Permutation groups, partitions, and the Krasner–Kaloujnine theorem

Peter J. Cameron
University of St Andrews
with Marina Anagnostopoulou-Merkouri (Bristol) and
R. A. Bailey (St Andrews)

Mathematics and Statistics Research Day
University of St Andrews, 23 January 2025

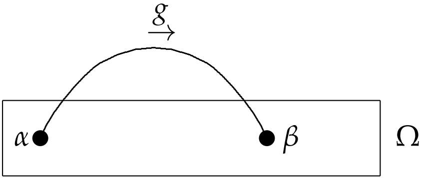
Transitive groups and invariant partitions

This is my favourite set-up. Ω is a set, and G is a group of permutations on Ω (bijective maps from Ω to Ω). The degree of G is the cardinality of Ω.

Ω

Transitive groups and invariant partitions

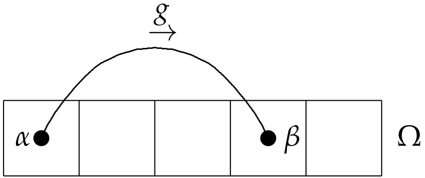
This is my favourite set-up. Ω is a set, and G is a group of permutations on Ω (bijective maps from Ω to Ω). The degree of G is the cardinality of Ω.



The action of G on Ω is transitive if, for any two points α and β in Ω, there is an element $g \in G$ which maps α to β.

Transitive groups and invariant partitions

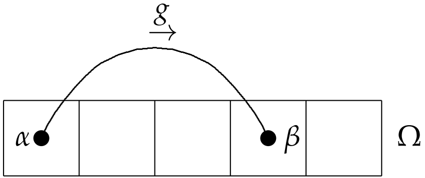
This is my favourite set-up. Ω is a set, and G is a group of permutations on Ω (bijective maps from Ω to Ω). The degree of G is the cardinality of Ω.



The action of G on Ω is transitive if, for any two points α and β in Ω, there is an element $g \in G$ which maps α to β.
A partition Π of Ω is invariant under G if elements of G map parts of Π to parts of Π. If g maps α to β then it maps the part containing α to the part containing β.

Transitive groups and invariant partitions

This is my favourite set-up. Ω is a set, and G is a group of permutations on Ω (bijective maps from Ω to Ω). The degree of G is the cardinality of Ω.



The action of G on Ω is transitive if, for any two points α and β in Ω, there is an element $g \in G$ which maps α to β.
A partition Π of Ω is invariant under G if elements of G map parts of Π to parts of Π. If g maps α to β then it maps the part containing α to the part containing β.
If G is transitive and Π is invariant under G, then all parts of Π must have the same number of points: we say that Π is uniform.

A construction

In this situation, we can define two smaller permutation groups, each acting transitively:

A construction

In this situation, we can define two smaller permutation groups, each acting transitively:

- G_1, the group of permutations induced on a part of Π by the subgroup of G fixing it;

A construction

In this situation, we can define two smaller permutation groups, each acting transitively:

- G_1, the group of permutations induced on a part of Π by the subgroup of G fixing it;
- G_2, the group of permutations induced on the set of parts of Π by G.

A construction

In this situation, we can define two smaller permutation groups, each acting transitively:

- G_1, the group of permutations induced on a part of Π by the subgroup of G fixing it;
- G_2, the group of permutations induced on the set of parts of Π by G.

Construction

Let Π be a uniform partition of Ω. Let G_1 be a transitive permutation group whose degree is the size of a part of Π, and G_2 a transitive permutation group whose degree is the number of parts of Π. Now build a group G as follows: G is generated by

A construction

In this situation, we can define two smaller permutation groups, each acting transitively:

- G_1, the group of permutations induced on a part of Π by the subgroup of G fixing it;
- G_2, the group of permutations induced on the set of parts of Π by G.

Construction

Let Π be a uniform partition of Ω. Let G_1 be a transitive permutation group whose degree is the size of a part of Π, and G_2 a transitive permutation group whose degree is the number of parts of Π. Now build a group G as follows: G is generated by

- *permutations of Ω fixing every part of Π and acting on each part as an element of G_1;*

A construction

In this situation, we can define two smaller permutation groups, each acting transitively:

- G_1, the group of permutations induced on a part of Π by the subgroup of G fixing it;
- G_2, the group of permutations induced on the set of parts of Π by G.

Construction

Let Π be a uniform partition of Ω. Let G_1 be a transitive permutation group whose degree is the size of a part of Π, and G_2 a transitive permutation group whose degree is the number of parts of Π. Now build a group G as follows: G is generated by

- *permutations of Ω fixing every part of Π and acting on each part as an element of G_1;*
- *permutations moving the parts of Π around as elements of G_2.*

A construction

In this situation, we can define two smaller permutation groups, each acting transitively:

- G_1, the group of permutations induced on a part of Π by the subgroup of G fixing it;
- G_2, the group of permutations induced on the set of parts of Π by G.

Construction

Let Π be a uniform partition of Ω. Let G_1 be a transitive permutation group whose degree is the size of a part of Π, and G_2 a transitive permutation group whose degree is the number of parts of Π. Now build a group G as follows: G is generated by

- *permutations of Ω fixing every part of Π and acting on each part as an element of G_1;*
- *permutations moving the parts of Π around as elements of G_2.*

This group is the wreath product of G_1 and G_2, denoted by $G_1 \wr G_2$.

A theorem

Note that in this construction, Ω is bijective with $\Omega_1 \times \Omega_2$.

A theorem

Note that in this construction, Ω is bijective with $\Omega_1 \times \Omega_2$.

The Krasner–Kaloujnine theorem asserts the following:

A theorem

Note that in this construction, Ω is bijective with $\Omega_1 \times \Omega_2$.

The Krasner–Kaloujnine theorem asserts the following:

Theorem

Let G be a transitive permutation group on Ω, having an invariant partition of Π. Let G_1 be the group induced on a part of Π by its setwise stabiliser, and G_2 the group induced on the set of parts by G. Then G is naturally embedded as a subgroup of $G_1 \wr G_2$.

The lattice of partitions

Let Π_1 and Π_2 be partitions. We say that Π_1 refines Π_2 if every part of Π_1 is contained in a part of Π_2 (written $\Pi_1 \preceq \Pi_2$).

The lattice of partitions

Let Π_1 and Π_2 be partitions. We say that Π_1 refines Π_2 if every part of Π_1 is contained in a part of Π_2 (written $\Pi_1 \preceq \Pi_2$). This is a partial order, and in fact a lattice: infima or meets (greatest lower bounds) and suprema or joins (least upper bounds) exist. The infimum of two partitions is the partition whose parts are all non-empty intersections of a part of the first with a part of the second. The supremum is a little more complicated to define but I will not need it.

The lattice of partitions

Let Π_1 and Π_2 be partitions. We say that Π_1 refines Π_2 if every part of Π_1 is contained in a part of Π_2 (written $\Pi_1 \preceq \Pi_2$).
This is a partial order, and in fact a lattice: infima or meets (greatest lower bounds) and suprema or joins (least upper bounds) exist. The infimum of two partitions is the partition whose parts are all non-empty intersections of a part of the first with a part of the second. The supremum is a little more complicated to define but I will not need it.
The infimum and supremum of two partitions Π_1 and Π_2 are denoted $\Pi_1 \wedge \Pi_2$ and $\Pi_1 \vee \Pi_2$ respectively.

The lattice of partitions

Let Π_1 and Π_2 be partitions. We say that Π_1 refines Π_2 if every part of Π_1 is contained in a part of Π_2 (written $\Pi_1 \preceq \Pi_2$).
This is a partial order, and in fact a lattice: infima or meets (greatest lower bounds) and suprema or joins (least upper bounds) exist. The infimum of two partitions is the partition whose parts are all non-empty intersections of a part of the first with a part of the second. The supremum is a little more complicated to define but I will not need it.
The infimum and supremum of two partitions Π_1 and Π_2 are denoted $\Pi_1 \wedge \Pi_2$ and $\Pi_1 \vee \Pi_2$ respectively.
The partitions invariant under any group form a lattice.

Commmuting partitions

Another structure on partitions comes from noting that each partition Π is defined by an equivalence relation R; we will say that partitions commute if the corresponding equivalence relations do, in the sense that $R_1 \circ R_2 = R_2 \circ R_1$, where

$$R_1 \circ R_2 = \{(\alpha, \gamma) : (\exists \beta)(\alpha, \beta) \in R_1, (\beta, \gamma) \in R_2\}.$$

This notion is important in statistics since it means that the factors corresponding to the two partitions are statistically orthogonal, which makes the analysis much easier.

Distributive lattices

We will be interested in lattices that satisfy the distributive laws, the following (equivalent) statements:

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c), \qquad (a \wedge b) \vee c = (a \vee c) \wedge (b \vee c).$$

Distributive lattices

We will be interested in lattices that satisfy the distributive laws, the following (equivalent) statements:

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c), \qquad (a \wedge b) \vee c = (a \vee c) \wedge (b \vee c).$$

The structure theorem for these asserts that any finite distributive lattice Λ is embeddable in the Boolean lattice of subsets of a set; more exactly, there is a poset (partially ordered set) $(\mathcal{P}, \sqsubseteq)$ such that Λ is isomorphic to the lattice of down-sets (sets closed downwards) of $\mathcal{P}$.

Distributive lattices

We will be interested in lattices that satisfy the distributive laws, the following (equivalent) statements:

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c), \qquad (a \wedge b) \vee c = (a \vee c) \wedge (b \vee c).$$

The structure theorem for these asserts that any finite distributive lattice Λ is embeddable in the Boolean lattice of subsets of a set; more exactly, there is a poset (partially ordered set) $(\mathcal{P}, \sqsubseteq)$ such that Λ is isomorphic to the lattice of down-sets (sets closed downwards) of $\mathcal{P}$.
In the other direction, $\mathcal{P}$ is the subset of join-indecomposable elements of Λ (those which cannot be written as the join of smaller elements).

Distributive lattices and poset block structures

Now given a poset $\mathcal{P}$, suppose that a set Ω_p of size greater than 1 is associated with each point $p \in \mathcal{P}$.

Distributive lattices and poset block structures

Now given a poset $\mathcal{P}$, suppose that a set Ω_p of size greater than 1 is associated with each point $p \in \mathcal{P}$.

Let us suppose that we have a group G_p acting transitively on Ω_p for each $p \in P$. Then there is a construction called the generalized wreath product, first described by Charles Holland, which produces a permutation group G on the Cartesian product Ω of the sets Ω_p over $p \in P$. Unfortunately, it is too complicated to describe here.

Distributive lattices and poset block structures

Now given a poset $\mathcal{P}$, suppose that a set Ω_p of size greater than 1 is associated with each point $p \in \mathcal{P}$.

Let us suppose that we have a group G_p acting transitively on Ω_p for each $p \in P$. Then there is a construction called the generalized wreath product, first described by Charles Holland, which produces a permutation group G on the Cartesian product Ω of the sets Ω_p over $p \in P$. Unfortunately, it is too complicated to describe here.

Note that, if $\mathcal{P}$ is a 2-element chain, then the g.w.p is just the wreath product defined earlier, while if $\mathcal{P}$ is a 2-element antichain then the g.w.p is the direct product.

Corresponding to each element $\lambda \in \Lambda$, the lattice of down-sets in $\mathcal{P}$, we have a partition Π_λ of Ω; and these partitions commute pairwise.

Distributive lattices and poset block structures

Now given a poset $\mathcal{P}$, suppose that a set Ω_p of size greater than 1 is associated with each point $p \in \mathcal{P}$.

Let us suppose that we have a group G_p acting transitively on Ω_p for each $p \in P$. Then there is a construction called the generalized wreath product, first described by Charles Holland, which produces a permutation group G on the Cartesian product Ω of the sets Ω_p over $p \in P$. Unfortunately, it is too complicated to describe here.

Note that, if $\mathcal{P}$ is a 2-element chain, then the g.w.p is just the wreath product defined earlier, while if $\mathcal{P}$ is a 2-element antichain then the g.w.p is the direct product.

Corresponding to each element $\lambda \in \Lambda$, the lattice of down-sets in $\mathcal{P}$, we have a partition Π_λ of Ω; and these partitions commute pairwise.

A structure like this (a distributive lattice of pairwise commuting uniform partitions) is known to statisticians as a poset block structure.

The main theorem

Our main theorem generalizes the Krasner–Kaloujnine theorem.

Theorem

Suppose that G is a permutation group on Ω, which has a set of invariant partitions forming a poset block structure; let $\mathcal{P}$ be the corresponding poset.
Then it is possible to extract a group G_p for every $p \in \mathcal{P}$ such that G is naturally embedded in the generalized wreath product of the groups G_p over $p \in \mathcal{P}$.

The main theorem

Our main theorem generalizes the Krasner–Kaloujnine theorem.

Theorem

Suppose that G is a permutation group on Ω, which has a set of invariant partitions forming a poset block structure; let $\mathcal{P}$ be the corresponding poset.
Then it is possible to extract a group G_p for every $p \in \mathcal{P}$ such that G is naturally embedded in the generalized wreath product of the groups G_p over $p \in \mathcal{P}$.

Two closing remarks:

The main theorem

Our main theorem generalizes the Krasner–Kaloujnine theorem.

Theorem

Suppose that G is a permutation group on Ω, which has a set of invariant partitions forming a poset block structure; let $\mathcal{P}$ be the corresponding poset.
Then it is possible to extract a group G_p for every $p \in \mathcal{P}$ such that G is naturally embedded in the generalized wreath product of the groups G_p over $p \in \mathcal{P}$.

Two closing remarks:

1. There is some subtlety in the construction of the groups G_p; the straightforward construction in the Krasner–Kaloujnine theorem does not work.

The main theorem

Our main theorem generalizes the Krasner–Kaloujnine theorem.

Theorem

Suppose that G is a permutation group on Ω, which has a set of invariant partitions forming a poset block structure; let $\mathcal{P}$ be the corresponding poset.
Then it is possible to extract a group G_p for every $p \in \mathcal{P}$ such that G is naturally embedded in the generalized wreath product of the groups G_p over $p \in \mathcal{P}$.

Two closing remarks:

1. There is some subtlety in the construction of the groups G_p; the straightforward construction in the Krasner–Kaloujnine theorem does not work.
2. We cannot weaken the hypotheses of the theorem. Even deleting "distributive" in the definition of a poset block structure (giving a more general class of objects called orthogonal block structures in statistics) does not work.