# Constructing transitive permutation groups of fixed degree

Alexander Hulpke

Department of Mathematics

Colorado State University

Fort Collins, CO 80523, USA

hulpke@math.colostate.edu

**http://www.math.colostate.edu/~hulpke**

September 2001

# The problem

Prize question (1858) of the Académie des Sciences:

**GRAND PRIX DE MATHEMATIQUES,**

PROPOSÉ POUR 1847, PUIS POUR 1854, REMIS A 1857, ET PROROGÉ JUSQU'EN 1860.

(Commissaires, MM. Liouville, Lamé, Duhamel, Cauchy, Bertrand rapporteur.)

variables de toutes les manières possibles. Il existe sur ce sujet des théorèmes remarquables qui suffisent aux applications de cette théorie à la démonstration de l'impossibilité de la résolution par radicaux d'une équation de degré supérieur à quatre ; mais la question générale qu'il faudrait résoudre serait la suivante :

« *Quels peuvent être les nombres de valeurs des fonctions bien définies qui* » *contiennent un nombre donné de lettres, et comment peut-on former les* » *fonctions pour lesquelles il existe un nombre donné de valeurs?* »

Tel est le problème dont nous vous demandons de proposer la solution comme sujet du grand prix de Mathématiques à décerner en 1860.

*Quels peuvent être les nombres de valeurs des fonctions bien définies qui contiennent un nombre donné de lettres, et comment peut-on former les fonctions pour lesquelles il existe un nombre donné de valeurs?*

*Quels peuvent être les nombres de valeurs des fonctions bien définies qui contiennent un nombre donné de lettres, et comment peut-on former les fonctions pour lesquelles il existe un nombre donné de valeurs?*

In modern words:

*What are the orbit lengths of $S_n$ on the polynomials $\mathbb{Q}[x_1, \ldots, x_n]$; find all possible orbits*

*Quels peuvent être les nombres de valeurs des fonctions bien définies qui contiennent un nombre donné de lettres, et comment peut-on former les fonctions pour lesquelles il existe un nombre donné de valeurs?*

In modern words:

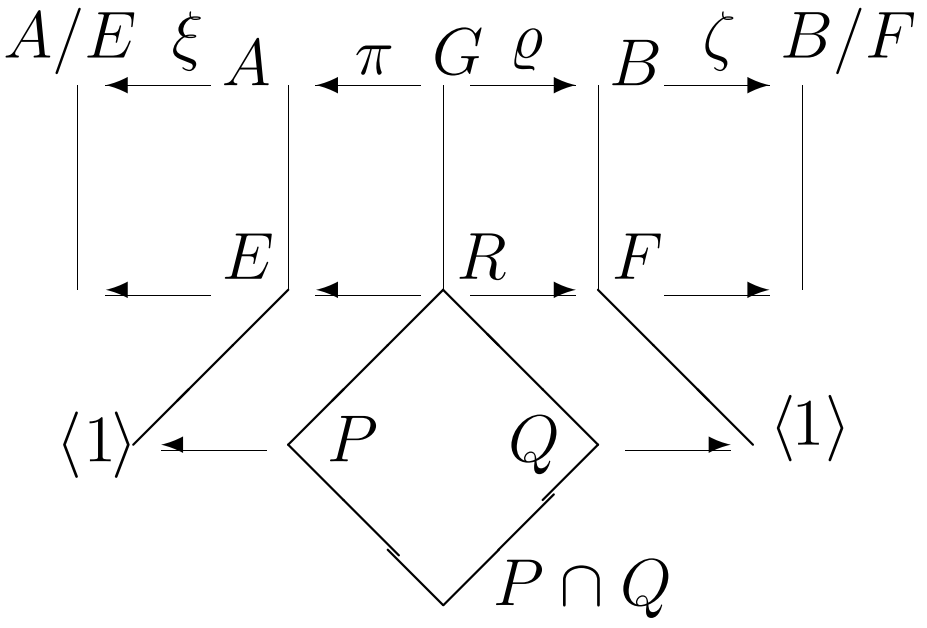
*What are the orbit lengths of $S_n$ on the polynomials $\mathbb{Q}[x_1, \ldots, x_n]$; find all possible orbits*

Respectively:

*Classify the subgroups of $S_n$ up to conjugacy*

# Intransitive groups

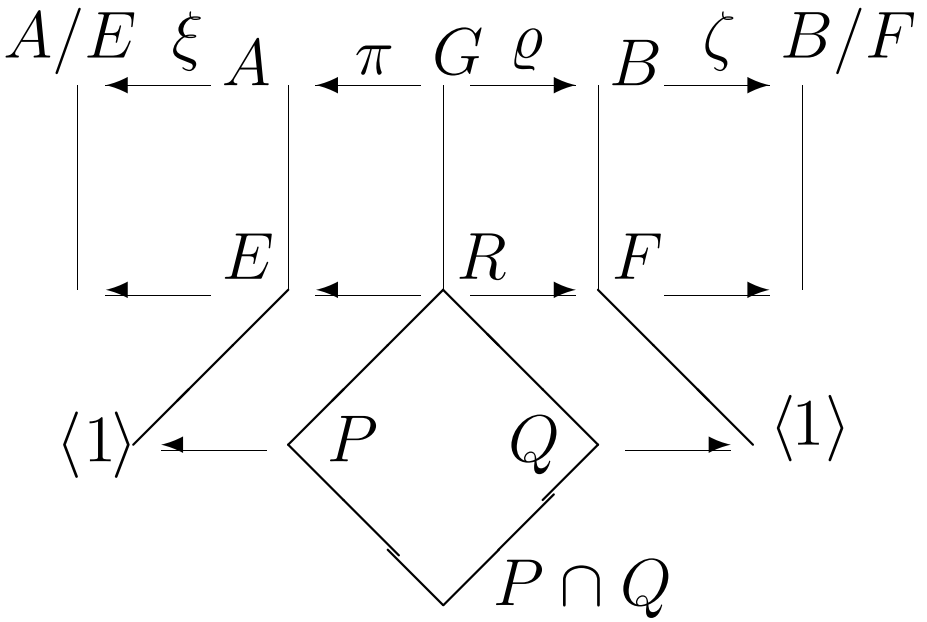
If $G \leq S_n$ is intransitive, take projections $\pi$, $\rho$ on the orbits.




The images are $A$ and $B$, the kernels intersect trivially. Factors of $A$ and $B$ are isomorphic.

# Intransitive groups

If $G \leq S_n$ is intransitive, take projections $\pi$, $\rho$ on the orbits.




The images are $A$ and $B$, the kernels intersect trivially. Factors of $A$ and $B$ are isomorphic.

Vice versa, we can construct $G$ as a *subdirect product* (REMAK) of its factors $A$ and $B$ which are groups of smaller degree.

# Transitive Groups

Thus it suffices to classify transitive subgroups of $S_n$.

Classifications up to degree 15 were done $\sim 1900$:

- MILLER
- COLE
- KUHN

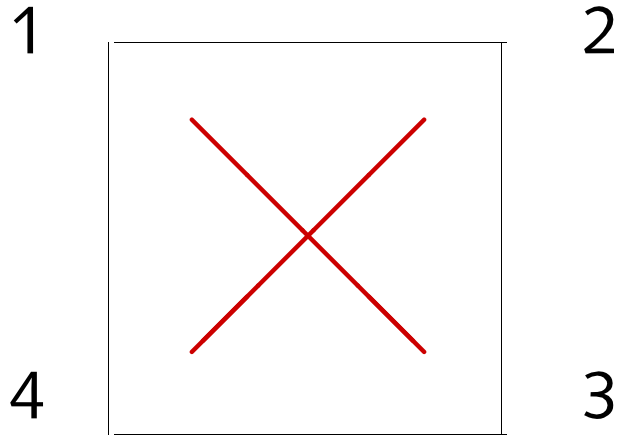
and $1980 - 1990$ with computer help:

- BUTLER-MCKAY (up to 11)
- ROYLE (12)
- BUTLER (14,15)

Their techniques to not carry through to higher degrees.

# Structure of a transitive group

Let $G \leq S_n$ be transitive. A *block system* for $G$ is a partition of $\{1, \ldots, n\}$ that is invariant under $G$:

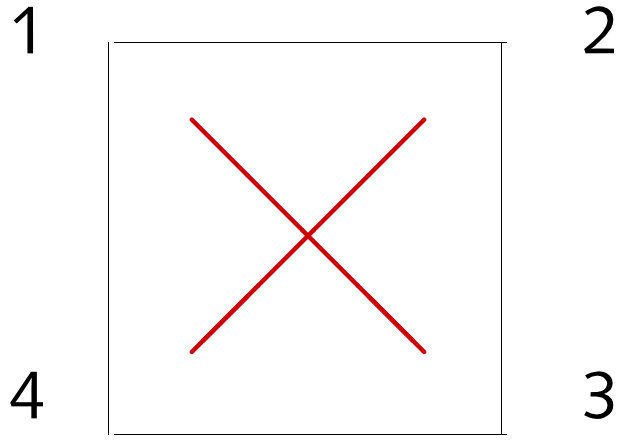



$$G = \langle (1,2,3,4), (1,3) \rangle$$

$$\mathcal{B} = \{\{1,3\}, \{2,4\}\}$$

# Structure of a transitive group

Let $G \leq S_n$ be transitive. A *block system* for $G$ is a partition of $\{1, \ldots, n\}$ that is invariant under $G$:



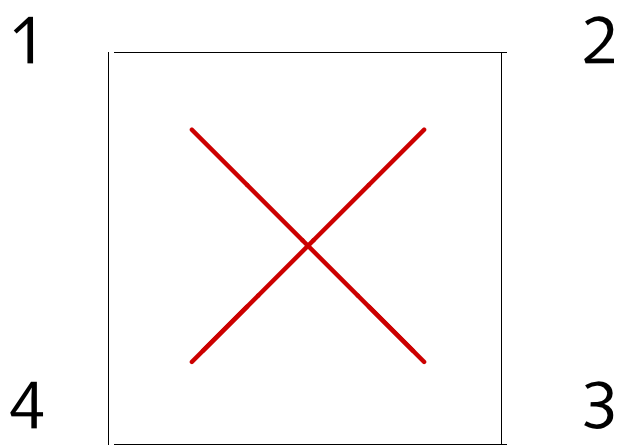

$$G = \langle (1,2,3,4), (1,3) \rangle$$

$$\mathcal{B} = \{\{1,3\},\{2,4\}\}$$

If the only block systems are$\{\{1, \ldots, n\}\}$ and $\{\{1\}, \{2\}, \ldots, \{n\}\}$, the group is called *primitive*

# Structure of a transitive group

Let $G \leq S_n$ be transitive. A *block system* for $G$ is a partition of $\{1, \ldots, n\}$ that is invariant under $G$:




$$G = \langle (1,2,3,4), (1,3) \rangle$$

$$\mathcal{B} = \{\{1,3\},\{2,4\}\}$$

If the only block systems are$\{\{1, \ldots, n\}\}$ and $\{\{1\}, \{2\}, \ldots, \{n\}\}$, the group is called *primitive*

## Theorem:

Block systems correspond to subgroups between $G$ and $\mathrm{Stab}_G(1)$.

# Primitive groups

There is an extensive structure theory for primitive groups (O'NAN-SCOTT theorem).

Using the classification of simple groups, one can classify primitive groups:

- JORDAN 1872 (up to 17)
- SIMS 1970 (up to 20, later up to 50)
- DIXON/MORTIMER 1988 ("non-affine" up to 1000)
- SHORT 1992 ("affine" solvable up to 255)
- THEISSEN 1997 ("affine" nonsolvable up to 255, explicit generators up to 1000)

# Primitive groups

There is an extensive structure theory for primitive groups (O'NAN-SCOTT theorem).

Using the classification of simple groups, one can classify primitive groups:

- JORDAN 1872 (up to 17)
- SIMS 1970 (up to 20, later up to 50)
- DIXON/MORTIMER 1988 ("non-affine" up to 1000)
- SHORT 1992 ("affine" solvable up to 255)
- THEISSEN 1997 ("affine" nonsolvable up to 255, explicit generators up to 1000)

For our purposes we can assume that the primitive groups are known.

# Structure of an imprimitive group

Let $G$ be imprimitive with block system $\mathcal{B}$.

There are $m$ blocks of size $l$ each, $n = l \cdot m$.

# Structure of an imprimitive group

Let $G$ be imprimitive with block system $\mathcal{B}$.

There are $m$ blocks of size $l$ each, $n = l \cdot m$.

$G$ acts on the blocks in $\mathcal{B}$.

Call this action $\varphi$ and its kernel $M = \ker \varphi$.

The image $T = G\varphi$ is a transitive group of smaller degree.

# Structure of an imprimitive group

Let $G$ be imprimitive with block system $\mathcal{B}$.

There are $m$ blocks of size $l$ each, $n = l \cdot m$.

$G$ acts on the blocks in $\mathcal{B}$.

Call this action $\varphi$ and its kernel $M = \ker \varphi$.

The image $T = G\varphi$ is a transitive group of smaller degree.

The point stabilizer $V = \mathsf{Stab}_G(1)$ in $G$ is a subgroup of the block stabilizer $U = \mathsf{Stab}_G(B_1) = (\mathsf{Stab}_{G\varphi}(1))\varphi^{-1}$.

# Structure of an imprimitive group

Let $G$ be imprimitive with block system $\mathcal{B}$.

There are $m$ blocks of size $l$ each, $n = l \cdot m$.

$G$ acts on the blocks in $\mathcal{B}$.

Call this action $\varphi$ and its kernel $M = \ker \varphi$.

The image $T = G\varphi$ is a transitive group of smaller degree.

The point stabilizer $V = \mathrm{Stab}_G(1)$ in $G$ is a subgroup of the block stabilizer $U = \mathrm{Stab}_G(B_1) = (\mathrm{Stab}_{G\varphi}(1))\varphi^{-1}$.

If we assume the blocks in $\mathcal{B}$ to be of minimal size (i.e. $G\varphi$ is as big as possible), $V$ is maximal in $U$.

## Distinguish

a) $M$ is trivial

b) $M$ is not trivial

# Trivial $M$

Then $\varphi$ is an isomorphism $G \to T$. $V\varphi$ is a maximal subgroup of $U\varphi = \mathsf{Stab}_T(1)$.

We get $G$ from $T$ by acting on the cosets of a maximal subgroup of $\mathsf{Stab}_{G\varphi}(1)$. Call such a group an *inflation* of $T$.

# Trivial $M$

Then $\varphi$ is an isomorphism $G \to T$. $V\varphi$ is a maximal subgroup of $U\varphi = \mathsf{Stab}_T(1)$.

We get $G$ from $T$ by acting on the cosets of a maximal subgroup of $\mathsf{Stab}_{G\varphi}(1)$. Call such a group an *inflation* of $T$.

To construct inflations:

- Run though possible $T$ (groups of degree dividing $n$)
- Find maximal subgroups of $\mathsf{Stab}_T(1)$ of suitable index. (Often $\mathsf{Stab}_T(1)$ is solvable, there is an efficient algorithm.)
- Take the action on the cosets of this maximal subgroup.

# Trivial $M$

Then $\varphi$ is an isomorphism $G \to T$. $V\varphi$ is a maximal subgroup of $U\varphi = \mathrm{Stab}_T(1)$.

We get $G$ from $T$ by acting on the cosets of a maximal subgroup of $\mathrm{Stab}_{G\varphi}(1)$. Call such a group an *inflation* of $T$.

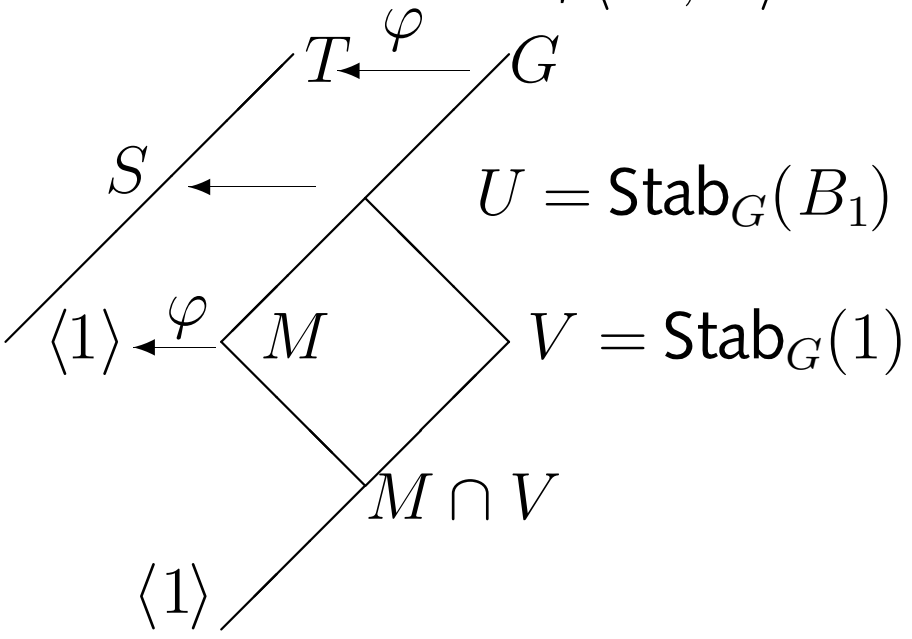
To construct inflations:

- Run though possible $T$ (groups of degree dividing $n$)
- Find maximal subgroups of $\mathrm{Stab}_T(1)$ of suitable index. (Often $\mathrm{Stab}_T(1)$ is solvable, there is an efficient algorithm.)
- Take the action on the cosets of this maximal subgroup.

(Conjugacy of inflations in $S_n$ reduces to conjugacy of maximal subgroups of $T$ under $\mathrm{Aut}(T)$.)

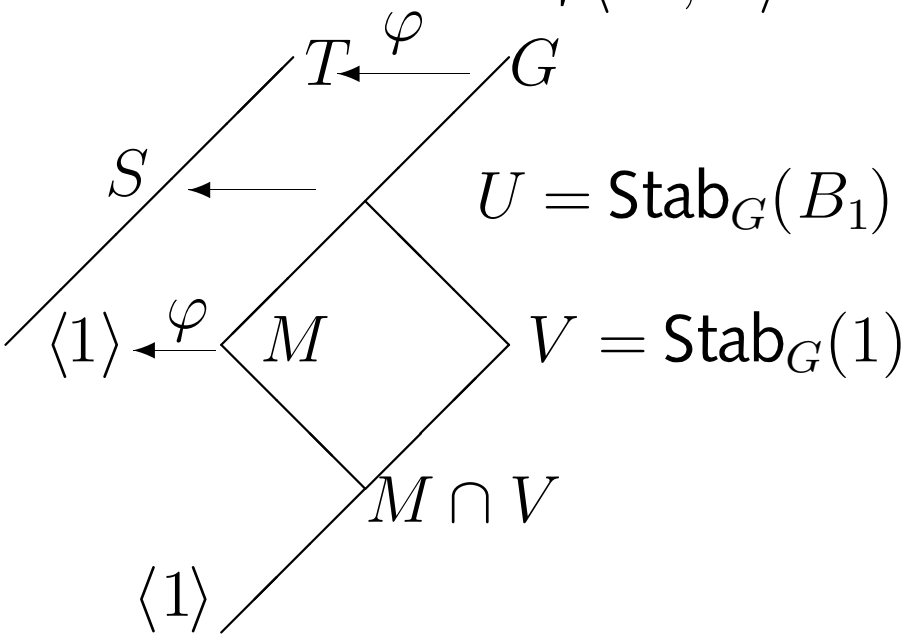
# Nontrivial $M$

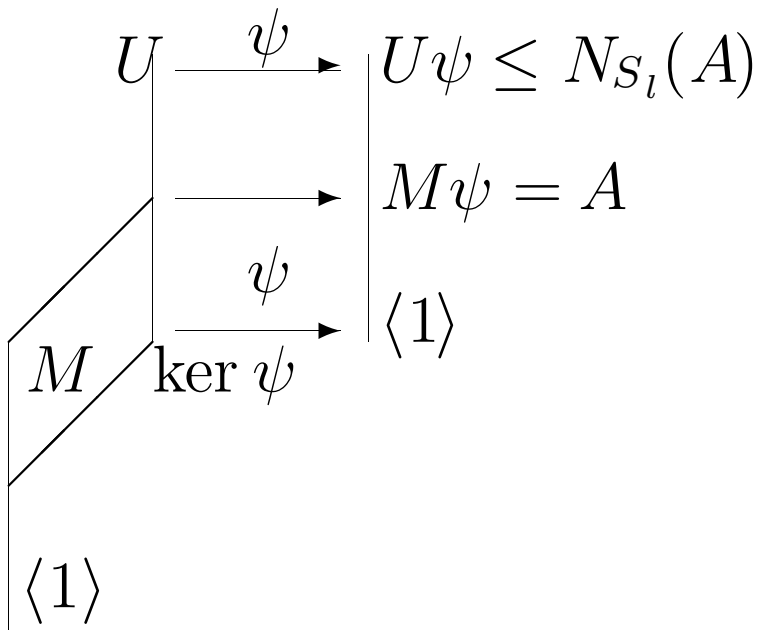
As $V$ is maximal in $U$, $\langle M, V\rangle = U$:



# Nontrivial $M$

As $V$ is maximal in $U$, $\langle M, V\rangle = U$:



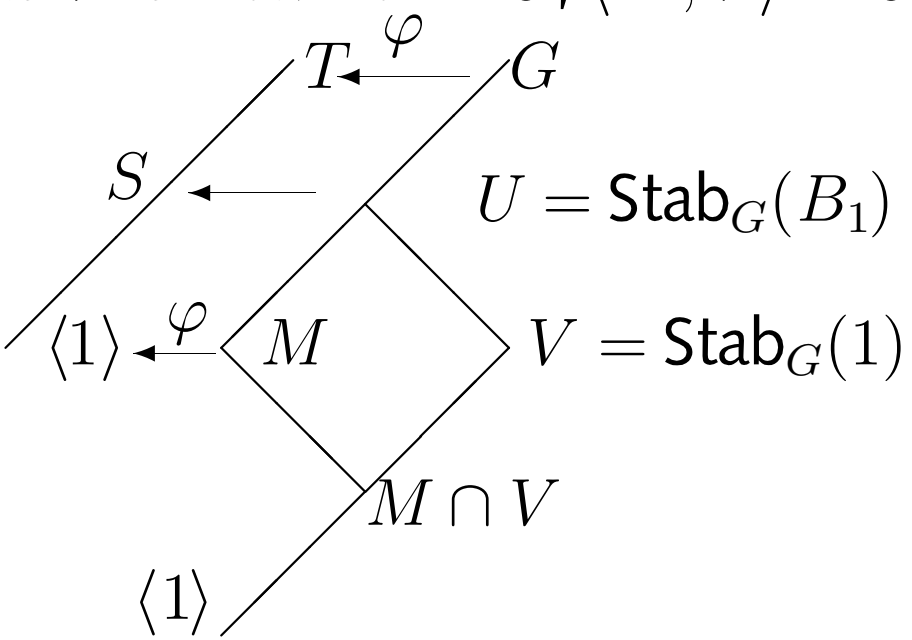



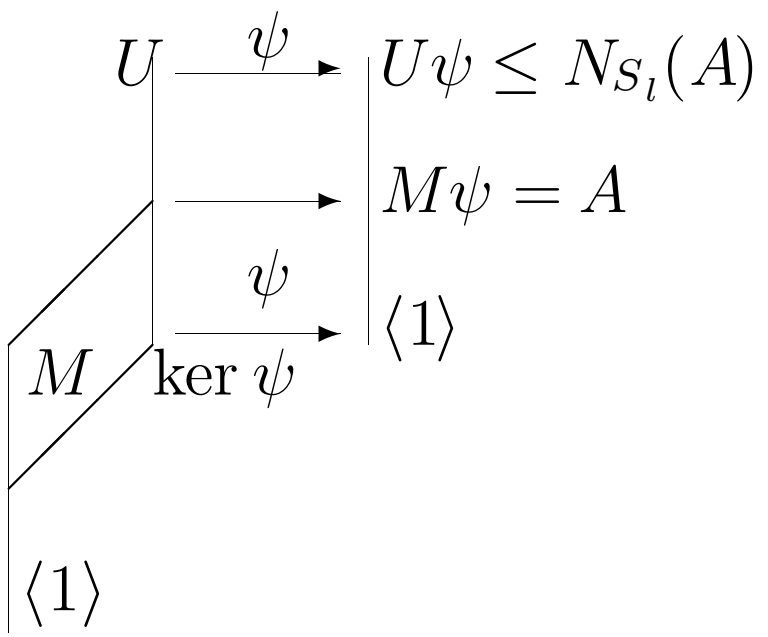

Let $\psi$ be the action of $U$ on $B_1$. $U\psi \leq S_l$ is primitive.

Then $M\psi =: A$ is a transitive normal subgroup of $U\psi$.

# Nontrivial $M$

As $V$ is maximal in $U$, $\langle M, V\rangle = U$:




Let $\psi$ be the action of $U$ on $B_1$. $U\psi \leq S_l$ is primitive.

Then $M\psi =: A$ is a transitive normal subgroup of $U\psi$.

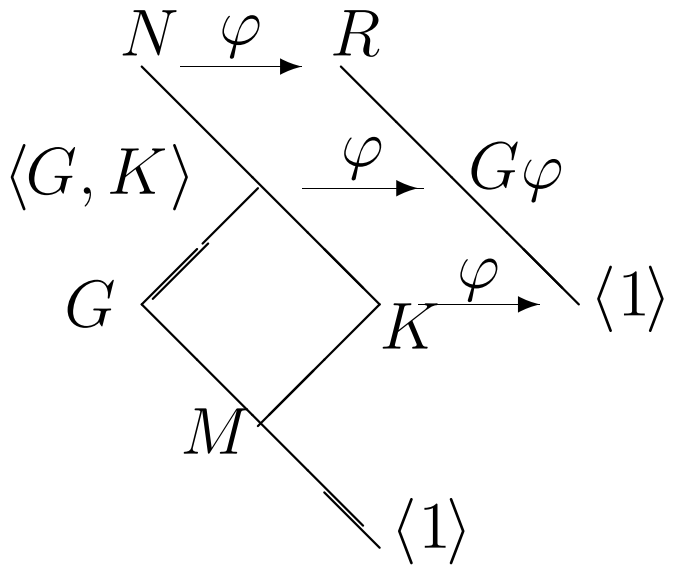
The action of $M$ on *every* block is permutation isomorphic to $A$.

In other words: $M$ is an iterated subdirect product (subpower) of $m$ copies of $A$.

# Connection between $G$ and $M$

Certainly $G \leq N_{S_n}(M) =: N$.

Extend $\varphi$ (block action) to $N$ and let $K$ be the kernel in $N$.




- $R := N\varphi \leq S_m$ is a transitive group.
- $G\varphi \leq R$ is a transitive subgroup.
- $G \cap K = M$.
- $G/M$ is a complement to $K/M$ in $\langle G, K\rangle/M$

# Strategy

- For all nontrivial factorizations $n = l \cdot m$:
- Get all possible $A$ (transitive normal subgroups of primitive groups of degree $l$, index bounds)
- Construct all subpowers of $A$ (the possible $M$)
- For every $M$ compute $N_{S_n}(M)$, transitive subgroups of $R = N\varphi$, complements to preimages of these subgroups.
- Any such complement is a transitive subgroup of $S_n$
- Conjugate groups in the construction lead to permutation isomorphic groups.

# Removing Duplicates

After discarding conjugate groups on all levels, the only possibility to construct the "same" group twice is if a group can be constructed via *several different* block systems.

# Removing Duplicates

After discarding conjugate groups on all levels, the only possibility to construct the "same" group twice is if a group can be constructed via *several different* block systems.

We therefore put further (slightly arbitrary) restrictions on the block system to be used, such as:

- Blocks of minimal size
- Kernel $M$ of minimal size
- Isomorphism of action on blocks minimal

# Removing Duplicates

After discarding conjugate groups on all levels, the only possibility to construct the "same" group twice is if a group can be constructed via *several different* block systems.

We therefore put further (slightly arbitrary) restrictions on the block system to be used, such as:

- Blocks of minimal size
- Kernel $M$ of minimal size
- Isomorphism of action on blocks minimal

If we construct a group with respect to a block system, and this block system does not fulfill all conditions, we discard the group.

The only remaining duplications can arise if a group has essentially two "equivalent" block systems.

Often this implies the existence of special automorphisms.

In this (rare) case we have to test for conjugacy in $S_n$.

## The possible subpowers $M$

For each possible $A$ we can construct the possible $M$ in a recursive process by forming all possible subdirect products and test for conjugacy in $S_n$ by a backtrack search.

## The possible subpowers $M$

For each possible $A$ we can construct the possible $M$ in a recursive process by forming all possible subdirect products and test for conjugacy in $S_n$ by a backtrack search.

This construction is *the* time-critical part of the algorithm.

Pruning the construction tree to only lead to $M$ with transitive normalizer is crucial.

For this we can use the projections of $M$ on its $m$ orbits.

We project the kernel of each projection via every other projection, resulting in a matrix $(\ker \pi_i)\pi_j$.

The rows and columns of this matrix must be equal up to index permutation (since there must be a transitive normalizer of $M$).

For this we can use the projections of $M$ on its $m$ orbits.

We project the kernel of each projection via every other projection, resulting in a matrix $(\ker \pi_i)\pi_j$.

The rows and columns of this matrix must be equal up to index permutation (since there must be a transitive normalizer of $M$).

If we only construct an *initial part* $\bar{M}$ of $M$ (in the middle of the recursive construction), its matrix is a minor of the matrix for $M$.

If the matrix for $\bar{M}$ cannot be extended to an admissible matrix, *all groups that could arise from* $\bar{M}$ can be discarded.

# Invariant subgroups

We can embed any imprimitive $G$ in a wreath product $(U\psi) \wr (G\varphi) = U\psi \wr T$.

If we know that $G$ will induce the same action on $A^m \leq (U\psi)^m$ as the complement $T$ in the wreath product, $M$ must be invariant under $T$.

# Invariant subgroups

We can embed any imprimitive $G$ in a wreath product $(U\psi) \wr (G\varphi) = U\psi \wr T$.

If we know that $G$ will induce the same action on $A^m \leq (U\psi)^m$ as the complement $T$ in the wreath product, $M$ must be invariant under $T$.

This is for example the case if $l = 2$ or if $|T|$ and $|U\psi|$ are coprime.

# Invariant subgroups

We can embed any imprimitive $G$ in a wreath product $(U\psi) \wr (G\varphi) = U\psi \wr T$.

If we know that $G$ will induce the same action on $A^m \leq (U\psi)^m$ as the complement $T$ in the wreath product, $M$ must be invariant under $T$.

This is for example the case if $l = 2$ or if $|T|$ and $|U\psi|$ are coprime.

In this situation we can compute the possible $M$ as subgroups of $A^m$ invariant under certain automorphisms.

This is usually faster than the recursive construction.

# Results

I have implemented this method in GAP and used it up to degree 30.

| d | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|
| p | 1 | 2 | 2 | 5 | 4 | 7 | 7 | 11 | 9 | 8 |
| t | 1 | 2 | 5 | 5 | 16 | 7 | 50 | 34 | 45 | 8 |

| d | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|
| p | 6 | 9 | 4 | 6 | 22 | 10 | 4 | 8 | 4 | 9 |
| t | 301 | 9 | 63 | 104 | **1954** | 10 | **983** | 8 | **1117** | **164** |

| d | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|
| p | 4 | 7 | 5 | 28 | 7 | 15 | 14 | 8 | 4 | 12 |
| t | **59** | 7 | **25000** | **211** | **96** | **2392** | **1854** | 8 | **5712** | 12 |

Bold numbers indicate a hitherto unknown result.

On a 933MHz Pentium III, degrees up to 15 take a few minutes each, degrees 16-22 a few hours, degrees 24-30 are done one or two days each.

I'm still (...) in the process of checking the results before releasing the data.

I also computed the minimal transitive groups of the relevant degrees.

On a 933MHz Pentium III, degrees up to 15 take a few minutes each, degrees 16-22 a few hours, degrees 24-30 are done one or two days each.

I'm still (...) in the process of checking the results before releasing the data.

I also computed the minimal transitive groups of the relevant degrees.

Degree 32 will have several 100 000 groups and thus is a good point to stop.