Article Submitted to Journal of Symbolic Computation

Constructing Transitive Permutation Groups

Alexander Hulpke

Department of Mathematics, Colorado State University,
Fort Collins, CO 80523,
hulpke@math.colostate.edu

Abstract

This paper presents a new algorithm to classify all transitive subgroups of the symmetric group up to conjugacy. It has been used to determine the transitive groups of degree up to 30.

1. Introduction

This article describes a method to construct the transitive groups of a given degree n, that is to classify the transitive subgroups of S_n up to conjugacy. Its prerequisites are the transitive groups of all degrees dividing n as well as the primitive groups of degree n. Given the primitive groups this permits a recursive construction of all groups.

The algorithm has been used successfully to verify the lists of groups of degree up to 15 and to construct the hitherto unclassified groups of degree 16-30. These calculations were done in the computer algebra system GAP 4 [GAP, 2002], which provides methods for all the underlying calculations which we shall use as building blocks.

An extended description of the construction process has been given in the the author's dissertation [Hulpke, 1996]. This article aims to give a description of this process of reasonable length, leaving out some technical details, such as an explicit description of backtrack searches. (For these we will refer to Hulpke [1996].) It also corrects (in section 12.1) several errors in preliminary results reported in this thesis.

The long delay between the publication of the thesis and this paper is due to extensive reruns and checks for potential errors.

2. History

The problem of classifying subgroups of the symmetric group is easily one of the oldest problems in group theory, it is in fact the subject of the 1858 prize question of the Académie des Sciences: [Academie des sciences, 1857]:

> *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?*

This question is formulated in the language of invariants – at this time there was no formal definition of a permutation group – and what it asks for are possible orbit lengths ("*nombre de valeurs*") for the action of S_n on polynomials in n invariants by permuting the invariants. In other words, it asks for the indices of all subgroups of S_n. (There were three submissions in 1860, however no prize was awarded.)

It is easily seen that intransitive groups can be constructed as subdirect products of transitive groups of smaller degree, so the main task is to classify transitive groups.

By the beginning of the 20th century, a series of articles had appeared, which classified the transitive groups up to degree 15. The classification for the higher degrees culminates in the papers of Cole [1895], Miller [1896, 1898], Kuhn [1904]. A fuller history of this endeavour can be found in [Short, 1992, Appendix A, pp. 122–124]. All these classifications relied more or less on ad-hoc arguments, the long sequel of papers correcting previous classifications does not encourage trust is the results.

With the advent of computers, starting in the early 1980s the classifications up to degree 15 were redone by Butler and McKay [1983], Royle [1987], Butler [1993]. A complete list of these groups with names and properties can be found in Conway et al. [1998]. Apart from a few errors in degree 12 they confirm the results of the hand classifications. Still, the methods used rely on ad-hoc arguments and are unlikely to permit classifications for degrees beyond 15.

2.1. Classification of primitive groups

For primitive groups the situation is much better. The primitive groups up to degree 17 were already classified in by Jordan [1872]. Sims [1970] published a list up to degree 20 and later extended it up to degree 50. Solvable primitive groups of degree < 256 were classified by Short [1992], Eick and Höfling [2003] extend this classification to degree 6560. Finally, Roney-Dougal and Unger [2003] classify all affine groups of degree up to 1000.

The O'Nan-Scott theorem [Scott, 1980] and the classification of finite simple groups [Gorenstein, 1982] essentially reduce the problem of classifying primitive groups to the classification of maximal subgroups of simple groups and to the problem of classifying irreducible matrix groups.

Dixon and Mortimer [1988] classify the non-affine primitive groups up to degree 999. This classification was made explicit by Theißen [1997], which also gives the non-solvable affine groups up to degree 255.

These primitive permutation groups are accessible in GAP via the command `PrimitiveGroup`.

We can sum these results up by saying that primitive groups have been classified up to degree 999. The techniques used do not stop at this degree but should be able to classify groups of degree up to several thousands if such a classification was desired.

In particular, a classification of transitive groups only needs to classify the imprimitive groups.

3. The structure of an imprimitive group

Assume that G is an imprimitive group of degree n with a block system whose blocks are minimal proper blocks with respect to inclusion. This block system is denoted by $\mathcal{B} = \{\mathrm{B}_1, \ldots, \mathrm{B}_m\}$, so the block size is $l = |\mathrm{B}_i| = \frac{n}{m}$. Without loss of generality we may assume that $1 \in \mathrm{B}_1$.

Let $V = \mathrm{Stab}_G(1)$ and $U = \mathrm{Stab}_G(\mathrm{B}_1)$ (set-wise), then $V \leq U$ and $[U{:}V] = l$. The action φ of G on $\mathcal{B}$ yields a transitive permutation representation $T := G\varphi$ of G of degree m. Its kernel is

$$M := \ker\varphi = \bigcap_{g\in G} U^g.$$

In analogy to wreath products, we call M the *base group* of G (with respect to $\mathcal{B}$). Because $\mathcal{B}$ was chosen to have minimal blocks, V is a maximal subgroup of U. Thus we have either $M \leq V$ or $\langle M, V\rangle = U$. We shall treat both cases separately

3.1. Faithful block action

In this case we assume that $M \leq V$. As the action on the cosets of V is faithful (G is a transitive permutation group), this implies that $M = \langle 1\rangle$ and $T = G\varphi \cong G$. The subgroup $\widetilde{V} := V\varphi \leq T$ is a maximal subgroup of index l of the point stabilizer $\widetilde{U} = U\varphi$ in T. The permutation action of G can be obtained from the action of T on the cosets of $\widetilde{V}$. We call G an *inflation* of T.

Vice versa if T is a transitive group of degree m, every maximal subgroup of index l of its point stabilizer defines a inflation that is a transitive subgroup of S_n. (In practice, inflations only are a minority among the transitive groups of degree n.)

To examine conjugacy among inflations, we now assume that G_1 and G_2 are both inflations of the transitive group $T \leq S_m$, corresponding to the maximal subgroups $\widetilde{V}_1$ and $\widetilde{V}_2$ of the point stabilizer of T. We denote the corresponding permutation representations by $\phi_1 \colon T \to G_1$ and $\phi_2 \colon T \to G_2$. If G_1 and G_2 are

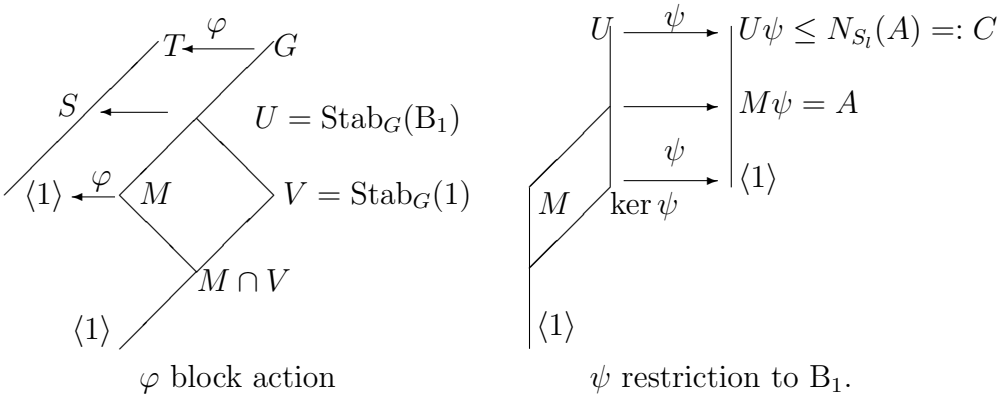

Figure 1: Structure of proper extensions of T

conjugate under S_n via the inner automorphism σ of S_n, then $\alpha = \phi_1\sigma\phi_2^{-1}\colon T \to T$ is an automorphism of T. As σ is induced by a conjugating permutation, it must map the point stabilizer of G_1 onto a point stabilizer of G_2, thus $\widetilde{V}_1\alpha = \widetilde{V}_2^t$ for a suitable $t \in T$. That is, the subgroups $\widetilde{V}_1$ and $\widetilde{V}_2$ are conjugate under the automorphism group of T. Vice versa an automorphism of T that maps $\widetilde{V}_1$ to $\widetilde{V}_2$ induces a bijection of the cosets $\widetilde{V}_1\backslash T$ onto the cosets $\widetilde{V}_2\backslash T$ and thereby a permutation in S_n that conjugates G_1 into G_2. In other words:

LEMMA 3.1: *The* $\mathrm{Aut}(T)$*-classes of maximal subgroups of the point stabilizer of* T *are in bijection with the* S_n*-classes of inflations of* T*.*

3.2. Proper extensions

In the sequel we assume that M is not trivial and thus $\langle M, V\rangle = U$. We denote the restriction of the natural permutation action of U to B_1 by $\psi\colon U \to S_l$. Its image $U\psi$ is primitive because V is maximal in U. In addition, M contains representatives for all cosets of V in U and thus acts transitively on B_1. Therefore $A := M\psi$ is a transitive normal subgroup of the primitive group $U\psi$, and we get the inequality

$$[U\psi{:}A] = [U\psi{:}M\psi] \;\Big|\; [U{:}M] = |\mathrm{Stab}_T(1)|\,, \tag{1}$$

which will be used to limit the possibilities for A.

Figure 1 illustrates the situation.

Considering the relation between G and the constituents $U\psi$ and $G\varphi$, we shall frequently use the embedding theorem for wreath products in the following form

THEOREM 3.1: *(Krasner and Kaloujnine [1951]) G can be embedded as a permutation group into the wreath product $(U\psi)\wr T$ in its natural imprimitive action, this embedding maps the block system $\mathcal{B}$ onto the block system of the wreath product.*

Vice versa, if G can be embedded in this way into a wreath product $X \wr Y$, then $G\varphi$ is permutation isomorphic to a subgroup of Y and $U\psi$ to a subgroup of X.

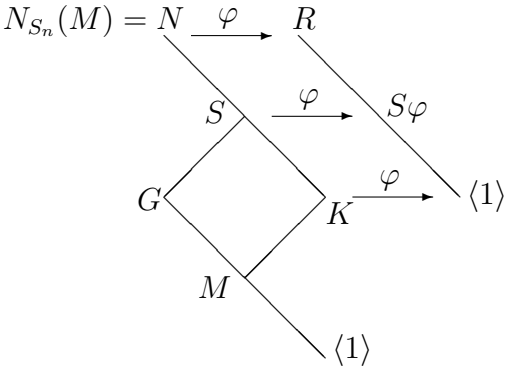

Figure 2: Supergroups of the subpower M.

The kernel M of the block action φ will fix all blocks in $\mathcal{B}$ set-wise, on the other hand G acts transitively on the set of these blocks. Thus the action of M on *every* block is permutation isomorphic to A. Therefore M is an iterated subdirect product of m copies of A and thus a subgroup of the m-fold direct product $A^{\times m}$ of copies of A. We call such a group a *subpower* of A of *length* m and write $\mathrm{length}(M) = m$.

Definition 3.2: *A transitive subgroup $T \leq S_m$ is called* minimally transitive, *if no proper subgroup of T is transitive on $\{1, \ldots m\}$. This is the case if and only if all maximal subgroups of T are intransitive.*

Remark 3.3: *If T is not a minimally transitive group, the full preimage $H \leq G$ under φ of a minimally transitive subgroup of T will contain M. H also acts transitively on the set of blocks and thus is a transitive group of degree n as well. The base group of H is M.*

For any analysis which does not require particular properties of the block system (for example $\mathcal{B}$ is not necessarily pertinent — see Definition 4.1 — to H), we may therefore assume the factor group T to be minimally transitive.

Now consider the normalizer $N := N_{S_n}(M)$. It contains G. We extend the block action φ to N and denote its kernel and image by $K := \ker\varphi$ and $R := \mathrm{Image}\,\varphi$. By definition $K \cap G = M$ and $T = G\varphi \leq R$ is a transitive group of degree m. Denote the full preimage of T by $S = GK$. Then G/M is a complement to K/M in S/M. Figure 2 serves as an illustration.

Vice versa, if $T \leq R$ is a transitive subgroup, and $S = T\varphi^{-1}$ its full preimage, every subgroup $M \leq H \leq S$ such that H/M complements K/M in S/M has transitive image $T = G\varphi$ and contains M. H therefore is a transitive subgroup of S_n. Thus:

Lemma 3.2: *The imprimitive groups, which are not inflations, are preimages of complements to* $\ker\varphi/M$ *in S/M, where M is a subpower of a transitive group*

$A \leq S_l$ with transitive normalizer $N = N_{S_n}(M)$, and $S\varphi \leq N\varphi$ is a transitive subgroup.

To construct all transitive groups which are proper extensions it is thus sufficient to construct first all possible base groups M, and then to get for each base group M the corresponding transitive groups as preimages of complements in a factor group of the normalizer of M.

4. Eliminating Duplicates

We now want to use the structure analysis of the previous section to describe transitive subgroups of S_n up to conjugacy in S_n. For this we will have to analyze the influence of conjugation on the construction via base groups. One further complication is that we fixed one block system $\mathcal{B}$ in the preceding analysis, while a transitive group typically has several block systems. To overcome this problem we will try for a transitive imprimitive group G to mark one block system as "special". For this we shall assume that the classes $[T]$ of transitive groups of smaller degree are ordered (in an arbitrary way, for example by comparing index numbers in a classification of groups of that degree, see section 13) and denote by $\mathfrak{T}_m$ the set of classes of degree m.

Definition 4.1: *Let $G \leq S_\Omega$ be transitive and imprimitive, preserving the partition $\mathcal{B}$ of Ω as a block system. Then $\mathcal{B}$ is called* pertinent to G *if:*

- *P1 G affords no (proper) block system with blocks of smaller size.*
- *P2 Among all block systems with blocks of this size, the order of the kernel of the action on the set of blocks (the group M in the last section) is minimal.*
- *P3 Among those block systems the class $[(\mathrm{Stab}_G(\mathrm{B}_1))^{\mathrm{B}_1}]$ of a block stabilizer's action on one block (unless it is trivial) is minimal in $\mathfrak{T}_l$ ($l = |\mathrm{B}_1|$) .*
- *P4 Among those block systems the class $[T]$ of the block action is minimal in $\mathfrak{T}_m$ ($m = |\mathcal{B}|$).*

The criteria for pertinence have been chosen to permit a quick test whether a given block system is pertinent to a group. Obviously every imprimitive group has a pertinent block system, but there may be several ones (for example the Klein four group $\langle (1,2)(3,4), (1,3)(2,4)\rangle$ has three pertinent block systems). The conditions are however sufficiently restrictive that the case of several pertinent block systems usually corresponds to automorphisms of the group that are induced by its normalizer in the symmetric group.

To test for pertinence, we will have to compute all block systems [Schönert and Seress, 1994]. We also need to identify and compare the classes $[T]$ of transitive groups of smaller degree. The easiest way to do this seems to be to use the identification process described in section 13 and to compare the indices of the classes of groups in $\mathfrak{T}_m$.

When constructing imprimitive groups, we will construct groups with respect to a pertinent block system. If a group has been constructed from a block system which turns out to be not pertinent, we can immediately discard it (as it will be constructed also with respect to a pertinent block system).

We also note that pertinence is invariant under conjugation by elements of the symmetric group: if $\mathcal{B}$ is pertinent to G then $\mathcal{B}^g$ is pertinent to G^g. Tests for conjugacy therefore can assume that the pertinent block system of one group must be mapped to a pertinent block system of the other group. This greatly reduces the difficulty of conjugacy tests and eventually will lead us to a kind of parameterization of the imprimitive groups that we shall use for the construction.

4.1. Total ordering of groups

In eliminating conjugates we will also need a "tie-break" rule that tells us which of two conjugate groups to pick. The easiest way to do this is to pick the "smallest" group with respect to some total order.

We shall therefore assume that we have a total order $\preceq$ defined on the set of all permutation groups. We also assume (as this will be useful) that this order is invariant under translation, i.e. if we replace for a fixed integer j each point i by $i + j$ (for example for $j = 5$ the permutation $(1, 2, 3)$ would become $(6, 7, 8)$ then the ordering of groups remains invariant). The comparison of the lexicographically smallest generating systems of Hulpke and Linton [2003] for example fulfills these conditions.

In the following description we will refer to choices such as "the minimal group in the list", implying comparison with respect to this ordering $\preceq$.

4.2. Inflations up to Conjugacy

Because of condition P2, we can separate the case of inflations completely from the case of faithful action and we will deal with them separately:

Let $G, H \leq S_n$ be inflations with respect to pertinent block systems $\mathcal{B}$ and $\mathcal{C}$. We assume that G and H are conjugate via the inner automorphism σ of S_n. Because of pertinence condition P4, G and H must be inflations of the same transitive group $T \leq S_m$. Lemma 3.1 parameterizes these up to conjugation.

The process to construct representatives of all classes of inflations now proceeds as follows for each representative T of the classes of transitive groups of degree $m \mid n$: Compute representatives of the $\mathrm{Aut}(T)$-classes of maximal subgroups U of the point stabilizer $\mathrm{Stab}_T(1)$ for which the index is $\left[\mathrm{Stab}_T(1):U\right] = l = n/m$. For each representative compute the corresponding inflation.

In most cases this point stabilizer is so small that it is easy to get the maximal subgroups by computing all subgroups or using the method for solvable groups of Eick [1993]. If the groups get bigger the methods of Eick and Hulpke [2001] and Cannon and Holt [in preparation] could be used. Since the computation of $\mathrm{Aut}(T)$ can be difficult, the following criterion can be helpful to determine the cases, in which $\mathrm{Aut}(T)$ can be replaced by the normalizer $N_{S_m}(T)$.

REMARK 4.2: *Let V_1, V_2 be maximal subgroups of the point stabilizer $U = \mathrm{Stab}_T(1)$ and $\alpha \in \mathrm{Aut}(T)$ with $V_1^\alpha = V_2$. Thus $V_2 \leq U$ and $V_2 = V_1^\alpha \leq U^\alpha$. If α is not induced by $N_{S_m}(T)$ then U^α is not a point stabilizer ([Dixon and Mortimer, 1988, Lemma 1.6B]). Thus the inflation of T via V_2 has two maximal block systems (corresponding to U and to U^α) such that the image of the action on the set of blocks is permutation isomorphic to T.*
Instead of computing $\mathrm{Aut}(T)$ it is therefore worth to check first whether any of the inflations (for classes fused under $N_{S_m}(T)$) has this property; if not, then no extra fusion under $\mathrm{Aut}(T)$ will take place.

4.3. Conjugacy of Proper Extensions

We now want to examine conditions for conjugacy under S_n. Let $G, H \leq S_n$ be both imprimitive groups that arise from the pertinent block systems $\mathcal{B}$ and $\mathcal{C}$ respectively with base groups $M \lhd G$ and $\widehat{M} \lhd H$. We assume that neither group is an inflation, so $M \neq \langle 1 \rangle \neq \widehat{M}$.

Suppose that there is an element $g \in S_n$ such that $H = G^g$. Then $\mathcal{B}^g$ is a block system pertinent to $H = G^g$, the kernel of the corresponding block action is $M^g \lhd H$.

Assume first that $M^g = \widehat{M}$: Since conjugate base groups M will yield conjugate classes of transitive groups we need to construct the base groups M only up to conjugacy. In this case we thus have that $M = \widehat{M}$. The conjugating element g then normalizes M and is thus contained in $N = N_{S_n}(M)$. It thus induces an inner automorphism of N/M which maps G/M to H/M and GK/K to HK/K and $G\varphi \leq N\varphi$ to $H\varphi$.

Vice versa conjugate subgroups $X\varphi, Y\varphi \leq N\varphi$ lead to conjugate preimages $X, Y \leq N$ and conjugate classes of complements to K/M.

Representatives up to conjugacy by $N\varphi$ can be obtained as follows: First classify the transitive subgroups of $N\varphi$ up to conjugacy; then compute for each preimage S representatives of the classes of complements to K/M, and finally compute representatives for the further fusion under the action of N/M. (In fact, since S must be stabilized, only the action of the preimage of $N_{N\varphi}(S\varphi)$ is relevant.) The transitive groups then are obtained as preimages under the natural homomorphism $N \to N/M$.

The second case is that of $M^g \neq \widehat{M}$. Then $\mathcal{B}^g \neq \mathcal{C}$ is a *second* block system pertinent to H. This case therefore can only occur if the resulting groups have at least *two* pertinent block systems. If this is the case, we have to check for each block system pertinent to the group (except for the one with respect to which it has been constructed) whether the group has also been constructed in another way.

To do so for a group G, we compute conjugating elements g_i such that the different pertinent base groups $M_i \leq G$ are brought into their "normal" form (i.e. the normal form used in the construction of the possible base groups, see

section 7.1). We can do this with the same algorithms as will be used in the process to construct all possible M.

We shall now assume that all conjugates $M_i^{g_i}$ are in normal form. Next, we introduce an arbitrary total order on all base groups. We discard G, if any $M_i^{g_i}$ is smaller (in this order) than the M with respect to which G was constructed. (One could have made this an extra condition for pertinence.)

The only remaining case is that M is equal to some $M_i^{g_i}$. In this case we have to keep the affected groups in a separate list and finally test them via a backtrack search for conjugacy in S_n, discarding conjugates. (This situation happens rarely. It also is the only place in the construction where we have to test for conjugacy of transitive groups in S_n.)

5. The construction algorithm

Based on the preceding structure analysis, we obtain the following construction algorithm for (representatives of) the transitive groups of degree n.

1) For each divisor $l \mid n$ construct representatives of the imprimitive groups with pertinent block system with m blocks of size l as follows (Steps 2-11):
2) Compute representatives of all groups that are obtained as inflations (see section 4.2).
3) Compute representatives of all possible base groups M with m blocks (see section 6). For each such $M \leq A^{\times m}$
    4) Compute the normalizer $N = N_{S_n}(M)$. (By Theorem 3.1 we have that $N \leq W = C \wr S_m$ where $C = N_{S_m}(A)$.)
    5) Compute the action φ of N on the blocks. In the image group R compute representatives of the classes of transitive subgroups (see section 10.1). For each preimage S of such a subgroup
        6) Compute representatives of the conjugacy classes of complements to $\ker\varphi/M$ in S/M. Obtain representatives of the $N_N(S)$-classes of these (see section 10.2). Every preimage G of such a complement under φ is an imprimitive group with base group M.
        7) For every such G, compute all block systems.
        8) Eliminate G if the construction block system is not pertinent.
        9) If G has more than one pertinent block system, compute for each pertinent base group M_i a conjugating element g_i such that $M_i^{g_i}$ is in normal form. Discard G if M is not minimal among these.
        10) If several conjugates $M_i^{g_i}$ are equal to M, store M in a special list of groups that have to be filtered for S_n conjugacy. Otherwise add G to the list of all imprimitive groups (see section 4.3).
    11) Eliminate conjugates from the list of groups with several pertinent base groups conjugate to M. Add the remaining representatives to the list of groups.

12) Add representatives of the primitive groups of degree n (see section 2.1).

6. Construction of all possible base groups

The first (and most time consuming) part of the algorithm is to construct all possible base groups M. We remember that each M is a subpower of m copies of a group A, where $A \leq S_l$ is a normal subgroup of a primitive group $P = U\psi$ of degree l and index $[P{:}A]$ bounded according to (1). For each group A that fulfills these conditions, we have to compute subpowers of length m up to conjugacy.

The general process for this is a recursive construction that will be described in section 7. However, since we are only interested in subpowers that have a transitive normalizer in S_n, the construction tree can be pruned substantially. Methods for this will be described in section 8.

In many cases we can also show, that a transitive group of degree n must not only permute the blocks, but also permute the points in the blocks in a nice way. In this situation the potential subpowers of length m are subgroups of $A^{\times m}$ which are invariant under an automorphism action. We shall study this situation in section 9.

From now on, assume that $A \leq S_l$ is fixed and let $C = N_{S_l}(A)$. We shall regard a subpower M of length m as a subgroup of $A^{\times m} \lhd C^{\times m}$ which is given in a natural way as an intransitive subgroup of S_n ($n = lm$). The list of orbits of $C^{\times m}$ is denoted by

$$\mathcal{B} = \{\{1, \ldots, l\}, \ldots, \{n-l+1, \ldots, n\}\},$$

we call the subsets of $\mathcal{B}$ *components*. Thus the constituent projections

$$\pi_i\colon \begin{array}{ccc} C^{\times m} & \to & C \\ (c_1, \ldots, c_m) & \mapsto & c_i \end{array}$$

can be considered as restrictions to the blocks $\mathrm{B}_i \in \mathcal{B}$. We also define projections

$$\mu_i\colon \begin{array}{ccc} C^{\times m} & \to & C^{\times i} \\ (c_1, \ldots, c_m) & \mapsto & (c_1, \ldots, c_i) \end{array}$$

Definition 6.1: *We call* $\overleftarrow{\frac{M}{i}} := M\mu_i$ *the* i-th initial part *of* M*; we also call* M *a* completion *of its initial parts.*

We finally set $W = C \wr S_m$. Then if M is a subpower of A of length m we have (by Theorem 3.1) that $N_{S_n}(M) \leq W$.

7. Construction of Subpowers

A subpower M of length m is a subdirect product of its initial part $\overleftarrow{\frac{M}{m-1}}$ with A. Since the initial part is a subpower again, we can construct subpowers of

increasing length recursively, starting with A. On the $i+1$-th level we then have to construct all subdirect products of all initial parts $\overleftarrow{\underset{i}{M}}$ with A.

According to Remak [1930] the subdirect products of an initial part $\overleftarrow{\underset{i}{M}}$ with A are parameterized by pairs of normal subgroups of $\overleftarrow{\underset{i}{M}}$ and of A with isomorphic factor groups, as well as by the isomorphisms between these factor groups:

In a subdirect product $\overleftarrow{\underset{i}{M}} \curlywedge A$ with projections $\mu_i \to \overleftarrow{\underset{i}{M}}$ and $\pi_{i+1} \to A$ these normal subgroups are the projection kernel images $(\ker \mu_i)\pi_{i+1} \lhd A$ and $(\ker \pi_{i+1})\mu_i \lhd \overleftarrow{\underset{i}{M}}$.

7.1. Canonical Representatives

This recursive process would construct *all* subdirect products. Reducing the list to representatives up to conjugacy then would become very expensive. We shall therefore – as far as possible – try to construct only representatives and to weed out as early as possible in the construction process those partially constructed products that will only lead to conjugate subdirect products. The key to this aim will be to designate "canonical" representatives, such that each product is conjugate to exactly one canonical representative, and to restrict the construction as far as possible towards constructing only canonical products.

Definition 7.1: *If X and Y are permutation groups, we say that Y is* small under X*, if Y is minimal in the orbit $Y^X = \{Y^x \mid x \in X\}$ (with respect to the total ordering $\preceq$ on groups defined in section 4.1).*

We denote by C_i the copy of C in $C^{\times m}$ acting on the i-th component of $\mathcal{B}$. A subpower M is considered as a subdirect product of its initial part $\overleftarrow{\underset{m-1}{M}}$ with A, the constituent projections yield normal subgroups $F \lhd \overleftarrow{\underset{m-1}{M}}$ and $E \lhd A$. In the subdirect product the A-part then acts on the m-th orbit, so we consider A as a subgroup of C_m.

Definition 7.2: *A subpower M is called* canonical *if the following conditions hold:*

- *K1 The initial part $\overleftarrow{\underset{m-1}{M}}$ is canonical (and so — by induction — are all other initial parts).*
- *K2 F is small under $N_{C \wr S_{m-1}}\left(\overleftarrow{\underset{m-1}{M}}\right)$. (We consider $C \wr S_{m-1}$ to be acting on the first $m-1$ orbits in $\mathcal{B}$.)*
- *K3 E is small under C_m.*
- *K4 Under the remaining W-conjugates of M, fulfilling conditions K1 to K3, M is minimal with respect to the total ordering on all groups.*

At the first view, this definition might look very complex. Its parts however fit a recursive construction: Condition K1 ensures that we only need to extend canonical representatives, conditions K2 and K3 restrict the number of products to construct.

LEMMA 7.1: *For each subpower M there is exactly one canonical representative in the class $[M]$ of M under the action of W.*

Proof: Condition K4 ensures there is at most one canonical representative. By conjugating with $C \wr S_{m-1}$ we can ensure condition K1. This condition will not be affected by further conjugation with $N_{C\wr S_{m-1}}\left(\underset{m-1}{\overleftarrow{M}}\right) \times C_m$. We can thus fulfill conditions K2 and K3 so that the set of canonical representatives is not empty. □

If a subpower M is given, we can find the canonical representative of $[M]$ in a backtrack search, in which we construct all conjugates of M which fulfill conditions K1 to K3 and then take the minimal one among them.

The conjugating elements correspond to the leafs of a tree, given by the decomposition of the acting wreath product $W = C \wr S_m$ of the form $W = T_1C_1T_2C_2 \cdot \cdots \cdot T_mC_m$ with T_i a transversal for the left cosets $\mathrm{Stab}_{S_m}(1,\ldots,i-1)/\mathrm{Stab}_{S_m}(1,\ldots,i)$ in the factor S_m. (This transversal consists of representatives for each $j \in \{i,\ldots m\}$ that map the j-th block to the i-th block.) We traverse this tree, selecting first all possible t_1, then all possible c_1, then all t_2 and so forth and computing the corresponding conjugates.

As a partial product $t_1c_1t_2c_2 \cdot \cdots \cdot t_ic_i$ defines the initial part $\underset{i}{\overleftarrow{(M^g)}}$, we only need to consider those branches of the tree, for which this initial part is canonical (by condition K1). Condition K2 then serves as a restriction on the possible t_i, condition K3 as a restriction on c_i.

An explicit description of the backtrack algorithm used to construct for a given M its canonical conjugate can be found in [Hulpke, 1996, IV.2].

7.2. Construction of subpower representatives

Since we only want to construct subpowers in canonical form, the construction process can be trimmed down as well: To construct representatives of all subpowers of length m we inductively construct canonical representatives of subpowers of length 1, length 2, and so on up to length m. In each step, we construct the subpowers of length $i+1$ as subdirect products of an initial part $B = \underset{i}{\overleftarrow{M}}$ (which is a subpower of A of length i) with the group A. For each pair (B, A), we compute all pairs of normal subgroups $F \lhd B$ and $E \lhd A$ such that the factor groups B/F and A/E are isomorphic.

To compute the normal subgroups, the algorithm of Hulpke [1998] can be used.

We once precompute the normal subgroups of A and then only need to consider normal subgroups of $B = \overleftarrow{\frac{M}{i}}$ of suitable index.

However, as B often possesses many normal subgroups, and we are only interested in normal subgroups whose factor is isomorphic to a factor of A, the following two shortcuts are used in the case of a solvable A: If the derived length of A is j, we only need to find normal subgroups above the j-th derived subgroup of B.

The second shortcut involves iterated maximal subgroups:

DEFINITION 7.3: *Let G be a group, $U \leq G$ and $j \in \mathbb{N}$. We say that U is a j-ply maximal subgroup of G is there is a chain of subgroups $G = M_0 \geq M_1 \geq \cdots \geq M_j = U$ such that $M_i \leq M_{i-1}$ is a maximal subgroup. (We do not require a chain of minimal length.)*

Now suppose that every normal subgroup in A is the core of a j-ply maximal subgroup of A (in practice often $j \leq 2$). In this case we compute (by the method of Eick [1993]) the kernels of all j-ply maximal subgroups of B.

Because of conditions K2 and K3 we only need to consider the case that F is small under $N_{C \wr S_{i-1}}(B)$ and E is small under C. We can therefore reduce the choice of E and F to suitable orbit representatives.

For each such pair (F, E) we consider all isomorphisms $\chi\colon B/F \to A/E$. These isomorphisms are given by one isomorphism, and the automorphisms of the factor group (again precomputed once for all factor groups of A).

Furthermore we only need to consider these automorphisms of the factor group up to automorphisms induced by $N_{N_{C \wr S_{i-1}}(B)}(F)$, respectively by $N_C(E)$.

For each isomorphism obtained this way, we form the corresponding subdirect product M. We finally compute the canonical representative of this M and check by comparison whether M is canonical and collect all canonical representatives found in a list.

REMARK 7.4: *In practice it is worth to delay the – expensive – canonicity test to situations in which two subpowers have been constructed which are not known to be non-conjugate due to invariants such as the orders of the groups, orders of the derived subgroups, cycle structures of elements and – for small groups – even isomorphism type.*

Only in the case that two groups with the same set of invariants arise, both groups are tested for canonicity and those groups that are non-canonical representatives (it could be either group or both or none) are discarded.

The algorithm thus keeps a list of verified canonical representatives and a second list of "presumably canonical" representatives. At the end of the construction process the groups remaining in this list (i.e. each of the groups is uniquely determined by its invariants among all constructed groups) are automatically proven to be canonical as they could not be conjugate to any other group.

Again, for explicit pseudo-code and an example construction the reader is referred to [Hulpke, 1996, IV.3].

8. Transitivity Conditions

As described so far, the algorithm constructs all W-classes of subdirect products. Once m gets larger (usually beyond 6 or 7), however, their number gets in the range of a few hundred and construction can become exceedingly tiresome. On the other hand, we are only interested in subpowers that can be the base group of a transitive group. So all subpowers that cannot lead to such a base group can be discarded immediately, reducing the number of objects to be investigated.

The first reduction of this kind is straightforward: Once a subpower of (full) length m has been constructed, we compute its normalizer in $W = C \wr S_m$ and check whether it acts transitively and whether the normalizer admits block systems of smaller block size (in which case the block system used for the construction is not pertinent to the resulting transitive groups due to property P1). If either of these is the case, the group is immediately discarded before checking for canonicity.

Much more desirable, however, is a criterion that will prune the construction tree at higher level branches, if they cannot lead to a subpower with transitive normalizer action. For this we study the interaction of the different projections of a subdirect product:

8.1. Component Projections and Signatures

DEFINITION 8.1: *Let* $M_i := \ker(\pi_i) \cap M = \{(a_1, \ldots, a_m) \in M \mid a_i = 1\}$ *and let* $M_i^{\rightarrow j} := M_i\pi_j$.

We now fix two components $1 \le i < j \le m$ and define

$$\varpi := (\pi_i, \pi_j)\colon \begin{array}{ccc} C^{\times m} & \to & C \times C \\ (c_1, \ldots, c_i) & \mapsto & (c_i, c_j) \end{array}$$

Then $M\varpi$ is a subdirect product of A_i with A_j induced by the normal subgroups $M_i^j \lhd A_j$ and $M_j^i \lhd A_i$. The corresponding factor groups must be isomorphic, thus

$$A/M_i^{\rightarrow j} \cong A/M_j^{\rightarrow i}. \tag{2}$$

If we identify $C^{\times i}$ with $C^{\times m}\mu_i$ we have that $\mu_j\pi_i = \pi_i$ for $i \le j$. We therefore can compare the projections of M with those of an initial part of M:

LEMMA 8.1: *For* $i, j \le k \le m$ *we have* $M_i^{\rightarrow j} = \left(\overleftarrow{\frac{M}{k}}\right)_i^{\rightarrow j}$

Proof:

$$\begin{aligned} M_i^{\rightarrow j} &= \{m\pi_j \mid m \in M, m\pi_i = 1\} = \{m\mu_k\pi_j \mid m\mu_k \in M\mu_k = \overleftarrow{\frac{M}{k}}, m\mu_k\pi_i = 1\} \\ &= \{m\pi_j \mid m \in \overleftarrow{\frac{M}{k}}, m\pi_i = 1\} = \left(\overleftarrow{\frac{M}{k}}\right)_i^{\rightarrow j} \end{aligned}$$

□

Again, let $W := C \wr S_m = C^{\times m} \rtimes S_m$ and $N := N_W(M)$. Then N permutes the blocks in $\mathcal{B}$ via the action $\varphi\colon N \to R \leq S_m$. We now shall define an action of R on the set of the M_i:

LEMMA 8.2: *Let $g \in N$ with $j^{g\varphi} = i$. The automorphism of M induced by g is called θ. Then there is an $\alpha \in \mathrm{Aut}(A)$, induced by some element $c \in C$ such that*

$$\theta\pi_i = \pi_j\alpha = \pi_{(i^{(g^{-1}\varphi)})}\alpha, \tag{3}$$

Proof: Let $g = rc$ be a decomposition according to the semidirect product structure of W with $c = (c_1, \ldots, c_m) \in C^{\times m}$ and r permuting the components as $g\varphi$. For $m \in M$ we have

$$m\theta\pi_i = (c^{-1}r^{-1}mrc)\pi_i = ((m^r)^c)\,\pi_i = ((m^r)\pi_i)^{(c\pi_i)} = (m\pi_j)^{c_i} = m\pi_j\alpha,$$

with α denoting the inner automorphism of C induced by c_i. □

LEMMA 8.3: *For $g \in N$ we have $(M_i)^g = M_{(i^{(g\varphi)})}$.*

Proof: We have

$$(M_i)^g = \{m^g \mid m \in M, m\pi_i = 1\} = \{m \in M \mid (m^{g^{-1}})\pi_i = 1\}.$$

Inverting (3) yields $m^{g^{-1}}\pi_i = m\pi_{(i^{(g\varphi)})}\alpha^{-1}$ with α induced by an element of C. Therefore

$$(M_i)^g = \{m \in M \mid m(\pi_{(i^{(g\varphi)})}) = 1\alpha = 1\} = M_{(i^{(g\varphi)})}.$$

□

Thus for $r \in R$ the action

$$(M_i)^r := (M_i)^g = M_{i^r} \tag{4}$$

with $g\varphi = r$ is well defined and acts as a group isomorphism. Consequentially a transitive action of N *implies a transitive action of $R \leq S_m$ on the set $\{M_i\}$.*

We now examine the influence of this action on the $M_i^{\rightarrow j}$. By Lemma 8.2 the action of $g \in N$ may introduce automorphisms α induced by an element of C. Therefore we consider classes $[E]$ of normal subgroups $E \lhd A$ defined by

$$[E] = [F] :\Leftrightarrow A/E \cong A/F.$$

These classes obviously encompass classes given by conjugacy with C, however they are much easier to compute as they do not requitre a conjugacy test.

REMARK 8.2: *The following analysis does not use the particular definition of these classes. In practice one can replace $[\cdot]$ by a weaker equivalence, for example comparison of the groups orders, which is cheaper to check.*

By (2) we have $\left[M_i^{\rightarrow j}\right] = \left[M_j^{\rightarrow i}\right]$. Furthermore, Lemma 8.2 and 8.3 imply for $r \in R$ with $g\varphi = r$ that $M_{ir}^{\rightarrow j} = M_{ir}^{\rightarrow}\pi_j = (M_i^{\rightarrow})^g\pi_j = M_i^{\rightarrow j^{(r^{-1})}}\alpha$ for $\alpha \in \mathrm{Aut}(A)$. This implies that $A/M_{ir}^{\rightarrow j} \cong A/M_i^{\rightarrow j^{(r^{-1})}}$. Setting $j = k^r$ we get that

$$\left[M_i^{\rightarrow k}\right] = \left[M_{ir}^{\rightarrow k^r}\right]. \tag{5}$$

Thus the values of $\left[M_i^{\rightarrow j}\right]$ are constant on R-orbits.

THEOREM 8.3 (TRANSITIVITY CRITERION): *If the normalizer of M acts* transitively *on the m blocks (and thus R acts transitively on the points $\{1,\ldots,m\}$), we have for all $1 \le i,j \le m$:*

$$\left\{\left[M_i^{\rightarrow k}\right] \mid k \neq i\right\} = \left\{\left[M_j^{\rightarrow k}\right] \mid k \neq j\right\}$$

(counting multiplicities).

In other words: a subpower M may only afford a transitive normalizing action if the symmetric matrix $\left(\left[M_i^{\rightarrow j}\right]\right)_{i,j}$ possesses the entries $[E]$ in all rows with equal frequencies:

$$\forall E \lhd A \quad \exists e \in \mathbb{N}_0 : \quad \forall 1 \le i \le m : \quad \left|\{j \mid M_i^{\rightarrow j} = [E]\}\right| = e$$

Now let $\mathrm{Okl}(M) := \{[M_i^{\rightarrow j}] \mid 1 \le i,j \le m\}$ be the set of the occurring kernel classes.

DEFINITION 8.4: *For $K \in \mathrm{Okl}(M)$ we define a Relation $\sim_K$ on $\{1,\ldots,m\}$ by*

$$i \sim_K j :\Leftrightarrow [M_i^{\rightarrow j}] = K.$$

By (2) this relation is symmetric, it is trivially reflexive. The transitive closure (also denoted by $\sim_K$) thus is an equivalence relation.

By (5) this relation is R-invariant:

LEMMA 8.4: *The $\sim_K$-classes form a block system for the action of R on $\{1,\ldots,m\}$.*

We can use this relation (see section 11) to give an improved upper bound for the normalizer of M. We also note immediately:

COROLLARY 8.1: *If R is transitive, all $\sim_K$-classes must be of equal order.*

To simplify counting arguments needed when applying Theorem (8.3) we now define objects which count frequencies:

DEFINITION 8.5: *Let $\mathcal{N}$ be the set of $[\cdot]$-classes of normal subgroups of A:*

$$\mathcal{N} = \{[E] \mid A/E \cong A/E' \text{ for all } E' \in [E]\}$$

and let $\mathcal{S}$ be the free abelian group on $\mathcal{N}$ (written multiplicatively). For

$$s = \prod_{[E]\in\mathcal{N}} [E]^{a_E} \in \mathcal{S}$$

we call $\deg(s) = \sum a_E$ the degree *of s. We call such an element s a* signature *if $a_E \ge 0$ for all $[E] \in \mathcal{N}$.*

If $s,t \in \mathcal{S}$ are signatures such that s/t is a signature, we say that t divides s, written $t \mid s$. Furthermore we define for $s = \prod [E]^{s_E}$ and $t = \prod [E]^{t_E}$ the least common multiple

$$\mathrm{lcm}(s,t) = \prod_{[E]\in\mathcal{N}} [E]^{\max(s_E,t_E)}.$$

(It is easily seen that it behaves in the same way as the lcm of positive integers.)

Definition 8.6: *If M is a subpower of A of length m and $[E] \in \mathcal{N}$ let*

$$a_E(i) := \left|\{1 \le j \le m \mid \left[M_i^{\rightarrow j}\right] = [E]\}\right|$$

We call $\mathrm{sign}_i(M) = \prod_{[E]\in\mathcal{N}} [E]^{a_E(i)}$ *the i-th signature of M. If* $\mathrm{sign}_i(M) = s \in \mathcal{S}$ *for all $1 \le i \le m$, we say that M is* in parity *and simply call* $\mathrm{sign}(M) := s$ *the signature of M.*

We collect some easy consequences of these definitions:

1. $\deg(\mathrm{sign}_i(M)) = \mathrm{length}(M)$ (every component adds one to the degree).
2. For all $j \le i \le m$ we have $\mathrm{sign}_j\left(\overleftarrow{\underset{i}{M}}\right) \mid \mathrm{sign}_j(M)$ by Lemma 8.1.
3. If $N = N_{S_n}(M)$ is transitive, M is in parity by Theorem 8.3.

Additionally we obtain a criterion whether an initial part may be completed to a subpower which is a base group of a transitive group:

Theorem 8.7 (Initial part criterion): *Take a subpower M of length i. If there is a transitive, imprimitive G with base group $\widetilde{M}$ such that $M = \overleftarrow{\underset{i}{\widetilde{M}}}$ we have that*

$$\mathrm{lcm}_{1\le j\le i}(\mathrm{sign}_j(M)) \mid \mathrm{sign}(\widetilde{M}).$$

In particular, we have

$$\mathrm{length}(\widetilde{M}) \ge \deg(\mathrm{lcm}_{1\le j\le i}(\mathrm{sign}_j(M)).$$

Proof: As a base group $\widetilde{M}$ is in parity. On the other hand the signatures of the initial part (and thus their lcm) must divide the signature of $\widetilde{M}$. The last claim follows as $\mathrm{length}(\widetilde{M}) = \deg(\mathrm{sign}(\widetilde{M}))$. □

8.2. Application to the construction process

Assume we have constructed a subpower M of length $i < m$ and we want to see whether extending M can lead to a subpower $\widetilde{M}$ of length m with transitive block action. (If it cannot, we can discard M and do not need to construct subpowers arising from M. This cuts off a whole branch in the recursive construction tree.)

By Theorem 8.7, we need that $\mathrm{length}(\mathrm{lcm}_{1\le j\le i}(\mathrm{sign}_j(M))) \le m$. If this is not the case, M can be discarded.

Even better pruning can be obtained by using the fact that $\widetilde{M}$ must be in parity. We consider the matrix of block kernel projections, whose x, y entry is the class $\left[\widetilde{M_x^{\to y}}\right]$. By Lemma 8.1, the matrix $[M_x^{\to y}]$, consisting of the kernel projection classes of M, gives the minor consisting of the first i rows and columns of this matrix. We can try to complete this minor to a full matrix (potential projections for $\widetilde{M}$) by adding (pairs of) entries that keep the matrix symmetric, with diagonal 1 and compatible with the lcm of the signatures. If this turns out to be impossible, M cannot extend to a subpower in parity and can be discarded.

For example, suppose a subpower of length 4 gives the projection matrix (the numbers can be considered as arbitrary names of factor groups):

$$\begin{pmatrix} 1 & 1 & 6 & 6 \\ 1 & 1 & 6 & 6 \\ 6 & 6 & 1 & 3 \\ 6 & 6 & 3 & 1 \end{pmatrix}.$$

Then the lcm of the signatures is $1^2 + 3 + 6^2$ of length 5. However trying to complete the matrix to a 5×5 matrix (adding the only possible row and column entries to get the desired signature) yields

$$\begin{pmatrix} 1 & 1 & 6 & 6 & 3 \\ 1 & 1 & 6 & 6 & 3 \\ 6 & 6 & 1 & 3 & 1 \\ 6 & 6 & 3 & 1 & 1 \\ 3 & 3 & 1 & 1 & 1 \end{pmatrix},$$

in which the last row does not have the required signature. So this subpower of length 4 cannot lead to extension of length 5 in parity.

For a larger m there often is a potential choice for certain extending entries. Without loss of generality (this amounts to renumbering the components by which we extend) we can set for each new row one value arbitrarily (as far as compatible with the lcm of the signatures) to reduce the number of choices.

9. Bases as invariant subgroups

By Theorem 3.1, we can embed a transitive group G into $C \wr T$ with $C = N_{S_l}(A)$ and $T = G\varphi = G/M$. In this embedding the base group $M \lhd G$ becomes a subgroup of $A^{\times m} \lhd C \wr T$. Conjugation with coset representatives in G induces a homomorphism $\alpha\colon T \to \mathrm{Aut}(A^{\times m})$. Conjugation with the complement in the wreath product induces another homomorphism $\beta\colon T \to \mathrm{Aut}(A^{\times m})$. While α depends on the group G, β is given by the wreath product structure.

Now suppose, that α is induced by β (for a choice of an isomorphism between G/M and a complement to $C^{\times m}$ in $C \wr T$), i.e.

$$a^{t\alpha} = a^{t\beta} \text{ for all } a \in A^{\times m}, t \in T. \tag{6}$$

Then M is a subgroup of $A^{\times m}$ which is invariant under the (known) action of T via β. Furthermore T contains a minimal transitive subgroup $\hat{T}$, and M is invariant under $\hat{T}$ as well.

If we know a priori, that condition (6) is always fulfilled for a given A and all minimally transitive T of a given degree (by remark 3.3 these are sufficient to find the possible M), we can therefore obtain all possible base groups as those subgroups of $A^{\times m}$, which are invariant under the action of a complement to $C^{\times m}$ in $C \wr T$.

Let us examine therefore, in which cases condition (6) is fulfilled. We first note, that this is not always the case:

Remark 9.1: *Let*

$$\begin{aligned} G &= \langle (1,4,7)(2,5,8)(3,6,9)(10,11,18)(12,13,14)(15,16,17), \\ &\quad (1,10,2,11,3,12,5,14)(4,13,6,15,9,18,7,16)(8,17)\rangle \end{aligned}$$

which is transitive of degree 18 and of order 72. The partition

$$\mathcal{B} = \left\{ \{1,2,\ldots,9\}, \{10,11,\ldots,18\} \right\}$$

is a minimal block system of G. The action on the blocks has image $T = \langle (1,2)\rangle$. Its kernel is

$$\begin{aligned} M &= \langle (2,5,9,6)(3,4,8,7)(10,15,16,11)(12,18,14,17), \\ &\quad (1,2,9)(3,4,5)(6,7,8)(10,12,17)(11,13,15)(14,16,18)\rangle \end{aligned}$$

of order 36. *The stabilizer of the block $\{1,\ldots,9\}$ acts on this block as*

$$C = \langle (2,9)(3,8)(4,7)(5,6), (1,3,6,4)(2,7,8,9)\rangle$$

which is isomorphic to $E(9)$:4, the 9th transitive group of degree 9. Thus G embeds in $W = C \wr T$. In this wreath product, the (only) class of complements to its base group is

$$T \cong K = \langle (1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18)\rangle$$

which has 36 conjugates. However M is not invariant under either of these conjugates (its normalizer in each of them is trivial).

Lemma 9.1: *Condition (6) is fulfilled when at least one of the following holds:*

a) $l = 2$.

b) A is abelian and for all minimal transitive groups $\hat{T}$ of degree m the condition $\gcd(\left|\mathrm{Stab}_{\hat{T}}(1)\right|, [C{:}A]) = 1$ *holds.*

c) A is abelian and m is prime.

d) For all minimal transitive groups $\widehat{T}$ of degree m: $\gcd\left(\left|\widehat{T}\right|, |A|\right) = 1$ *holds.*

Proof: a) S_2 is abelian, thus C^m does not act on itself and the action of G on $C \wr T$ is induced by the action of the natural complement T.

In the other cases we assume by remark 3.3 that G/M is minimal transitive and $T = \hat{T}$:

b) By (1) the index of A in the image $U\psi$ of the action of $\mathrm{Stab}_G(\mathrm{B}_1)$ on B_1 divides $|\mathrm{Stab}_T(1)|$. On the other hand, $U\psi \leq C$. If $\gcd(|\mathrm{Stab}_T(1)|, [C{:}A]) = 1$, we have that $[U\psi{:}A] = 1$. By Theorem 3.1, G thus embeds in $A \wr T$ and each element of G acts on $A^{\times m}$ as a complement does.

c) Minimal transitive groups of prime degree are cyclic. So $|\mathrm{Stab}_T(1)| = 1$ in b).

d) The gcd criterion means that there must be a complement in G to M by the Schur-Zassenhaus theorem [Zassenhaus, 1958, Thm.IV.27]. This complement also is a complement to $C^{\times m}$ in $C \wr T$. □

In each of these cases, we compute representatives of the classes of complements (there might be several complement classes) to $C^{\times m}$ in $C \wr T$, where T runs through the minimal transitive groups of degree m, and compute the subgroups of $A^{\times m}$ invariant under either of these complements. All possible base groups M must be among these invariant subgroups.

If A is abelian, the invariant subgroups are submodules one can obtain via the algorithm of Lux et al. [1994]; if A is a solvable group, the invariant subgroups algorithm of Hulpke [1999] can be used.

Not all resulting invariant subgroups of $A^{\times m}$ will project surjectively onto A in each component. Again, these have to be filtered out. (This surjectivity also can be used directly as a criterion in the algorithm of Hulpke [1999] to avoid constructing some unsuitable groups in the first place.)

There are further variants of Lemma 9.1: Instead of using the full transitive action, we can take the preimage $H \leq G$ of an *intransitive* subgroup $H\varphi \leq G\varphi$. If $\gcd(|A|, [H{:}M]) = 1$, there exists a complement to M in H. This complement is a complement to $C^{\times m}$ in the (probably intransitive) wreath product $C \wr (H\varphi)$. If every minimal transitive group of degree m contains such a subgroup $H\varphi$ of order coprime to $|A|$, we can consider subgroups invariant under the respective complements. (Some of the resulting invariant subgroups may not afford a transitive normalizing action. These can be discarded immediately.) However if $H\varphi$ is chosen too small (in particular, if it is the trivial group), there will be too many invariant subgroups to make this approach practical.

Another variant is the case that there is a normal subgroup $L \lhd A$ that is transitive (on m points) and for which with $\gcd(|L|, [A{:}L]) = 1$. So for each subpower $M \leq A^{\times m}$, the intersection $\widetilde{M} := L^{\times m} \cap M \lhd M$ is a characteristic subgroup of M, so $\widetilde{M} \lhd G$. Furthermore, assume that for all minimal transitive groups T of degree m we have that $\gcd(|T|, [A{:}L]) = 1$ (but not $\gcd(|T|, |L|) = 1$). Then (assuming again without loss of generality that $G\varphi$ is minimal transitive) $G/\widetilde{M}$

splits over $M/\widetilde{M}$, a complement yields a subgroup $H \leq G$ with $H\varphi = G\varphi$ and $\widetilde{M} \leq H$. Thus H is transitive as well, but the base group of H is a subpower of L. Obviously M is invariant under H.

In this situation, if we have already constructed all transitive groups H whose base groups are subpowers of L (as we would have when constructing *all* transitive groups) the subgroups of $A^{\times m}$ invariant under *any* of those H yield the subpowers of A that can be base groups. We can apply this for example in the case of $l = 3$, $m = 9$, $n = 27$, $A = S_3$ and $L = A_3$: All minimal transitive groups of degree 9 are regular, and thus of order coprime to $[S_3{:}A_3]$. (In this particular situation this reduces the total runtime from several months to two days.)

REMARK 9.2: *The construction of transitive groups of degree 14 and 15 by Butler [1993] assumes an even stronger criterion: If m is prime, there always is an element of prime order acting by pure block permutation (i.e. a subgroup of the factor of order p has a complement). Unfortunately this condition is too strong even for these degrees: The 22nd group of degree 14,*

$$\left[\tfrac{1}{6}\_F_{42}(7)^2\right] 2_2 \;=\; \langle (1,11,9)(2,4,8)(3,5,13)(6,12,10), \\ (1,12,7,2)(3,4,5,10)(6,9,8,13)(11,14)\rangle\,,$$

has only one block system with two blocks of order 7, and only two conjugacy classes of elements outside the kernel. These classes both contain elements of order 4 (and not order 2).

(Luckily, despite this wrong assertion, the lists of Butler [1993] turn out to be correct.)

9.1. Removal of conjugates

Many of the resulting subgroups of $A^{\times m}$ will be conjugate under the action of $C \wr S_m$. We remove conjugacy duplicates by computing for each subgroup $V \leq A^{\times m}$ a "standard" (defined by the following procedure) conjugate:

A permutation of V with the "smallest" (using an arbitrary total order) cycle structure and the smallest class size in V is to be mapped under $C \wr S_m$ to its lexicographically smallest (comparing permutations by their images of $1, 2, 3, \ldots$) $C \wr S_m$ conjugate (as $V \leq C \wr S_m$ the choice of class elements is unimportant). We find a suitable conjugating element g_1 and conjugate V with it. To preserve the condition, we then restrict conjugation to the centralizer of this smallest element's image (which will be in the class of "smallest" elements in V^{g_1}). We pick the next smallest class of elements in V^{g_1} and map one of its elements to the smallest possible conjugate and so forth.

Sometimes the choice of a "smallest" permutation is not unique. In this case we consider all possibilities and eventually take the smallest resulting group. This leads to a backtrack algorithm whose performance turns out to be reasonably fast for the groups of order at most a few thousand, which occur here. For further details see [Hulpke, 1996, IV.5.4].

The reason for using this process for groups of small order is, that that it turns out to be computationally cheaper than to compute the "canonical" form used for the construction of subpowers in each case. (However it is restricted to small order groups as it quickly becomes memory intensive.) If base groups are constructed as invariant subgroups we will therefore use this "smallest" conjugate as the definition of the "canonical" conjugate.

10. Construction of transitive groups from the base groups

We now describe the second part of the construction: Given a base group M, construct all transitive groups with base group M so that the block system of the construction is pertinent.

Following section 3.2, we compute $N = N_{C \wr S_m}(M)$ as well as the kernel K of the action of N on the set $\mathcal{B}$ of orbits of M. The transitive groups with base group M arise as preimages of complements in S/M to K/M for transitive subgroups $S\varphi \leq N\varphi$.

10.1. Transitive subgroups of the block action

The first sub-task is therefore to compute the classes of transitive subgroups of $R := N\varphi$. If R is small, this can be done by a straightforward subgroup lattice computation, using the methods of Neubüser [1960], Hulpke [1999], Cannon et al. [2001]. If R is the full symmetric group, we can take the lists of transitive groups of degree m (which are assumed to be known a priori). The classes of subgroups of A_m are easily obtained from this list as well: We have to consider only those groups, whose sign is even; the S_m class of a group will split in two A_m classes if and only if the normalizer in S_m is a subgroup of A_m.

If R is the wreath product of symmetric groups, the following theorem classifies its transitive subgroups:

THEOREM 10.1: *Let $T \leq S_m$ be transitive and $R = S_x \wr S_y$ in natural imprimitive action ($m = x \cdot y$). The R-classes of subgroups of R which are permutation isomorphic to T are in bijection to the orbits of $N_{S_m}(T)$ on the block systems of T with blocks of size x.*

Proof: By Theorem 3.1 R has a subgroup which is permutation equivalent to T, if and only if T has a block system with blocks of size x. Each block system yields an embedding of T, vice versa, each embedding imposes the natural block system $\mathcal{B}$ of R as a block system on T.

Suppose that $T, T' \leq R$ are two embeddings of T, belonging (without loss of generality) to the block systems $\mathcal{B}$ and $\mathcal{C}$ of T. The embedding $T' = T^h$ is given by an element $h \in S_m$ that will map the block system $\mathcal{C}$ onto $\mathcal{B}$. If there is $r \in R$ with $T^r = T'$, then $r \cdot h^{-1} \in N_{S_m}(T)$. Since R fixes $\mathcal{B}$, the embedded groups T, T' are thus R-conjugate, if and only if $\mathcal{B}$ and $\mathcal{C}$ are in the same orbit under $N_{S_m}(T)$. □

Again, in the case that $R \lhd S_x \wr S_y$ is of small index, classes of subgroups of this normal subgroup can be deduced easily from those of the wreath product.

REMARK 10.2: *Using the condition given in Theorem 3.1 for $T \leq X \wr Y$ in the natural action, one can strengthen Theorem 10.1 to describe for transitive groups X, Y the classes of transitive subgroups of $X \wr Y$, based on the $N_{S_x}(X)$-classes of transitive subgroups of X (and similar for Y). The resulting parameterization [Hulpke, 1996, Lemma 150] is quite technical and probably by now no longer needed thanks to progress in the calculation of subgroup lattices and maximal subgroups due to Cannon et al. [2001], Eick and Hulpke [2001], Cannon and Holt [in preparation].*

If we consider the groups R which arise when computing the transitive groups of small degree (up to 30), we observe that R is either relatively small (and thus the calculation of the subgroup lattice does not cause problems) or of relatively small index in S_m or a wreath product (and thus one can use one of the parameterizations of subgroups just described). For our purposes the problem of finding the classes of subgroups of R can therefore be considered to have been resolved.

REMARK 10.3: *In general, the question which block action types R are possible for the normalizer of a subpower M remains open. It is not only of theoretical interest, but might become useful in the design of normalizer algorithms. In particular, one can ask:*

> *Given $R \leq S_m$ and a positive integer l. Is there a group $A \leq S_l$ and a subpower $M \leq A^{\times m}$, such that the action of $N_{S_{l \cdot m}}(M)$ on the m blocks is permutation isomorphic to R? Can this always be achieved (for given R) by making l big enough?*

The observations from the construction process show that this is not true for an arbitrary small l. Certainly a necessary condition is to stabilize the subdirect product structure of M (so for example the block projections $M_i^{\rightarrow j}$).

On the other hand it is relatively easy to construct (for a big enough l) groups M (diagonals in direct products and their direct products) such that the image of the normalizer action is a wreath product of symmetric groups.

10.2. Complements

The next step in the construction is to take the preimage S of a transitive subgroup of R and to compute complements to K/M in S/M and to fuse these under $N_{N/M}(S/M)$. We perform these calculations in the factor group N/M (though it also would be possible to work with preimages and thus compute only with subgroups of S_n). The actual transitive groups then are obtained as preimages.

If the factor group N/M is solvable, we can use the approach of Sims [1990]

(see [Theißen, 1997, chapter 6] for adaption to factor groups) to compute a polycyclic presentation for the factor.

Otherwise, we compute a faithful permutation representation of N/M. It is well known [Neumann, 1986, Easdown and Praeger, 1988] that in general this can lead to exponential growth in the permutation degree. However, for the groups arising in this context, it turns out that a battery of heuristics (action on orbits or elements of the normal subgroup, cosets of stabilizers of fixed points or cosets of random subgroups – see [Hulpke, 1996, V.2]) produced permutation representations of workable degree.

In the degree range considered, the factor K/M turned out to be always solvable. (This is due to Schreier's conjecture, as for these small degrees the non-solvable primitive groups are almost simple, and for these groups K/M is a subgroup of $\mathrm{Out}(A)^{\times m}$.) We can therefore use the method of Celler et al. [1990] (using a presentation for the factor S/K which we get from the permutation representation of this group for example by the method of Babai et al. [1997]) to compute complements and fuse these under the action of $N_N(S)/M$.

11. Upper bounds for the normalizer

An essential part of the algorithm is the calculation of normalizers of subpowers in the full symmetric group. The general method used for this is a backtrack algorithm of Theißen [1997], Leon [1991]. Since the runtime of such calculations grows exponentially with the order of the group the normalizer is computed in, it can be beneficial to reduce the order of this group a priori.

The strategies given in this section were used by the author for the purpose of constructing transitive groups and worked well there. Other strategies for a similar purpose are given for example by Miyamoto [2000].

In our situation we have an intransitive subgroup $M \leq S_n$ whose orbits on $1, \ldots, n$ form the set $\mathcal{B} = \{\mathrm{B}_1, \ldots, \mathrm{B}_m\}$ with $|\mathrm{B}_1| = |\mathrm{B}_2| = \cdots = |\mathrm{B}_m| = l$. We denote the orbit actions by $\pi_i \colon M \to S_l$ and assume that all projections have the same image $M\pi = A \leq S_l$. We want to compute $N = N_{S_n}(M)$.

Let $C = N_{S_l}(A)$. We have seen already that $N \leq C \wr S_m$ in its natural imprimitive action with the blocks of $S_l \wr S_m$ arranged to coincide with $\mathcal{B}$.

We now consider the equivalence classes $\sim_K$ (see definition 8.4). By Lemma 8.4 they must form a block system for the action of N. Then the $\sim_K$-induced imprimitivity of the action of N permits us to replace the factor group S_m by a wreath product $S_a \wr S_b$. We thus know that $N \leq C \wr (S_a \wr S_b)$ and can perform the backtrack calculation in this this (smaller) group.

11.1. General Normalizer calculations

The methods described so far generalize to the computation of the normalizer of an arbitrary $G \leq S_n$ in S_n (such calculations are not required for the con-

struction of transitive groups, but they might be of interest independent of the construction).

What we will do is to follow the process outlined above. However, when certain criteria for the transitivity of the normalizer fail, we know that the normalizer will be contained in intransitive subgroups of S_n and we can use these again to reduce the group in which the final backtrack computation will take place. For the remainder of this section let $G \leq S_n$ and $N = N_{S_n}(G)$.

The first reduction now concerns orbits. Let $O_1, \ldots, O_k$ be the orbits of G on $\{1, \ldots, n\}$ and let P_i be the image of the permutation action of G on O_i. Then the normalizer N may map O_i to O_j only if $|O_i| = |O_j|$ and if P_i and P_j are permutation isomorphic. We therefore group the O_i into equivalence classes according to their orders as well (in the case that $|O_i|$ is small enough that a cheap permutation isomorphism test is available, for example following the results of section 13) as permutation isomorphism type of the P_i. Suppose the index sets $I_1, \ldots, I_m$ give these orbits.

For one index set I let G_I be image the of the action of G on the points in $\bigcup_{i \in I_j} O_i$. If $|I| > 1$ we can consider the kernel projections $\left[G_{I_i}^{\rightarrow j}\right]$. We apply the transitivity test of Theorem 8.3 to these. If this test fails to ensure transitivity, the orbits in I can be collected into smaller classes that must remain invariant under the normalizer. If this is the case, we replace the I_j by smaller index sets that reflect this refinement.

For the index set I_j we also set $l_j = |O_i|$ for one $i \in I_j$ as well as $Q_j = P_i$ for such an i. Then

$$\begin{aligned} N &\leq \left(\left(\bigtimes_{j \in I_1} N_{S_{l_1}}(P_j)\right) \rtimes S_{|I_1|}\right) \times \cdots \times \left(\left(\bigtimes_{j \in I_m} N_{S_{l_m}}(P_j)\right) \rtimes S_{|I_m|}\right) \\ &\cong \left(N_{S_{l_1}}(Q_1) \wr S_{|I_1|}\right) \times \cdots \times \left(N_{S_{l_m}}(Q_m) \wr S_{|I_m|}\right) = N_1 \times \cdots \times N_m \end{aligned}$$

Normalisation must take place separately in each component of this direct product. We therefore again consider the images $G_j = G_{I_j}$ of the action on the unions of orbits and get that

$$N \leq N_{N_1}(G_1) \times \cdots N_{N_m}(G_m)$$

In the computation of $N_{N_j}(G_j)$ we cannot do further reductions to intransitive groups, but we might be able to reduce the wreath product N_i:

If G_j acts intransitively on $\bigcup_{i \in I_j} O_i$ (this is the situation examined above in the construction process), we proceed as above and compute the equivalence classes $\sim_K$. If these give (by Lemma 8.4) the existence of block systems, we can replace the factor group $S_{|I_j|}$ by a wreath product $S_a \wr S_b$ and replace N_j by $N_{S_{l_j}}(Q_j) \wr (S_a \wr S_b)$.

If G_j acts transitively we consider instead block systems of G_j on $\bigcup_{i \in I_j} O_i$. If a block system is uniquely determined among all block systems of G by its block size a (or the image of the action on the blocks or the image of a block stabilizers

action on its blocks) this block system must be preserved by the normalizer. Thus we can again replace N_j by an iterated wreath product $N_{S_{l_j}}(Q_j) \wr (S_a \wr S_b)$. the same refinement is possible if a block system becomes unique by other properties, for example the order of the corresponding base group or the permutation type of the image of the action on the blocks.

Taken together these reductions can substantially enhance the computation of normalizers in the symmetric group.

12. Results

The algorithm described in the preceding sections has been used to verify the classification of the transitive groups of degree up to 15 and to classify the (hitherto unclassified) transitive groups of (non-prime) degrees between 16 and 30. Table 1 gives the numbers of groups of these degrees. (Degree 30 seems to be a reasonable choice to stop a classification. A partial run of the construction program for degree 32 produced over 150 000 groups in one subcase, before the program had to be stopped for lack of memory.) On a 933MHz Pentium III,

Degree	2	3	4	5	6	7	8	9	10	11
primitive	1	2	2	5	4	7	7	11	9	8
transitive	1	2	5	5	16	7	50	34	45	8

Degree	12	13	14	15	16	17	18	19	20	21
primitive	6	9	4	6	22	10	4	8	4	9
transitive	301	9	63	104	**1954**	10	**983**	8	**1117**	**164**

Degree	22	23	24	25	26	27	28	29	30	31
primitive	4	7	5	28	7	15	14	8	4	12
transitive	**59**	7	**25000**	**211**	**96**	**2392**	**1854**	8	**5712**	12

Bold numbers indicate a hitherto unknown result.

Table 1: Transitive groups of degree up to 31

degrees up to 15 take a few minutes each, degrees 16-22 a few hours, degrees 24-30 are done in one or two days each.

Naturally, the large number of groups makes it unsuitable to list them in printed form. The groups will therefore be made available in electronic form as a data library for the systems GAP [GAP, 2002] (starting with release 4.3). The groups will also be available (indexed in the same way) in the system MAGMA [Bosma et al., 1997].

12.1. Comparison with preliminary results

In comparison to preliminary results reported in Hulpke [1996], Conway et al. [1998], the counts for degrees 24,27 and 28 have been amended. Due to limitations in time and the computers available to the author, these calculations had to be done originally in parts, could be done only once, and some of the code had not yet been extensively tested. This caused a couple of errors which gave way to changed counts:

The now smaller number of groups in degree 24 could be traced back to a duplication of a base group which got introduced when pasting together results of partial runs.

In degree 27 one base group (a subpower of S_3 which was obtained as an invariant group using the special degree 27 argument described before remark 9.2) was initially missing due to an error in the routine that computes invariant subgroups. The construction has been redone also without using this shortcut to verify that the problem has been resolved

In degree 28 the conjugacy test for complements failed twice, while two inflated groups were not detected to be conjugate. Again, this was traced back to the conjugacy test.

In all cases the methods described in the following section have been used to ensure correctness of the numbers given in Table 1.

12.2. Correctness of the results

For a classification of this magnitude (and in view of the history of the problem reported in section 2 and in the previous section) correctness of the result is a principal concern. Errors can be twofold:

1) Two representatives are in fact conjugate.
2) Class representatives are missing.

To eliminate errors of type 1 the obtained groups were checked for conjugates, using the methods of section 13. In all cases the groups could either be distinguished by invariants, or an explicit conjugacy test in the symmetric group proved them non-conjugate. This gives high confidence that errors of type 1 have been eliminated.

Errors of type 2 are much more difficult to assess. Potential error sources include

a) Theoretical errors in the construction process.
b) Clerical errors.
c) Implementation errors for the construction algorithm.
d) Errors in the underlying software, computer hardware etc.

The description of the construction process in this paper aims to convince the reader that type a) errors can be excluded. Errors of type b) were eliminated

as far as possible by automatic handling of the lists of groups (see also subsection 12.1).

Errors of type c) or d) are harder to eliminate. To minimize their impact, the calculation was repeated several times over a period of several years and on different machines. Also, while the initial classification was done in a development version of GAP 3.4.4, the construction program has been converted to GAP 4 (which often provides slightly different implementations of the algorithms used) and the classification been redone there.

Finally, for an independent check, the following test was performed: For every transitive group in the catalog, a list of representatives of its maximal subgroups was computed, using the method of Eick and Hulpke [2001].

From those, the transitive subgroups were selected. For every group in this list, its representative in the catalog was determined (using the methods of section 13) and conjugacy to it established by an explicit conjugacy test. (Similarly to the methods in section 11, this conjugacy test needs only be performed in a wreath product instead of the full symmetric group.)

In the few cases that maximal subgroups of twisted wreath type might arise in degree 30 the following approach was used: Every maximal subgroup of twisted wreath type would be a complement to the socle $S \lhd G$ and would be isomorphic to G/S. Instead of computing complements, the faithful transitive representations of G/S of degree 30 were determined from the subgroup lattice of G/S. (This works well, since $|G/S| < 50000$.) This produced S_{30}-conjugates of all relevant transitive maximal subgroups of this type.

This test also succeeded and gives an independent confirmation of the results. It is hard to imagine a combination of program or hardware errors that would omit a transitive group in both processes.

Remark 12.1: *This test could be considered as a more simple-minded construction of transitive groups. What makes it unsuitable in practice to be used as a construction method on its own is the problem of eliminating duplicates: Since we have already a list of transitive groups, we can use this list to identify each transitive maximal subgroup and only have to perform one conjugacy test (which furthermore is bound to succeed and thus usually does not have to exhaust all possibilities to prove non-conjugacy) for each new group.*

Without such an identification feature, many more conjugacy tests would have to be performed which renders this approach useless for an independent construction.

12.3. Minimally Transitive Groups

Of particular interest are the minimally transitive groups of a given degree. For the considered degrees, these groups have been identified as well:

Following Royle [1987] we first form for each transitive group G (about 30) random proper subgroups and check whether any of these act transitively (if they do, G is not minimally transitive).

Furthermore, if G is imprimitive with block action φ, and $G\varphi$ is not minimally transitive, then G cannot be minimally transitive (remark 3.3). We also check subgroups of G generated by a subgroup of $\ker\varphi$ (for example the derived subgroup or one generated by random elements) and suitable transversal elements of $\ker\varphi$ on whether they act transitively.

These tests provide good filters to eliminate almost all non-minimal groups, in particular most of the remaining groups are small. To finally prove/disprove minimality, we have to compute their maximal subgroups [Eick, 1993, Eick and Hulpke, 2001, Cannon and Holt, in preparation] and check whether any of these acts transitively.

Table 2 gives the orders and indices (corresponding to the indices as used by the transitive groups library in GAP and for degree up to 15 in agreement with Conway et al. [1998]) of the non-regular minimal transitive permutation groups for those degrees up to 30 which are not prime or p^2 (by [Dixon and Mortimer, 1996, Exercise 1.6.21] the minimal transitive groups of degree p^2 are regular). Every regular group is obviously minimally transitive as well, they can be obtained from a list of all groups up to isomorphism, as given for example by Besche and Eick [1999].

An extended list of minimally transitive groups that also gives group generators is not given here for reasons of space; it can be found at `http://www.math.colostate.edu/~hulpke/paper/transgp.html`.

13. Identification of Transitive Groups

Given a group that acts transitively on a domain, it can be useful to identify the image of this action in a library of all possible permutation isomorphism types. Such an identification is also used in various parts of the construction process, for example to distinguish isomorphism classes in pertinence criterion P4.

The easiest way to do this seems to be to check properties of the groups that are invariant under conjugacy. For a first quick elimination of candidates, we use the order of a group, orbit lengths (and action parities) for the action on 2,3 and 4-sets as well as 2-sequences and occurring cycle structures of elements. (This data does not take much storage space and is precomputed once and stored with the groups.) Eliminating all group types which do not agree on all of these invariants usually leaves only a handful or even just one candidate.

The next class of tests has a substantially bigger identification "fingerprint" which therefore is not stored a priori. Instead it is computed for the group to be identified as well as for representatives of the possible remaining classes: We check not only cycle structures, but also the orders of the corresponding classes. Also isomorphism invariants, such as normal subgroups or (if the group is not too big) subgroup lattice are compared.

Finally, if even this test does not lead to a unique identification, an explicit conjugacy test in S_n is performed. (This is necessary on average for two or three classes in each thousand classes of groups.)

Degree	Groups
6	**12**: 4 **36**: 10
10	**20**: 4 **60**: 7 **80**: 8 **200**: 18
12	**24**: 7, 9 **36**: 17 **48**: 31 **72**: 34, 40, 46, 47 **96**: 57 **576**: 162, 166 **2592**: 246
14	**56**: 6 **168**: 10 **196**: 12 **1092**:30
15	**60**: 5 **75**: 9 **405**: 26
16	**32**: 33, 36, 40, 42, 49, 53 **64**: 77, 88, 90, 91, 92, 101, 108, 123, 127, 140, 160, 167, 170, 171, 173, 174 **128**: 212, 295, 323, 335, 343, 358, 363, 372, 375, 377 **256**: 555, 556, 559, 575, 585, 587, 589, 598, 609, 612, 620, 637, 643, 651, 682, 684, 695, 703 **1024**: 1118, 1133, 1146, 1187, 1196, 1207, 1210, 1212, 1229, 1232 **2048**: 1418
18	**36**: 7, 8, 10 **72**: 28 **108**: 44, 49, 54 **324**: 130, 141, 142, 143 **576**: 177 **972**: 246, 259 **1296**: 280 **2448**: 377 **34992**: 688 **69984**: 753
20	**40**: 13 **60**: 15 **80**: 17, 23 **120**: 31, 32 **160**: 43, 44 **200**: 47, 50, 55, 56 **320**: 79, 83 **360**: 89 **400**: 107, 110, 115 **720**: 146, 148 **800**: 161 **960**: 172 **1280**: 188, 193 **2560**: 239, 245, 247 **10000**: 385, 392, 399, 402 **20000**: 473, 478, 496, 501 **40000**: 596, 621, 628 **51200**: 651 **160000**: 818, 820 **518400**: 939
21	**3087**: 35 **5103**: 39 **20160**: 67
22	**484**: 8 **7920**: 22 **11264**: 23 **443520**: 38
24	**48**: 47, 50, 51, 55, 56, 57, 58, 59 **72**: 63, 72, 76, 81, 82 **96**: 93, 94, 96, 122, 174, 179, 180, 181, 184, 187, 191, 194, 198 **144**: 213, 214, 215, 216, 238, 239, 240, 241, 255, 257, 258, 259, 263, 267, 268, 273, 278 **192**: 307, 308, 309, 310, 311, 312, 315, 316, 317, 378, 379, 389, 424, 460, 468, 470, 481, 483, 496, 506 **288**: 596, 597, 598, 620, 622 **384**: 731, 945, 992, 998, 1027 **576**: 1371, 1392, 1410, 1489, 1491, 1505, 1506, 1508 **768**: 1633, 1634, 2128, 2129, 2130 **1152**: 2788, 2801, 2808, 2814 **1296**: 2898, 2901, 2902, 2928, 2937, 2939, 2941, 2943, 2944, 2946 **1536**: 3075, 3098 **2304**: 5077, 5078 **2592**: 5268, 5275, 5276, 5277, 5278, 5279, 5280, 5281, 5289, 5295, 5299 **3072**: 5509, 5535, 5693, 5872, 5873 **4608**: 7443, 7444, 7445, 7446, 7447, 7448 **5184**: 7688, 7690, 7692, 7694, 7695, 7696, 7697, 7729, 7731, 7737, 7754 **6144**: 7882, 7905 **6912**: 9630 **9216**: 9853, 9860, 9865, 9867 **10368**: 10036, 10162, 10163 **12288**: 10283 **18432**: 12266, 12269 **419904**: 20212, 20218, 20224, 20227, 20230, 20235, 20237, 20244 **663552**: 20656 **839808**: 21163, 21167, 21168, 21177, 21178, 21180, 21183 **1327104**: 21809 **1679616**: 21987, 21988, 21989, 21990, 21991, 22004, 22005, 22006, 22007, 22010, 22012, 22238, 22240, 22241, 22242, 22243, 22244, 22245 **3981312**: 23148, 23149 **6718464**: 23500, 23502, 23504, 23506, 23508, 23510, 23649, 23651, 23654, 23655 **13436928**: 23990
26	**52**: 4 **1352**: 20 **5616**: 39 **7800**: 42 **53248**: 64
27	**81**: 19, 24, 25, 26 **729**: 234, 235, 240, 242, 246, 247, 252, 253, 254 **19683**: 981, 988
28	**56**: 11 **112**: 20 **168**: 32 **196**: 35 **336**: 42, 43 **392**: 48, 55, 56, 57, 58 **448**: 61, 66 **896**: 98, 105 **1092**: 120 **1344**: 152, 153 **2184**: 200, 201 **3584**: 262, 263 **10752**: 371 **76832**: 630 **172032**: 795 **802816**: 1169
30	**60**: 6, 7, 9, 11 **120**: 25, 30 **150**: 35, 37, 38, 40 **180**: 45, 46, 48, 49 **240**: 50, 52 **300**: 70, 71, 78 **600**: 126, 131, 142, 143, 158 **720**: 162, 171 **810**: 190, 191, 192, 193 **960**: 216, 217 **1500**: 271, 277, 279, 281 **1620**: 293, 295, 296, 298, 299, 300, 302 **1800**: 321 **4860**: 549, 558 **6000**: 588, 589 **6480**: 629 **14400**: 817 **15000**: 866 **19440**: 908, 909, 911, 912, 920, 924 **22500**: 933, 935 **43740**: 1168 **45000**: 1180 **307200**: 1705 **414720**: 1801 **1312200**: 2104, 2107 **1500000**: 2165, 2191 **3000000**: 2420 **6000000**: 2763 **12000000**: 3141 **75582720**: 4096, 4105 **151165440**: 4370, 4376, 4378

Groups are listed by their index number (as given by GAP), bold numbers give orders. An underlined index indicates the group is not solvable.

Table 2: Indices of non-regular minimally transitive groups

Such a test, that returns the index number of the class of a transitive group, is available in GAP via the command `TransitiveIdentification`.

In most cases these tests work very quickly. There are however two pairs of groups in degree 30, with indices 2230, 2231 (structure $5^6.A_5.2$) as well as indices 4335, 4339 (structure $5^6.2^6.A_5.2$), in which both groups have very similar structure and are therefore hard to distinguish. For these two pairs the fastest identification is to do an explicit isomorphism test.

In fact it turns out that the second pair of groups (indices 4335/4339) is a Brauer pair (that is both groups have the same character table, including power maps, see Lux and Pahlings [1999]). To the author's knowledge this is the first example of a Brauer pair of non-solvable groups for which no proper factor groups form a Brauer pair.

14. Acknowledgment

Much of the initial work in this article was done for the author's dissertation at RWTH Aachen under the supervision of J. Neubüser.

The author would like to thank Gene Cooperman, Steve Linton, Lehrstuhl D für Mathematik of RWTH, CICMA at Concordia University, the Department of Mathematics at Ohio State, and the Department of Mathematics at Colorado State for providing computing resources that were used during parts of the construction and the subsequent verification.

Finally thanks are due to two referees for a thorough reading and many helpful remarks.

The classification of groups would have been impossible without the system GAP.

References

Academie des sciences. Grand prix de mathématiques. *C. R. Acad. Sci. Paris*, XLIV:793–795, 1857.

László Babai, Albert J. Goodman, William M. Kantor, Eugene M. Luks, and Péter P. Pálfy. Short presentations for finite groups. *J. Algebra*, 194:97–112, 1997.

Hans Ulrich Besche and Bettina Eick. The groups of order at most 1000 except 512 and 768. *J. Symbolic Comput.*, 27(4):405–413, 1999.

W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system I: The user language. *J. Symbolic Comput.*, 24(3/4):235–265, 1997.

Greg Butler. The transitive groups of degree fourteen and fifteen. *J. Symbolic Comput.*, 16:413–422, 1993.

Gregory Butler and John McKay. The transitive groups of degree up to 11. *Comm. Algebra*, 11:863–911, 1983.

John Cannon, Bruce Cox, and Derek Holt. Computing the subgroup lattice of a permutation group. *J. Symbolic Comput.*, 31(1/2):149–161, 2001.

John Cannon and Derek Holt. Computing maximal subgroups of finite groups. in preparation.

Frank Celler, Joachim Neubüser, and Charles R. B. Wright. Some remarks on the computation of complements and normalizers in soluble groups. *Acta Appl. Math.*, 21:57–76, 1990.

Frank N. Cole. List of the transitive substitution groups of ten and eleven letters. *Quart. J. Pure Appl. Math.*, 27:39–50, 1895. Corrigendum in Miller [1894/1895].

John H. Conway, Alexander Hulpke, and John McKay. On transitive permutation groups. *LMS J. Comput. Math.*, 1:1–8, 1998.

John D. Dixon and Brian Mortimer. The primitive permutation groups of degree less than 1000. *Math. Proc. Cambridge Philos. Soc.*, 103:213–238, 1988.

John D. Dixon and Brian Mortimer. *Permutation Groups*, volume 163 of *Graduate Texts in Mathematics*. Springer, 1996.

David Easdown and Cheryl E. Praeger. On minimal faithful permutation representations of finite groups. *Bull. Austral. Math. Soc.*, 38:207–220, 1988.

Bettina Eick. PAG-Systeme im Computeralgebrasystem GAP. Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1993.

Bettina Eick and Burkhard Höfling. The solvable primitive permutation groups of degree at most 6560. *LMS J. Comput. Math.*, 6:29–39, 2003.

Bettina Eick and Alexander Hulpke. Computing the maximal subgroups of a permutation group I. In William M. Kantor and Ákos Seress, editors, *Proceedings of the International Conference at The Ohio State University, June 15–19, 1999*, volume 8 of *Ohio State University Mathematical Research Institute Publications*, pages 155–168, Berlin, 2001. de Gruyter.

The GAP Group, `http://www.gap-system.org`. *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002.

Daniel Gorenstein. *Finite simple groups*. Plenum Press, 1982.

Alexander Hulpke. *Konstruktion transitiver Permutationsgruppen*. PhD thesis, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 1996.

Alexander Hulpke. Computing normal subgroups. In Oliver Gloor, editor, *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, pages 194–198. The Association for Computing Machinery, ACM Press, 1998.

Alexander Hulpke. Computing subgroups invariant under a set of automorphisms. *J. Symbolic Comput.*, 27(4):415–427, 1999. (ID jsco.1998.0260).

Alexander Hulpke and Steve Linton. Total ordering on subgroups and cosets. In J.R. Sendra, editor, *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 156–160. The Association for Computing Machinery, ACM Press, 2003.

Camille Jordan. Sur l'énumeration des groupes primitifs pour les dix-sept premiers degrés. *C. R. Acad. Sci. Paris*, 75:1754–1757, 1872.

Marc Krasner and Leo [A.] Kaloujnine. Produit complet des groupes de permutations et problème d'extension de groupes II. *Acta Sci. Math. (Szeged)*, 14: 39–66, 1951.

Harry W. Kuhn. On imprimitive substitution groups. *Amer. J. Math.*, 26: 45–102, 1904.

Jeffrey S. Leon. Permutation group algorithms based on partitions, I: theory and algorithms. *J. Symbolic Comput.*, 12:533–583, 1991.

Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. Ser. A*, 44:389–396, 1988.

Klaus Lux, Jürgen Müller, and Michael Ringe. Peakword Condensation and Submodule Lattices: An Application of the Meat-Axe. *J. Symbolic Comput.*, 17:529–544, 1994.

Klaus Lux and Herbert Pahlings. Computational aspects of representation theory of finite groups. II. In B. H. Matzat, G.-M. Greuel, and G. Hiss, editors, *Algorithmic Algebra and Number Theory*, pages 381–397. Springer, 1999.

George A. Miller. On the non-primitive substitution groups of degree ten. *Bull. Amer. Math. Soc.*, 1:67–72, 1894/1895.

George A. Miller. List of transitive substitution groups of degree twelve. *Quart. J. Pure Appl. Math.*, 28:193–231, 1896. Errata: ibid., 29:249, 1898

George A. Miller. On the transitive substitution groups of degree thirteen and fourteen. *Quart. J. Pure Appl. Math.*, 29:224–249, 1898.

Izumi Miyamoto. Computing normalizers of permutation groups efficiently using isomorphisms of association schemes. In Carlo Traverso, editor, *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*, pages 220–224. ACM Press, 2000.

Joachim Neubüser. Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programmgesteuerten elektronischen Dualmaschine. *Numer. Math.*, 2:280–292, 1960.

Peter M. Neumann. Some algorithms for computing with finite permutation groups. In Edmund F. Robertson and Colin M. Campbell, editors, *Groups – St Andrews 1985*, pages 59–92. Cambridge University Press, 1986.

Robert Remak. Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte. *J. Reine Angew. Math.*, 163:1–44, 1930.

Colva M. Roney-Dougal and William R. Unger. The affine primitive permutation groups of degree less than 1000. *J. Symbolic Comput.*, 35, 2003.

Gordon F. Royle. The transitive groups of degree twelve. *J. Symbolic Comput.*, 4:255–268, 1987.

Martin Schönert and Ákos Seress. Finding blocks of imprimitivity in small base groups in nearly linear time. In *Proc. ISSAC '94*. ACM Press, 1994.

Leonard L. Scott. Representations in characteristic p. In Bruce Cooperstein and Geoffrey Mason, editors, *The Santa Cruz conference on finite groups*, volume 37 of *Proc. Sympos. Pure Math.*, pages 318–331, Providence, RI, 1980. Amer. Math. Soc. Corrigendum in Liebeck et al. [1988].

Mark W. Short. *The Primitive Soluble Permutation Groups of Degree less than 256*, volume 1519 of *Lecture Notes in Mathematics*. Springer, 1992.

Charles C. Sims. Computational methods in the study of permutation groups. In John Leech, editor, *Computational Problems in Abstract Algebra*, pages 169–183. Pergamon press, 1970.

Charles C. Sims. Computing the order of a solvable permutation group. *J. Symbolic Comput.*, 9:699–705, 1990.

Heiko Theißen. *Eine Methode zur Normalisatorberechnung in Permutationsgruppen mit Anwendungen in der Konstruktion primitiver Gruppen*. Dissertation, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 1997.

Hans J. Zassenhaus. *The theory of groups*. Chelsea Publishing Company, New York, 1958.