the complements of 1324 in S_4.

5. Automorphisms and dual-automorphisms

Definition 7. Let the map $\Sigma: S_n \to S_n$ be given by $(\Sigma(\sigma))(i) = (n+1) - \sigma(i)$. □

Notation 4. For convenience, in this section we will use the function symbol R instead of $^\perp$. Note that for all $\sigma \in S_n$, $(R(\sigma))(i) = \sigma(n+1-i)$ for all $i \in \boldsymbol{n}$. □

This section examines the automorphisms and dual-automorphisms (involutions in the sense of Birkhoff, 1967, p. 3) of S_n and shows that the automorphism group is the two-element group. This result is attributed to Anders Björner by Kung and Sutherland (1988), but to the best of my knowledge, Björner has never published this result. This result was also independently published by Le Conte de Poly-Barbut (1990a). Since my proof, which first appeared in Markowsky (1990b), follows a similar strategy to his, I will omit many of the details. Kung and Sutherland (1988) contains a determination of the automorphism of the permutations under the strong Bruhat ordering. Le Conte de Poly-Barbut (1990b) contains a description of the permutation lattice as the intersection of two direct products of linear orders.

To analyze the automorphisms and dual automorphisms of S_n, the first step is to show that R and Σ are involutions such that $R\Sigma = \Sigma R$, or $R\Sigma$ is an automorphism of order 2. We will show that the group $\{Id, R, \Sigma, R\Sigma\}$ is the Klein 4-group where every non-identity has period 2, and is the complete group of automorphisms and dual-automorphisms of the lattice S_n for $n > 2$. Lemma 1 presents some properties of the map Σ that will be useful later. Its proof is left to the reader.

Lemma 1. $\mathrm{Inv}(\Sigma(\sigma)) = \{(i, j) \mid j > i,\ j,\ i \in \boldsymbol{n},$ *and* $(n+1-j,\ n+1-i) \in \mathrm{Agr}(\sigma)\} = \{(n+1-b,\ n+1-a) \mid b > a,\ a,\ b \in \boldsymbol{n},$ *and* $(a, b) \in \mathrm{Agr}(\sigma)\}$. □

Theorem 6.

(a) *Σ is an involution.*

(b) *For all $\sigma \in S_n$, $\Sigma(R(\sigma)) = R(\Sigma(\sigma))$.*

(c) *For $n \geq 3$, $R\Sigma$ is an automorphism of degree 2.*

(d) *For $n \geq 3$, S_n has exactly two automorphisms: identity and $R\Sigma$. For $n \leq 2$, S_n has exactly one automorphism.*

(e) *For $n \geq 3$, S_n has only two dual automorphisms: R and Σ. For $n \leq 2$, S_n has exactly one dual automorphism.*

Proof. (a) From Lemma 1 it follows that $\sigma \leq \pi$ if and only if $\text{Inv}(\sigma) \subseteq \text{Inv}(\pi)$ if and only if $\text{Inv}(\Sigma(\sigma)) \supseteq \text{Inv}(\Sigma(\pi))$ if and only if $\Sigma(\sigma) \geq \Sigma(\pi)$. This shows that Σ is a dual automorphism. $(\Sigma(\Sigma(\sigma)))(i) = n+1-(\Sigma(\sigma))(i) = n+1-(n+1-\sigma(i)) = \sigma(i)$ for all i, so $\Sigma(\Sigma(\sigma)) = \sigma$.

(b) $(\Sigma(R(\sigma)))(i) = n+1-(R(\sigma))(i) = n+1-\sigma(n+1-i)$. $(R(\Sigma(\sigma))(i) = (\Sigma(\sigma))(n+1-i) = n+1-\sigma(n+1-i)$.

(c) Part (b) implies that $R\Sigma R\Sigma = R\Sigma\Sigma R = RR = \text{identity}$. For $n \geq 3$, $R\Sigma \neq$ identity since $R\Sigma(2134\ldots n) = R((n-1)n(n-2)\ldots 1) = 1\ldots(n-2)n(n-1) \neq 2134\ldots n$.

(d) For $n \leq 2$, the result is trivial. For $n \geq 3$, part (c) shows that there are at least two automorphisms. That there are only two is shown below in a series of lemmas.

(e) For $n \leq 2$, the result is trivial. For $n \geq 3$, proceed as follows. Since R is a dual automorphism, it follows that if Γ is a dual automorphism, $R\Gamma$ is an automorphism. From part (d), $R\Gamma = \text{identity}$ or $R\Sigma$. Since $R = R^{-1}$, this means that $\Gamma = R$ or Σ. □

The proof of Theorem 6(d) uses the following observations about any automorphism Γ of S_n:

(1) It must preserve height. *ht*(σ) will denote the height of σ in S_n.

(2) If $\sigma \in S_n$, then $\text{ht}(\sigma^{\dagger}) = \text{ht}(\Gamma(\sigma)^{\dagger})$.

(3) If $\sigma \in S_n$ is join-irreducible, then $\Gamma(\sigma)$ is join-irreducible.

The proof of Theorem 6(d) first shows that all automorphisms behave either like the identity or $R\Sigma$ on the individual atoms of S_n. Next it extends this result to the set of all atoms considered as an ordered structure. Finally, it shows that the result holds for S_n.

Lemma 2. *Let $\Gamma: S_n \to S_n$ be an automorphism and let $\alpha \in S_n$ be an atom. Then $\Gamma(\alpha) = \alpha$ or $\Gamma(\alpha) = R(\Sigma(\alpha))$.*

Proof. If α is an atom, then $\exists k \in \boldsymbol{n-1}$ such that $\alpha = 12\ldots(k-1)(k+1)k(k+2)\ldots n$. Thus, $\alpha^{\dagger} = k\ldots 1n\ldots(k+1)$, so $\text{ht}(\alpha^{\dagger}) = |\text{Inv}(\alpha^{\dagger})| = \text{BIN}(k,2) + \text{BIN}(n-k,2)$, where $\text{BIN}(p,q)$ is the binomial coefficient giving the number of q element subsets of a p element set. Since $\text{ht}(\alpha^{\perp})$ is quadratic in k, there are at most two values of k that produce the same height for $\alpha^{\dagger}$. When $k \neq n/2$, the two values are k and $n-k$. When $k = n/2$, height has a unique minimum at $n/2$.

Now let $\mu = R(\Sigma(\alpha))$. Since $R\Sigma$ is an automorphism, $\text{ht}(\mu^{\dagger}) = \text{ht}(\alpha^{\dagger})$. If $k \neq n/2$, $\mu \neq \alpha$, while if $k = n/2$, $\mu = \alpha$. If n is even, $k = n/2$ is a possible value and the α corresponding to this value of k is invariant under all automorphisms since $\text{ht}(\alpha^{\dagger})$ is less than *ht*$(\beta^{\dagger})$, where β is any other atom. The element 1324 is this unique element in Fig. 1. Since an automorphism must preserve $\text{ht}(\alpha^{\dagger})$, it follows that for any automorphism Γ, $\Gamma(\alpha) = \alpha$ or $R(\Sigma(\alpha))$. □

Lemma 3. *Let $\Gamma: S_n \to S_n$ be an automorphism. Then $\Gamma \mid \text{Atoms} = \text{identity}$ or $R\Sigma$.*

Proof. Let $\alpha = 1\ldots(a-1)(a+1)a(a+2)\ldots n$ and $\beta = 1\ldots(b-1)(b+1)b(b+2)\ldots n$ be atoms. Let $\pi = \alpha \vee \beta$. Without loss of generality we may assume that $a < b$. It is easy to see that π can have one of two forms. If $a < b-1$, $\pi = 1\ldots(a-1)(a+1)a(a+2)\ldots(b-1)(b+1)b(b+2)\ldots n$, while if $a = b-1$, $\pi = 1\ldots(b-2)(b+1)b(b-1)(b+2)\ldots n$. In the first case $\text{ht}(\pi) = 2$ while in the second case $\text{ht}(\pi) = 3$.

The sequence $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$, where $\alpha_i = 1\ldots(i-1)(i+1)i(1+2)\ldots n$, has the following properties:

(1) $\text{ht}(\alpha_i \vee \alpha_j) = 3$ if and only if $|i-j| = 1$.

(2) $R(\Sigma(\alpha_i)) = \alpha_{n-i}$.

(3) Every atom appears in the sequence.

If Γ is an automorphism of S_n, the sequence $\Gamma(\alpha_1), \Gamma(\alpha_2), \ldots, \Gamma(\alpha_{n-1})$ must have properties (1) and (3). From Lemma 2 we know that $\Gamma(\alpha_1) = \alpha_1$ or $R(\Sigma(\alpha_1)) = \alpha_{n-1}$. If $\Gamma(\alpha_1) = \alpha_1$, properties (1) and (3) require that $\Gamma(\alpha_2) = \alpha_2, \ldots, \Gamma(\alpha_{n-1}) = \alpha_{n-1}$, so $\Gamma = \text{identity}$ in this case. If $\Gamma(\alpha_1) = \alpha_{n-1}$, then properties (1) and (3) imply that $\Gamma(\alpha_i) = \alpha_{n-i} = R(\Sigma(\alpha_i))$ for all i, so $\Gamma = R\Sigma$ in this case. □

Lemma 4. *Let $\sigma \in S_n$.*

(1) *If σ is not an atom, then σ can be covered by at most one join-irreducible element.*

(2) *If σ is an atom, then σ is covered by two join-irreducible elements if and only if there exists $k > 0$ such that $\sigma = 1\ldots k(k+2)(k+1)(k+3)\ldots n$ and $k+3 \leq n$.*

(3) *If σ is an atom and σ does not have the form described in* (2), *σ is covered by a unique join-irreducible element.*

(4) *O is covered by $n-1$ join-irreducible elements.*

Proof. Part (4) is easy since the $n-1$ join-irreducibles covering $12\ldots n$ are the permutations of the form $1\ldots(a-1)(a+1)a(a+2)\ldots n$ for $a \in \boldsymbol{n-1}$.

Bennett and Birkhoff (1990) established that β covers α iff we can swap an adjacent pair of elements ji with $j > i$. We call a consecutive pair of integers in the string representation of a permutation an *increasing adjacent pair* if the second number is greater than the first and a *decreasing adjacent pair* if the second number is less than the first. For example, in the permutation 2143, 21 and 43 are decreasing adjacent pairs, while 14 is an increasing adjacent pair.

A permutation β can be a join-irreducible if and only if there is just one decreasing adjacent pair in its string representation. In particular, if β is a join-irreducible in S_n it must have the form $a_1a_2 \ldots a_pb_1b_2 \ldots b_q$, where $p+q=n$, $a_1<a_2<a_3<\cdots<a_{p-1}<a_p>b_1<b_2<\cdots<b_{q-1}<b_q$.

If $n \geq 3$ and $\mathrm{ht}(\sigma)=1$, σ must have the form $1 \ldots (i+1)i(i+2) \ldots n$ and $\pi = 1 \ldots (i+1)(i+2)i \ldots n$ is a join-irreducible that covers σ. Thus, all atoms are covered by at least one join-irreducible.

The element α covered by a join-irreducible β must have the form $a_1 \ldots a_{p-1}b_1a_pb_2b_3 \ldots b_q$. There are four cases to consider: $a_{p-1}<b_1$ and $a_p<b_2$; $a_{p-1}<b_1$ and $a_p>b_2$; $a_{p-1}>b_1$ and $a_p<b_2$; and $a_{p-1}>b_1$ and $a_p>b_2$. Careful analysis of these four cases establishes the claims made by this lemma. □

Proof of Theorem 6(d). Let Γ be any automorphism of S_n. By Lemma 3 Γ is either the identity or $R\Sigma$ on the atoms. I will now sketch the proof that if Γ is the identity on the atoms, then Γ = identity on S_n. The same proof shows that if Γ is $R\Sigma$ on the atoms, then $\Gamma = R\Sigma$ on S_n.

The proof proceeds by induction on the height of the elements being considered. From Lemma 4, it follows that if $\mathrm{ht}(\sigma)=k$, then one of the following three cases must hold:

(a) $\sigma = \alpha \vee \beta$, where $\mathrm{ht}(\alpha)<\mathrm{ht}(\sigma)$ and $\mathrm{ht}(\beta)<\mathrm{ht}(\sigma)$.

(b) σ is the unique join-irreducible covering α, where $\mathrm{ht}(\alpha)=\mathrm{ht}(\sigma)-1$.

(c) σ is one of two join-irreducibles covering α, where $k=2$ and $\mathrm{ht}(\alpha)=\mathrm{ht}(\sigma)-1=1$.

It is easy to see that in cases (a) and (b), Γ must be the identity on σ as well. From Lemma 4, case (c) happens only if α has the form $1 \ldots p(p+2)(p+1)(p+3) \ldots n$, and the two join-irreducibles must have the forms $1 \ldots (p-1)(p+2)p(p+1)(p+3) \ldots n$ and $1 \ldots p(p+2)(p+3)(p+1)(p+4) \ldots n$. There is no loss of generality in assuming that σ is the first of the join-irreducibles and π is the second. Since $\mathrm{ht}(\alpha)=1$, $\Gamma(\alpha)=\alpha$ by our initial assumption.

Let $\mu = 1 \ldots (p-1)(p+1)p(p+2) \ldots n$. Since $\mathrm{ht}(\mu)=1$, $\Gamma(\mu)=\mu$. Now $\sigma \vee \mu = 1 \ldots (p-1)(p+2)(p+1)p(p+3) \ldots n$ which has height 3. On the other hand, $\pi \vee \mu = 1 \ldots (p-1)(p+2)(p+3)(p+1)p(p+4) \ldots n$ which has height 5. Since Γ must preserve height, $\Gamma(\sigma)=\sigma$ and $\Gamma(\pi)=\pi$. This proves that Γ is the identity on elements of height k. □

6. Poset of irreducibles

The poset of irreducibles, which is discussed in detail in Markowsky (1975), provides much information about a lattice. Bennett and Birkhoff (1990) determine the poset of irreducibles of the Tamari associativity lattices, and we will now determine the poset of irreducibles of S_n. Since we are working only with finite lattices, Definition 8 provides just what is needed in this case. For additional information, see Markowsky (1975).

Definition 8. Let L be a finite lattice. Its poset of irreducibles is the bipartite graph $(J(L), M(L), \mathrm{Arcs}(L))$, where $J(L)$ are the join-irreducibles of L, $M(L)$ are the meet-irreducibles of L and we have an arc from $j \in J(L)$ to $m \in M(L)$ if and only if $j \not\leq m$. Any $x \in J(L) \cap M(L)$ is represented by two distinct nodes, one in $J(L)$ and one in $M(L)$. □

Theorem 7. *The join-irreducibles of S_n correspond uniquely to pairs of subsets of **n**, (A, B), where A and B are complements and $A \neq i$ for all i. Similarly, the meet-irreducibles of S_n correspond uniquely to pairs of subsets of **n**, (C, D), where C and D are complements and $D \neq i$ for all i.*

Let j be a join-irreducible of S_n represented by (A, B), and m be a meet-irreducible of S_n represented by (C, D). We have that $j \not\leq m$ if and only if $\max(A \cap D) > \min(B \cap C)$.

Proof. As noted by Bennett and Birkhoff (1990, Theorem 7) and above, join-irreducibles must look like $a_1<a_2<\cdots<a_k>b_1<b_2<\cdots<b_{n-k}$, while meet-irreducibles must look like $c_1>c_2>\cdots>c_p<d_1>d_2>\cdots>d_{n-p}$. It is clear that $A=\{a_1, a_2, \ldots, a_k\}$ and $B=\{b_1, b_2, \ldots, b_{n-k}\}$. Given A there is only one way to order the elements in A and B so the representation is unique. The result for meet-irreducibles is dual.

Now $j \not\leq m$ if and only if there exist $(q, r) \in \mathrm{Inv}(j)$ such that $(q, r) \not\in \mathrm{Inv}(m)$. This can happen if and only if $q \in A$, $r \in B$, $q>r$, $q \in D$ and $r \in C$ in which case $q \in A \cap D$, $r \in B \cap C$ and $\max(A \cap D) \geq q > r \geq \min(B \cap C)$. On the other hand, if $\max(A \cap D) > \min(B \cap C)$, then both $A \cap D$ and $B \cap C$ are non-empty since $\max(\emptyset)=1$ and $\min(\emptyset)=n$. Let $q=\max(A \cap D)$ and $r=\min(B \cap C)$. It is easy to see that $(q, r) \in \mathrm{Inv}(j)$ but $(q, r) \not\in \mathrm{Inv}(m)$ so that $j \not\leq m$. □

7. Programs

Markowsky (1990a, 1990b) include BASIC programs for computing joins and meets, translating between permutations and multi-permutations, and computing pseudo-complements. These have been omitted from this paper, but are available from the author.

Acknowledgements

I wish to thank M.K. Bennett and G. Birkhoff for interesting me in the lattice of permutations and for many stimulating and helpful discussions and letters on the subject. I would also like to thank B. Monjardet and R. Stanley for some helpful references. Finally, I would like to thank the referees for their many valuable suggestions.

References

Many of the results in this paper were first presented at the 'Special Session on Lattices, Geometry and Combinatorics' of the AMS Meeting in Amherst, Massachusetts (20–21 October, 1990) and circulated in preprint form in Markowsky (1990a, b).

M.K. Bennett and G. Birkhoff, Two families of Newman lattices, preprint (1990), to appear in Algebra Universalis.

G. Birkhoff, Lattice Theory, 3rd edn. (American Mathematical Society, Providence, RI, 1967).

A. Björner, Orderings of Coxeter groups, in: C. Greene, ed., Combinatorics and Algebra (Contemporary Mathematics vol. 34) (American Mathematical Society, Providence, RI, 1984) pp. 175–184.

A. Björner, Weak orders of Coxeter groups. Referenced in Kung and Sutherland (1988), but to the best of my knowledge this has never appeared in print.

A. Björner and M.L. Wachs, Generalized quotients in Coxeter groups, Trans. Amer. Math. Soc. 308 (1988) 1–37.

C. Chameni-Nembua and B. Monjardet, Les trellis pseudocomplémentés finis, Europ. J. Combinatorics 13 (1992) 89–107.

C. Chameni-Nembua and B. Monjardet, Finite pseudocomplemented lattices and 'permutoedre', Discrete Mathematics 111 (1993) 105–112.

V. Duquenne and A. Cherfouh, On the permutation lattice, Report P.077, Centre d'Analyse et de Mathématique Sociales, Paris (1991).

G. Th. Guilbaud and P. Rosenstiehl, L'analyse algébrique d'un scrutin, Mathématiques et Sciences Humaines 4 (1963) 9–33.

J.E. Humphreys, Reflection Groups and Coxeter Groups (Cambridge University Press, Cambridge, 1990).

J.P.S. Kung and D.C. Sutherland, The automorphism group of the strong order of the symmetric group, J. London Math. Soc. 37 (1988) 193–202.

C. Le Conte de Poly-Barbut, Automorphismes du permutoèdre et votes de Condorcet, Math. Inf. Sci. Hum. 28 (1990a) 73–82.

C. Le Conte de Poly-Barbut, Le diagramme du treillis permutoèdre est intersection des diagrammes de deux produits directs d'ordres totaux, Math. Inf. Sci. Hum. 28 (1990b) 49–53.

C. Le Conte de Poly-Barbut, Sur le treillis de Coxeter finis, Report P.079, Centre d'Analyse et de Mathématique Sociales, Paris (1992).

G. Markowsky, The factorization and representation of lattices, Trans. Amer. Math. Soc. 203 (1975) 185–200.

G. Markowsky, Computing meets and joins of permutations, Report 90-4, University of Maine, Computer Science Department, Orono, ME (1990a).

G. Markowsky, Involutions, automorphisms and complements in the lattice of permutations, Report 90-5, University of Maine, Computer Science Department, Orono, ME (1990b).

G. Markowsky, Primes, irreducibles and extremal lattices, Order 9 (1992) 265–290.

T. Yanagimoto and M. Okamoto, Partial orderings of permutations and monotonicity of a rank correlation statistic, Ann. Inst. Statist. Math. 21 (1969) 489–506.