Orders, Conjugacy Classes, and Coverings of Permutation Groups

by

Attila Maróti

A thesis to be submitted to the University of Szeged
for the degree of Ph. D. in the Faculty of Sciences

August 2007

Acknowledgements

I thank my supervisor, Professor László Pyber for his generous help, patience, and guidance.

Thanks are also due to Professors Ágnes Szendrei, Bálintné Szendrei Mária, László Hatvani, and to Edit Annus.

Contents

Chapter 1

Introduction

Permutation groups arguably form the oldest part of group theory. Their study dates back to the early years of the nineteenth century and, indeed, for a long time groups were always understood to be permutation groups. Although, of course, this is no longer true, permutation groups continue to play an important role in modern group theory through the ubiquity of group actions and the concrete representations which permutation groups provide for abstract groups.

This thesis is built around three papers of the author; all three involving permutation groups. Chapter 3 considers a very old problem going back to Jordan and Bochert of bounding the order of a primitive permutation group of degree n not containing the alternating group A_n. This chapter is taken from [45]. Chapter 4 is an early version of the paper [48]. Here we consider the problem of bounding the number of conjugacy classes of a permutation group of degree $n > 2$. This problem is related to the so-called $k(GV)$-problem of group theory and more distantly to Brauer's $k(B)$-problem of representation theory. The previous problem was solved recently, while the latter is unsolved. The results in Chapter 4 will be used in [28] where we consider the so-called non-coprime $k(GV)$-problem proposed by Guralnick and Tiep in 2004. Finally, Chapter 5 deals with a more combinatorial problem of covering the symmetric groups by proper subgroups. This material is taken directly from [47].

Chapter 2 contains the preliminaries to this thesis. Not everything in Section 2.4 is used later in the text. For more background the reader can use [25] and [20].

Chapter 2

Preliminaries

2.1 Basic definitions

Let Ω be an arbitrary nonempty set; its elements are often called *points*. A bijection of Ω onto itself is called a *permutation* of Ω. The set of all permutations of Ω forms a group, under composition of mappings, called the *symmetric group* on Ω. This group is denoted by $\mathrm{Sym}(\Omega)$. If $\Omega = \{1, 2, \ldots, n\}$ for some positive integer n, then $\mathrm{Sym}(\Omega)$ is abbreviated as S_n. A subgroup of the symmetric group (on Ω) is called a *permutation group* (on Ω).

If G and H are permutation groups on Ω and Δ, respectively, then we say that G is *permutation equivalent* to H if there is a bijection $\phi : \Omega \to \Delta$ and an isomorphism $\psi : G \to H$ such that $(\omega g)\phi = (\omega\phi)(g\psi)$ for all $g \in G$, $\omega \in \Omega$.

Let G be any group and Ω be any nonempty set. Suppose we have a function from $\Omega \times G$ into Ω such that the image of a pair (α, x) is denoted by α^x for every $\alpha \in \Omega$ and $x \in G$. We say that this function defines an *action* of G on Ω (or we say that G *acts on* Ω) if the following two conditions hold.

(i) $\alpha^1 = \alpha$ for all $\alpha \in \Omega$;

(ii) $(\alpha^x)^y = \alpha^{xy}$ for all $\alpha \in \Omega$ and all x, $y \in G$.

For example, if H is any subgroup of any group G, then G acts on the set of right

cosets of H in G in a natural way.

When a group G acts on a set Ω, a typical point α is moved by elements of G to various other points. The set of these images is called the *orbit* of α under G (or the *G-orbit* containing α), and we denote it by $\alpha^G = \{\alpha^x \mid x \in G\}$. A kind of dual role is played by the set of elements in G which fix a specified point α. This is called the *stabilizer* of α in G and is denoted $G_\alpha = \{x \in G \mid \alpha^x = \alpha\}$. Suppose that G is a group acting on a set Ω and that $x, y \in G$ and $\alpha, \beta \in \Omega$. Then the following three statements are true.

(i) Two orbits α^G and β^G are either equal (as sets) or disjoint, so the set of all orbits is a partition of Ω into mutually disjoint subsets.

(ii) The stabilizer G_α is a subgroup of G and $G_\beta = x^{-1}G_\alpha x$ whenever $\beta = \alpha^x$. Moreover, $\alpha^x = \alpha^y$ if and only if $G_\alpha x = G_\alpha y$.

(iii) We have $|\alpha^G| = |G : G_\alpha|$ for all $\alpha \in \Omega$. In particular, if G is finite then $|\alpha^G||G_\alpha| = |G|$.

A group G acting on a set Ω is said to be *transitive* on Ω if it has only one orbit, and so $\alpha^G = \Omega$ for all $\alpha \in \Omega$. Equivalently, G is transitive if for every pair of points $\alpha, \beta \in \Omega$ there exists $x \in G$ such that $\alpha^x = \beta$. A group which is not transitive is called *intransitive*. A group G acting transitively on a set Ω is said to act *regularly* if $G_\alpha = \{1\}$ for each $\alpha \in \Omega$ (equivalently, only the identity fixes any point). Similarly, a permutation group G is called *regular* if it is transitive and only the identity fixes any point.

2.2 Blocks and primitivity

In what follows we shall extend the action of G on Ω to subsets of Ω by defining $\Gamma^x = \{\gamma^x \mid \gamma \in \Gamma\}$ for each $\Gamma \subseteq \Omega$. Let G be a group acting transitively on a set Ω. A nonempty subset Δ of Ω is called a *block* for G if for each $x \in G$ either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \emptyset$. Every group acting transitively on Ω has Ω and the singletons $\{\alpha\}$ ($\alpha \in \Omega$)

as blocks. These two types of blocks are called *trivial blocks*. Any other block is called *nontrivial*. The importance of blocks arises from the following observation. Suppose that G acts transitively on Ω and that Δ is a block for G. Put $\Sigma = \{\Delta^x \mid x \in G\}$. Then the sets in Σ form a partition of Ω and each element of Σ is a block for G. We call Σ the *system of blocks* containing Δ. Now G acts on Σ in an obvious way, and this new action may give useful information about G provided Δ is not a trivial block. Let G be a group acting transitively on a set Ω. We say that the group is *primitive* if G has no nontrivial block on Ω. Otherwise G is called *imprimitive*. We may also talk about primitive and imprimitive permutation groups.

Let G act on a set Ω. This action may be transitive or intransitive. If it is transitive, then it can be primitive or imprimitive. We will mainly be interested in primitive groups. Hence it is useful to mention the following fact. The transitive group G is primitive if and only if the point stabilizer G_α is a maximal subgroup in G for all $\alpha \in \Omega$.

2.3 The Aschbacher-O'Nan-Scott theorem

The so-called Aschbacher-O'Nan-Scott theorem gives a description of finite primitive permutation groups (primitive permutation groups with finitely many elements). This section closely follows the paper of Liebeck, Praeger, Saxl [41]. For more information on individual groups the reader may use [20] as a reference.

A minimal normal subgroup of a nontrivial group X is a normal subgroup $K \neq \{1\}$ of X which does not contain properly any other nontrivial normal subgroup of X. For example, a simple group itself is its only minimal normal subgroup, while an infinite cyclic group has no minimal normal subgroup. The *socle* of a group X is the subgroup generated by the set of all minimal normal subgroups of X. It is denoted by $\mathrm{soc}(X)$. By convention, we put $\mathrm{soc}(X) = \{1\}$ if X has no minimal normal subgroup. Since the set of all minimal normal subgroups of X is mapped into itself by every automorphism

of X, the socle $\mathrm{soc}(X)$ is a characteristic subgroup of X. Every nontrivial finite group has at least one minimal normal subgroup so has a nontrivial socle.

For groups A and B we denote by $A.B$ a (not necessarily split) extension of A and B. The split extension of A by B is denoted by $A : B$.

In what follows, X will be a primitive permutation group on a finite set Ω of size n, and α a point in Ω. Let B be the socle of X. The socle of a finite primitive permutation group is the direct product of a simple group. So in this case, $B \cong T^k$ for some simple group T and some integer $k \geq 1$. Consider the following types of permutation groups: I, II, III(a), III(b), and III(c).

I. Affine groups. Here $T = Z_p$ for some prime p, and B is the unique minimal normal subgroup of X and is regular on Ω of degree $n = p^k$. The set Ω can be identified with $B = (Z_p)^k$ so that X is a subgroup of the affine group $AGL(k, p)$ with B the translation group and $X_\alpha = X \cap GL(k, p)$ irreducible on B.

II. Almost simple groups. Here $k = 1$, T is a non-abelian simple group and $T \leq X \leq \mathrm{Aut}(T)$. Also $T_\alpha \neq 1$.

III. In this case $B \cong T^k$ with $k \geq 2$ and T a nonabelian simple group. We distinguish three types.

III(a). Simple diagonal action. Define

$$W = \{(a_1, \ldots, a_k).\pi \mid a_i \in \mathrm{Aut}(T),\ \pi \in S_k,\ a_i \equiv a_j \bmod \mathrm{Inn}(T) \text{ for all } i \text{ and } j\},$$

where $\pi \in S_k$ just permutes the components a_i naturally. With the obvious multiplication, W is a group with socle $B \cong T^k$, and $W = B.(\mathrm{Out}(T) \times S_k)$, a (not necessarily split) extension of B by $\mathrm{Out}(T) \times S_k$. We define an action of W on Ω by setting

$$W_\alpha = \{(a, \ldots, a).\pi \mid a \in \mathrm{Aut}(T), \pi \in S_k\}.$$

Thus $W_\alpha \cong \mathrm{Aut}(T) \times S_k$, $B_\alpha \cong T$ and $n = |T|^{k-1}$.

For $1 \leq i \leq k$ let T_i be the subgroup of B consisting of the k-tuples with 1 in all but the i-th component, so that $T_i \cong T$ and $B = T_1 \times \ldots \times T_k$. Put $\mathcal{T} = \{T_1, \ldots, T_k\}$, so that W acts on $\mathcal{T}$. We say that the subgroup X of W is of type III(a) if $B \leq X$ and, letting P be the permutation group $X^{\mathcal{T}}$, one of the following holds:

(i) P is primitive on $\mathcal{T}$,

(ii) $k = 2$ and $P = 1$.

We have $X_\alpha \lesssim \mathrm{Aut}(T) \times P$, and $X \leq B.(\mathrm{Out}(T) \times P)$. Moreover, in case (i) B is the unique minimal normal subgroup of X, and in case (ii) X has two minimal normal subgroups T_1 and T_2, both regular on Ω.

III(b). Product action. Let H be a primitive permutation group on a set Γ of type II or III(a). For $\ell > 1$, let $W = H \wr S_\ell$, and take W to act on $\Omega = \Gamma^\ell$ in its natural product action. Then for $\gamma \in \Gamma$ and $\alpha = (\gamma, \ldots, \gamma) \in \Omega$ we have $W_\alpha = H_\gamma \wr S_\ell$, and $n = |\Gamma|^\ell$. If K is the socle of H then the socle B of W is K^ℓ, and $B_\alpha = (K_\gamma)^\ell \neq 1$.

Now W acts naturally on the ℓ factors in K^ℓ, and we say that the subgroup X of W is of type III(b) if $B \leq X$ and X acts transitively on these ℓ factors.

Finally, one of the following holds.

(i) H is of type II, $K \cong T$, $k = \ell$ and B is the unique minimal normal subgroup of X,

(ii) H is of type III(a), $K \cong T^{k/\ell}$ and X and H both have m minimal normal subgroups, where $m \leq 2$; if $m = 2$ then each of the two minimal normal subgroups of X is regular on Ω.

III(c). Twisted wreath action. Here X is a twisted wreath product $T\mathrm{twr}_\phi P$, defined as follows. Let P be a transitive permutation group on $\{1, \ldots, k\}$ and let Q be the stabilizer P_1. We suppose that there is a homomorphism $\phi : Q \to \mathrm{Aut}(T)$ such that $\mathrm{Im}(\phi)$ contains $\mathrm{Inn}(T)$. Define

$$B = \{f : P \to T \mid f(pq) = f(p)^{\phi(q)} \text{ for all } p \in P,\ q \in Q\}.$$

Then B is a group under pointwise multiplication, and $B \cong T^k$. Let P act on B by $f^p(x) = f(px)$ for p, $x \in P$. We define $X = T\mathrm{twr}_\phi P$ to be the semidirect product of B by P with this action, and define an action of X on Ω by setting $X_\alpha = P$. We then have $n = |T|^k$, and B is the unique minimal normal subgroup of X and acts regularly on Ω.

We say that the group X is of type III(c) if it is primitive on Ω. (Note that the primitivity of X in the above construction depends on some quite complicated conditions on P which we do not investigate here.)

Theorem 2.3.1 (Aschbacher-O'Nan-Scott)**.** *Any finite primitive permutation group is permutation equivalent to one of the types I, II, III(a), III(b), and III(c) described above.*

Chapter 3

On the orders of primitive permutation groups

3.1 Introduction

Bounding the order of a primitive permutation group in terms of its degree was a problem of 19-th century group theory. Apart from some early results of Jordan probably the first successful estimate for the orders of primitive groups not containing the alternating group is due to Bochert [8] (see also [20] or [69]): if G is primitive and $(S_n : G) > 2$, then $(S_n : G) \geq [\frac{1}{2}(n+1)]!$. This bound will prove useful since it is the sharpest available general estimate for very small degrees. But it is far from best possible. Based on Wielandt's method [70] of bounding the orders of Sylow subgroups Praeger and Saxl [57] obtained an exponential estimate, 4^n, where n is the degree of the permutation group. Their proof is quite elaborate. Using entirely different combinatorial arguments, Babai [3] obtained an $e^{4\sqrt{n}\ln^2 n}$ estimate for uniprimitive (primitive but not doubly transitive) groups. For the orders of doubly transitive groups not containing the alternating group, Pyber obtained an $n^{32\log^2 n}$ bound for $n > 400$ in [60] by an elementary argument (using some ideas of [4]). Apart from $O(\log n)$ factors in

the exponents, the former two estimates are asymptotically sharp. To do better, one has to use the Aschbacher-O'Nan-Scott theorem and the classification of finite simple groups. An $n^{c \ln \ln n}$ type bound with "known" exceptions has been found by Cameron [14], while an $n^{9 \log_2 n}$ estimate follows from Liebeck [39]. In this paper we use the classification of finite simple groups to set the sharpest upper bounds possible for the orders of primitive permutation groups via a reasonably short argument. First the following is proved.

Theorem 3.1.1. *Let G be a primitive permutation group of degree n. Then one of the following holds.* 1t11

(i) G is a subgroup of $S_m \wr S_r$ containing $(A_m)^r$, where the action of S_m is on k-element subsets of $\{1, ..., m\}$ and the wreath product has the product action of degree $n = \binom{m}{k}^r$;

(ii) $G = M_{11}$, M_{12}, M_{23} or M_{24} with their 4-transitive action;

(iii) $|G| \leq n \cdot \prod_{i=0}^{[\log_2 n]-1}(n - 2^i) < n^{1+[\log_2 n]}$.

This is a sharp version of the above-mentioned result of Liebeck. The theorem practically states that if G is a primitive group, which is not uniprimitive of case (i), and is not 4-transitive, then the estimate in (iii) holds. The bound in (iii) is best possible. There are infinitely many 3-transitive groups, in particular the affine groups, $AGL(t, 2)$ acting on 2^t points and the symmetric group, S_5 acting on 6 points for which the estimate is exact. In fact, these are the only groups among groups not of case (i) and (ii) for which equality holds. But there is one more infinite sequence of groups displaying the sharpness of the bound. The projective groups, $PSL(t, 2)$ acting on the $t > 2$ dimensional projective space have order $\frac{1}{2} \cdot (n+1) \cdot \prod_{i=0}^{[\log_2 n]-1}(n + 1 - 2^i) < n \cdot \prod_{i=0}^{[\log_2 n]-1}(n - 2^i)$, where $n = 2^t - 1$.

An easy direct consequence is

Corollary 3.1.1. *Let G be a primitive subgroup of S_n.* 1c11

(i) If G is not 3-transitive, then $|G| < n^{\sqrt{n}}$;

(ii) If G does not contain A_n, then $|G| < 50 \cdot n^{\sqrt{n}}$.

This is a sharp version of a result of Cameron [14]. The estimate in (i) is asymptotically sharp for uniprimitive groups of case (i) of Theorem 3.1.1 and is sharp for the automorphism group of the Fano-plane. The estimate in (ii) is sharp for the biggest Mathieu group. Theorem 3.1.1 also leads to a sharp exponential bound.

Corollary 3.1.2. *If G is a primitive subgroup of S_n not containing A_n, then $|G| < 3^n$.* 1c12
Moreover, if $n > 24$, then $|G| < 2^n$.

This improves the Praeger-Saxl [57] theorem. The proof will also display M_{12} as the "largest" primitive group. M_{24} has order greater than 2^{24}, which explains the requirement $n > 24$ in the latter statement. But let us put this in a slightly different form with the use of the prime number theorem.

Corollary 3.1.3. *If G is a primitive subgroup of S_n not containing A_n, then $|G|$ is* 1c13
at most the product of all primes not greater than n, provided that $n > 24$.

Kleidman and Wales published a list of primitive permutation groups of order at least 2^{n-4} in [36]. However their list is rather lengthy, and it is not easy to use. Using our results above we will relax the bound to 2^{n-1} to give a shorter list of "large" primitive groups. These exceptional groups are referred to in [43]. (Note that the Kleidman-Wales list can also be deduced by a similar argument.)

Corollary 3.1.4. *Let G be a primitive permutation group of degree n not containing* 1c14
A_n. If $|G| > 2^{n-1}$, then G has degree at most 24, and is permutation isomorphic to one of the following 24 groups with their natural permutation representation if not indicated otherwise.

(i) $AGL(t,q)$ with $(t,q) = (1,5)$, $(3,2)$, $(2,3)$, $(4,2)$; $A\Gamma L(1,8)$ and $2^4 : A_7$;

(ii) $PSL(t,q)$ with $(t,q) = (2,5)$, $(3,2)$, $(2,7)$, $(2,8)$, $(3,3)$, $(4,2)$; $PGL(t,q)$ with $(t,q) = (2,5)$, $(2,7)$, $(2,9)$; $P\Gamma L(2,8)$ and $P\Gamma L(2,9)$;

(iii) M_i *with* $i = 10, 11, 12, 23, 24$*;*

(iv) S_6 *with its primitive action on* 10 *points, and* M_{11} *with its action on* 12 *point.*

From the above list, using an inductive argument, one can deduce the theorem of Liebeck and Pyber [42] stating that a permutation group of degree n has at most 2^{n-1} conjugacy classes.

Another possible application of the previous result was suggested in [61] by Pyber. Improving restrictions on the composition factors of permutation groups one can bound their order. For example, Dixon [18] proved that a solvable permutation group of degree n has order at most $24^{(n-1)/3}$, and Babai, Cameron, Pálfy [5] showed that a subgroup of S_n that has no composition factors isomorphic to an alternating group of degree greater than $d (d \geq 6)$ has order at most d^{n-1}. Applying the former results Dixon's theorem may be generalized and Babai-Cameron-Pálfy's estimate may be sharpened as follows.

Corollary 3.1.5. *Let* G *be a permutation group of degree* n*, and let* d *be an integer not less than* 4*. If* G *has no composition factors isomorphic to an alternating group of degree greater than* d*, then* $|G| \leq d!^{(n-1)/(d-1)}$*.* 1c15

This bound is best possible. If n is a power of d, then the iterated wreath product of n/d copies of S_d has order precisely $d!^{(n-1)/(d-1)}$. The proof will show that the Mathieu group, M_{12} is again of special importance.

For an application of this corollary see chapter 3 of the book by Lubotzky and Segal [43], and for an alternative approach to dealing with nonabelian alternating composition factors see the paper [34] by Holt and Walton.

3.2 Proof of Theorem 3.1.1.

Before starting the actual proof of the theorem, an easy observation has to be made on the bound in (iii). It is strictly monotone in n, and

$$n^{[\log_2 n]} < n \cdot \prod_{i=0}^{[\log_2 n]-1} (n - 2^i) < n^{1+[\log_2 n]}$$

holds. The former inequality follows from replacing every $(n - 2^i)$ in the product by $\frac{1}{2}n$, while the latter inequality is straightforward.

Theorem 3.1.1 is proved in four steps.

1. It may be assumed that G is almost simple. For if G is affine of prime power degree $n = p^t$ for some prime p, then $|G| \leq |AGL(t,p)| = n \cdot \prod_{i=0}^{[\log_p n]-1}(n - p^i) \leq n \cdot \prod_{i=0}^{[\log_2 n]-1}(n - 2^i)$. Note that the latter inequality holds even when p is replaced by any prime power q, and n is replaced by q^k. This observation is used in the second step of the proof. If G is of diagonal type of degree n ($n \geq 60$), then $|G| < n^{3+\ln\ln n}$ by [14], and the right hand side is smaller than $n^{[\log_2 n]}$. If G is of product type, then it is a subgroup of some primitive permutation group of the form $H \wr S_r$, where $r \geq 2$ and H is primitive of diagonal type or is almost simple acting on a set of size t ($t \geq 5$). In this case the degree of G is $n = t^r$. If H is an alternating group, A_m ($m \geq 5$) acting on k-element subsets of $\{1, ..., m\}$ and $n = \binom{m}{k}^r$, then G is of case (i) of the theorem. If H is a 4-transitive Mathieu group, then it is easily checked that $|G| \leq |H \; wr \; S_r| < n^{[\log_2 n]}$. Otherwise $|G| \leq |H \; wr \; S_r| < (t^{1+[\log_2 t]})^r \cdot r!$ by assumption, and elementary calculations show that the right hand side is less than $n^{[\log_2 n]}$. Finally, if G is nonaffine of twisted product type, then $|G| \leq |H|^r \cdot |S_r| \leq n \cdot \log_{60} n^{\log_{60} n}$ for some nonabelian simple group, H and integer, r ($r \geq 2$), where the degree of G is $n = |H|^r$. The right hand side of the former inequality is considerably smaller than $n^{[\log_2 n]}$ for $n \geq 60^2$.

2. It may be assumed that G has an alternating or a projective nonabelian simple

socle. For if G has unitary socle $U(t,q)$, where $t \geq 3$, q a prime power, and $(t,q) \neq (3,5)$, then G has minimal degree at least q^t by [37], while $|G| \leq |AGL(t,q)|$. If G has symplectic socle $PSp(2m,q)$, where $m \geq 2$ and $q > 2$, then its minimal degree is at least q^{2m-1} by [37], while $|G| \leq |AGL(2m-1,q)|$. If G has orthogonal socle $P\Omega^{\pm\epsilon}(t,q)$, then its minimal degree is at least q^{t-2} by [37], while $|G| \leq |AGL(t-2,q)|$. If $U(3,5) \leq G \leq Aut(U(3,5))$, then G has degree at least 50, while $|G| < n^{[\log_2 n]}$ for $n \geq 50$. If $PSp(2m,2) \leq G \leq Aut(PSp(2m,2))$, then G has minimal degree $2^{m-1}(2^m-1)$ if $m \geq 3$ by [37], else G has socle $A_6 \cong PSL(2,9)$. In the previous case it can be verified, that $|G| \leq 2^{m^2} \cdot \prod_{i=1}^{m}(4^i-1) \leq n \cdot \prod_{i=0}^{[\log_2 n]-1}(n-2^i)$, where $n \geq 2^{m-1}(2^m-1)$. This means that all nonprojective classical almost simple groups satisfy (iii) of the theorem. Finally, let G have socle isomorphic to an exceptional group of Lie-type or to a sporadic simple group. Furthermore, suppose that G is not of type (ii) of the theorem. It will be shown that G is of case (iii). To show this, n can be taken to be the minimal degree of a permutation representation of G. By [39] the order of G is bounded above by n^9. Since we have $n^9 \leq n^{[\log_2 n]} < n \cdot \prod_{i=0}^{[\log_2 n]-1}(n-2^i)$ for $n \geq 512$, it can also be assumed that $n \leq 511$. Now using the list in [19], it is easily checked that G has order at most the relevant bound of (iii) of the theorem.

3. It may be assumed that G is a projective almost simple group. For if G has a nonprojective nonabelian alternating socle, then $A_m \leq G \leq S_m$ for some m ($m \geq 7$). The one-point stabilizer of G in its primitive action on the set $\{1,...,n\}$ is primitive, imprimitive, or intransitive as a subgroup of S_m. If it is intransitive, then G is of type (i) of the theorem. If it is primitive, then $|G| \leq n^4 \leq n^{[\log_2 n]}$ if $n \geq 16$, by Bochert's lemma, else $n = 15$ and $G \cong A_7$. Easy calculation shows that this latter group is again of case (iii) of the theorem, since $|G| < 15^3$. Finally, suppose that the point stabilizer of G is imprimitive as a subgroup of S_m. Then there exist integers a and b both at least 2, such that $m = a \cdot b$ and $n = m!/(b!^a \cdot a!)$. Thus one can assume, that $m \geq 8$. The following lemma shows that these groups also have order at most the bound in

(iii).

Lemma 3.2.1. *For integers a, b and m such that $m \geq 8$; $a, b \geq 2$ and $m = a \cdot b$, the inequality $m! \leq (m!/(b!^a \cdot a!))^{[\log_2(m!/(b!^a \cdot a!))]}$ holds.*

Proof. Since $m! \leq 2^{[(m+1)/2]^2}$ holds for all m of the statement of the lemma, it is sufficient to see $m!/(b!^a \cdot a!) \geq 2^{[(m+1)/2]}$. This inequality is proved below. Three assumptions, A, B and C are made on the product decomposition of m. Through steps A and B we show that it is enough to consider the case when a is the smallest prime factor of m. Then in step C it is proved that only cases $a = 1, 3$ and 5 have to be dealt with.

A. Suppose that $b \geq a$. For if $a > b$, then $m!/(a!^b \cdot b!) < m!/(b!^a \cdot a!)$, since $a!^{b-1} > b!^{a-1}$, which means that the right hand side of the inequality in question can be decreased by interchanging a and b.

B. Suppose that a is the smallest prime divisor of m. This restriction can also be drawn. For let $m = a_1 b_1 = a_2 b_2$ with a_1, b_1, a_2, $b_2 \geq 2$ be two decompositions of m satisfying the previous assumption. If $a_1 \leq a_2$ and $b_1 \geq b_2$, then

$$\frac{m!}{{b_1!}^{a_1} \cdot a_1!} \leq \frac{m!}{{b_2!}^{a_1} \cdot (b_2+1)^{a_1} \ldots {b_1}^{a_1} \cdot a_1!} \leq \frac{m!}{{b_2!}^{a_1} \cdot a_1! \cdot {b_2}^{a_1(b_1-b_2)}} \leq$$

$$\leq \frac{m!}{{b_2!}^{a_1} \cdot a_1! \cdot (b_2! \cdot a_2)^{\frac{a_1}{b_2} \cdot (b_1-b_2)}} \leq \frac{m!}{{b_2!}^{a_1} \cdot a_1! \cdot (b_2! \cdot a_2)^{(a_2-a_1)}} \leq$$

$$\leq \frac{m!}{{b_2!}^{a_1} \cdot a_1! \cdot {b_2!}^{(a_2-a_1)} \cdot (a_1+1) \ldots a_2} \leq \frac{m!}{{b_2!}^{a_2} \cdot a_2!}$$

follows. This means that a can be taken to be smallest possible. So a is indeed the smallest prime divisor of m. (Assumption A is used in establishing the third inequality of the derivation.)

Before making the third assumption, it is straightforward to see that $m!/(b!^a \cdot a!) \geq p^{\pi(m)-\pi(b)}$ holds, where $\pi(x)$ denotes the number of primes not greater than x, and p is

the smallest prime greater than b. The estimate $0.92 < \pi(x) \cdot \ln x/x < 1.11$ found in [17] is also needed.

C. Suppose that $a = 2, 3$ or 5. For if $a \geq 7$, then $m = 49, 77$ or $m \geq 91$. If $m = 49$, then $m!/(b!^a \cdot a!) = 49!/(7!^7 \cdot 7!) > 11^{\pi(49)-\pi(7)} > 11^{11} > 2^{[(m+1)/2]}$. If $m = 77$, then $m!/(b!^a \cdot a!) = 77!/(11!^7 \cdot 7!) > 13^{\pi(77)-\pi(11)} > 13^{16} > 2^{[(m+1)/2]}$. Finally, if $m \geq 91$, then

$$\frac{m!}{(b!^a \cdot a!)} \geq (m/7)^{\pi(m)-\pi(m/7)} >$$

$$> (m/7)^{(0.92 \cdot m/\ln m)-(1.11 \cdot (m/7)/\ln (m/7))} > 2^{(m+1)/2} = 2^{[(m+1)/2]}$$

follows from the above-mentioned estimate of [17].

If $a = 2$, then we have $m!/(b!^a \cdot a!) = \frac{1}{2} \cdot \binom{m}{m/2} \geq \frac{((m/2)+1)^{m/2}}{(m/2)!} \geq$
$\geq \frac{((m/2)+1)^{m/2}}{(((m/2)+1)/2)^{m/2}} = 2^{[(m+1)/2]}$.

If $a = 3$, then $m!/(b!^a \cdot a!) = m!/((m/3)!^3 \cdot 3!) \geq \frac{1}{2} \cdot \binom{m+1}{(m+1)/2} \geq 2^{[(m+1)/2]}$.

Finally, if $a = 5$, then $m!/(b!^a \cdot a!) = m!/((m/5)!^5 \cdot 5!) \geq \frac{1}{2} \cdot \binom{m+1}{(m+1)/2} \geq 2^{[(m+1)/2]}$ follows. The lemma is now proved.

4. If G has socle isomorphic to a projective group, then it is of case (iii) of Theorem 3.1.1 or it is of type (i) with $r = k = 1$. This is proved below.

Lemma 3.2.2. *Let G be an almost simple primitive subgroup of S_n not containing A_n. If G has a projective socle, then $|G| \leq n \cdot \prod_{i=0}^{[\log_2 n]-1}(n - 2^i)$.*

Proof. Let G have socle isomorphic to $PSL(t, q)$. The proof consists of three steps.

A. It may be assumed that G is acting on a set of size at least $(q^t - 1)/(q - 1)$. For if $(t, q) \neq (2, 5); (2, 7); (2, 9);\ (2, 11); (4, 2)$, then $PSL(t, q)$ has minimal degree $(q^t - 1)/(q - 1)$; else easy calculations show that G contains A_n, or it is of case (iii) of Theorem 3.1.1.

B. It may be assumed that both t and q are greater than 2. For if $q = 2$, then G is permutation equivalent to $PSL(t, 2)$ acting on $n = 2^t - 1$ points, or it has degree $n \geq 2^t$.

In the previous case $|PSL(t,2)| \leq \frac{1}{2}\cdot(n+1)\cdot\prod_{i=0}^{[\log_2 n]-1}(n+1-2^i) < n\cdot\prod_{i=0}^{[\log_2 n]-1}(n-2^i)$ follows, while in the latter one we have $|P\Gamma L(t,2)| \leq n^{[\log_2 n]}$. Now suppose that $t=2$ and $q>2$. n can be taken to be $q+1$. If q is a prime we may suppose that $q \geq 11$, and so $|G| \leq q(q^2-1) \leq (q+1)q(q-1) = n(n-1)(n-2) \leq n^{[\log_2 n]}$ follows. If $q=4$, then G has socle isomorphic to $PSL(2,5)$. This case was already treated in step A. If $q \geq 16$ and it is not a prime, we have $|G| < \frac{q}{2}q(q^2-1) \leq (q+1)q(q-1)(q-3) \leq n^{[\log_2 n]}$. Finally if $q=8$ or 9 we have $|G| \leq n\cdot\prod_{i=0}^{[\log_2 n]-1}(n-2^i)$.

C. Let $t>2$ and $q>2$. Suppose that $n=(q^t-1)/(q-1) > q^{t-1}$. Then it is straightforward to see that $|G| < q^{t^2}$. We also have $n^{[\log_2 n]} > q^{(t-1)^2\log_2 q-(t-1)}$. Now consider the $q^{t^2} < q^{(t-1)^2\log_2 q-(t-1)}$ inequality. This is equivalent to $(t^2+t-1)/(t-1)^2 < \log_2 q$. If $q \geq 7$, then the former inequality is always true. If $q=5$, then it is true only if $t \geq 4$. If $q=4$, then it only holds if $t \geq 5$, and if $q=3$, then it is only true if $t \geq 7$. It is checked that if $(t,q) = (3,4);(4,4);(4,3);(5,3);(6,3);(3,5)$, then $|G| < n^{[\log_2 n]}$. Finally, if $(t,q)=(3,3)$, then $|G| < n\cdot\prod_{i=0}^{[\log_2 n]-1}(n-2^i)$ follows. □

□

3.3 Corollaries

Corollaries 3.1.1-3.1.4 are proved almost simultaneously in this section. First of all, it is necessary to give an upper estimate for the orders of primitive groups of case (i) of Theorem 3.1.1.

Lemma 3.3.1. *Let G be a primitive group of degree n not of case (iii) of Theorem 3.1.1. If G is not 3-transitive, then $|G| < n^{\sqrt{n}}$.*

Proof. It may be assumed that G is of type (i) of Theorem 3.1.1 with $m \geq 7$. If $r=1$, then $k \geq 2$, and so $|G| \leq m! \leq \binom{m}{2}^{\sqrt{\binom{m}{2}}} \leq \binom{m}{k}^{\sqrt{\binom{m}{k}}} = n^{\sqrt{n}}$ follows; else $r \geq 2$, and we have $|G| \leq m!^r \cdot r! < m^{r\sqrt{m^r}} \leq \binom{m}{k}^{r\sqrt{\binom{m}{k}^r}} = n^{\sqrt{n}}$. □

The 5-transitive Mathieu group, M_{12} is the largest primitive group in the following sense.

Lemma 3.3.2. *If G is a primitive subgroup of S_n not containing A_n, then $|G| \leq |M_{12}|^{\frac{n}{12}} < 3^n$.* 1l32

Proof. Let c be the constant $|M_{12}|^{\frac{1}{12}} = 95040^{\frac{1}{12}} \approx 2.59911....$ The $|G| \leq c^n$ estimate has to be proved. If $n \leq 9$, then Bochert's bound, while if $n \geq 10$, then both $n^{\sqrt{n}}$ and $n^{1+[\log_2 n]}$ are smaller than c^n. The 4-transitive Mathieu groups are easily checked to have order at most c^n. □

The classification of exponentially large primitive groups is essential in order to complete the proofs of Corollaries 3.1.1 and 3.1.2. The proof of Corollary 3.1.4 is what follows.

Proof. Let G be a primitive permutation group of degree n not containing A_n. If $|G| > 2^{n-1}$, then G is a 4-transitive Mathieu group or n is at most 22. For if $n \geq 23$, then $n^{\sqrt{n}}$ and $n \cdot \prod_{i=0}^{[\log_2 n]-1}(n - 2^i)$ are smaller than 2^{n-1}. From [19] it follows that a primitive permutation group of degree at most 22 is affine, Mathieu or almost simple with alternating or projective socle. It is checked that if such a group has order greater than 2^{n-1}, then it is permutation equivalent to one of the groups in the list. It is also checked that all permutation groups in the list have order greater than 2^{n-1}. □

The next lemma finishes the proof of Corollaries 3.1.2 and 3.1.1 part (i).

Lemma 3.3.3. *Let G be primitive of degree n not containing A_n.* 1l33

(i) If $|G| > 2^n$, then G is a 2-transitive group of degree at most 24;

(ii) If $|G| \geq n^{\sqrt{n}}$, then G is 3-transitive of degree at most 24.

Proof.

(i) If $|G| > 2^n$, then G is permutation equivalent to one of the groups in the list of Corollary 3.1.4. It is checked that only 2-transitive groups in the list have order at least 2^n. Moreover, $|M_{24}| > 2^{24}$.

(ii) If $|G| \geq n^{\sqrt{n}}$, then G is permutation equivalent to one of the groups in the list of Corollary 3.1.4. For if $n \leq 21$, then $2^{n-1} < n^{\sqrt{n}}$; else $n = 22$ and G has socle isomorphic to M_{22}, so it does have order less than $n^{\sqrt{n}}$. It is checked that only 3-transitive groups in the list have order at least $n^{\sqrt{n}}$. Moreover, $|M_{24}| > n^{\sqrt{n}}$. □

Corollary 3.1.1 part (ii) follows from Lemma 3.3.3 part (ii).

For the proof of Corollary 3.1.3 notice that the product of all primes not greater than n, is at least $n^{0.5\cdot(\pi(n)-\pi(\sqrt{n}))} > n^{(0.46\cdot n - 1.11\cdot\sqrt{n})/\ln n}$ by [17]. This is greater than $n^{\sqrt{n}}$ for $n \geq 200$. For cases $24 < n < 200$ it is checked by computer that $\prod_{p<n} p > 2^{n-1}$ holds.

3.4 An application

Corollary 3.1.5 is proved now. We proceed by induction on n. If $n \leq d$ then the estimate is straightforward. Let $n > d$. If G is primitive then $|G| \leq |M_{12}|^{(n-1)/11} < d!^{(n-1)/(d-1)}$. (The former inequality follows from Lemma 3.3.2 for $n \geq 12$, and holds also for $4 < n < 12$ by inspection.) If G is transitive with k-element blocks of imprimitivity then

$$|G| \leq \left(d!^{(k-1)/(d-1)}\right)^{n/k} \cdot d!^{(n/k-1)/(d-1)} = d!^{(n-1)/(d-1)}$$

follows by induction. Finally, if G is intransitive with an orbit of length k, then

$$|G| \leq d!^{(k-1)/(d-1)} \cdot d!^{(n-k-1)/(d-1)} < d!^{(n-1)/(d-1)}.$$

Chapter 4

On the number of conjugacy classes of a permutation group

4.1 Introduction

We have talked about why it is more natural to count complex irreducible characters than conjugacy classes for a finite group. However, sometimes it is indeed more natural to work with conjugacy classes. Here is an example.

Nagao [53] proved that if G is a finite group and N is a normal subgroup, then the number of irreducible characters of G is at most the number of irreducible characters of N multiplied by the number of irreducible characters of the factor group, G/N. Later, Gallagher [24] proved this fact using conjugacy classes. We believe that this proof is more natural. If we denote the number of conjugacy classes of a finite group G by $k(G)$, then Nagao's result translates to

Lemma 4.1.1 (Nagao, [53]). *If G is a finite group and N a normal subgroup in G, then $k(G) \leq k(N) \cdot k(G/N)$.*

This lemma is very important. It was first used in proving that for p-solvable groups, Brauer's $k(B)$-problem is equivalent to the $k(GV)$-problem, and most recently

it was used many times in proving the $k(GV)$-problem itself.

Here, we give another application of Lemma 4.1.1 of a (seemingly) different flavor.

Theorem 4.1.1 (Kovács, Robinson, [38]). *If G is a permutation group of degree n, then $k(G) \leq 5^{n-1}$.* t2

The proof is inductive. First we prove the claim for primitive, then for imprimitive and finally for intransitive groups. The induction starts by giving a universial upper bound for the numbers of conjugacy classes for primitive groups, after which we apply Lemma 4.1.1 in each step of the induction. The initial case is the most difficult one. In the Kovács-Robinson proof the Praeger-Saxl [57] bound on the orders of primitive permutation groups was used. This makes Theorem 4.1.1 independent of the Classification Theorem of Finite Simple Groups (CTFSG).

However, if one wants to improve on the bound in Theorem 4.1.1, then CTFSG is necessary. By a result of the previous chapter on the orders of primitive groups, one can give a short proof for

Theorem 4.1.2 (Liebeck, Pyber, [42]). *If G is a permutation group of degree n, then $k(G) \leq 2^{n-1}$.* t3

Originally, Theorem 4.1.2 was proved by estimating the numbers of conjugacy classes of simple groups via existing recurrence relations for these numbers. (Indeed, Kovács and Robinson had verified a relevant reduction to almost simple groups.) Recently, the Liebeck-Pyber bound for simple groups (of Lie-type) was (and is being) improved by Fulman and Guralnick in [23] and in a paper in preparation. In this thesis we make no use of these improvements in proving

Theorem 4.1.3. *Any permutation group of degree $n > 2$ has at most $3^{(n-1)/2}$ conjugacy classes.* t3.5

4.2 Linear groups

In this section we give upper bounds for the number of conjugacy classes of a linear group. The first of these is crucial for us in dealing with primitive permutation groups.

A subgroup of the general linear group, $GL(n, q)$ is called completely reducible if it acts completely reducibly on the natural n-dimensional module over the field $GF(q)$.

Our first result is the following.

Theorem 4.2.1. *If G is a completely reducible subgroup of $GL(n, q)$, then $k(G) \leq q^{5n}$.* t5

Proof. Let G be a completely reducible subgroup of $GL(n, q)$ acting on V, an n-dimensional vector space over $GF(q)$ where q is a fixed prime power. We show $k(G) \leq q^{5n}$ by induction on n.

This is true for $n = 1$ since G is then cyclic of order at most $q - 1$.

Suppose now that $n > 1$, and that the claim holds for all integers less than n.

First of all, we may assume that G is irreducible. For if G is not, then the $GF(q)G$-module V is a direct sum of two non-trivial submodules, say V_1 and V_2, of dimensions $1 \leq m < n$ and $n - m$, respectively. Let the kernel of the action of G on the vector space V_1 be B. Since $B \triangleleft G$, by Clifford's theorem, we see that B is completely reducible on V and also on V_2. By induction, we have $k(G/B) \leq q^{5n}$ and $k(B) \leq q^{5\cdot(n-m)}$, hence we get

$$k(G) \leq k(B) \cdot k(G/B) \leq q^{5n}$$

by Lemma 4.1.1.

The vector space V admits an m-space decomposition $V = V_1 \oplus \ldots \oplus V_t$ for some $1 \leq m \leq n$ and $t \geq 1$ with respect to the irreducible group G. (Each vector space, V_i (for $1 \leq i \leq t$) has dimension m, and V is an imprimitive irreducible G-module if $t > 1$.) Choose t to be as large as possible. If $t = n$ and $m = 1$, then we have

$$k(G) \leq k(B) \cdot k(G/B) \leq q^n \cdot 2^{n-1} \leq q^{5n}$$

by Lemma 4.1.1 and by Theorem 4.1.2 where B denotes the kernel of the action of G on the set of subspaces $\{V_1, \ldots, V_t\}$.

Let $t < n$ and $m \geq 2$. For each $1 \leq i \leq t$, the set stabilizer, G_i of the vector space $\{0\} \oplus \ldots \oplus V_i \oplus \ldots \oplus \{0\}$ in G may be considered as a group acting irreducibly on the vector space V_i. (Note that the G_i's are conjugate subgroups in G each of index t.) By the maximality of t, the V_i's do not admit non-trivial direct sum decompositions (that is, decompositions with at least two summands) with respect to the G_i's. However, they could admit tensor product decompositions. For each $1 \leq i \leq t$, let $V_i \cong W_{i1} \otimes \ldots \otimes W_{ir}$ be a tensor product decomposition with respect to G_i so that $r \geq 1$ is as large as possible and that $dim(W_{ij}) = n_0 > 1$ for all $1 \leq j \leq r$. (Note that the W_{ij}'s are not subspaces of V nor of any of the V_i's.)

From now on, B denotes the maximal normal subgroup of G which preserves each vector space W_{ij} of the decomposition

$$V = (W_{i1} \otimes \ldots \otimes W_{1r}) \oplus \ldots \oplus (W_{t1} \otimes \ldots \otimes W_{tr}).$$

Notice that G/B may be viewed as a permutation group of degree tr, and that B is considered to be a subgroup of

$$H = (H_{11} \circ \ldots \circ H_{1r}) \times \ldots \times (H_{t1} \circ \ldots \circ H_{tr})$$

where the H_{ij}'s are isomorphic groups with irreducible representations on the W_{ij}'s. Moreover, for each projection π_{ij} of H to the component H_{ij}, we have $\pi_{ij}(B) = H_{ij}$. Also, notice that by our construction (by the maximality of t and r), the W_{ij}'s do not admit non-trivial direct sum nor non-trivial tensor product decompositions (that is, decompositions with at least two factors) with respect to the H_{ij}'s.

We now need a theorem of Liebeck.

Theorem 4.2.2 (Liebeck, [40]). *Let G_0 be a simple classical group with natural* t4

projective module V of dimension n over $GF(q)$, and let G be a group such that $G_0 \lhd G \leq Aut(G_0)$. If H is any maximal subgroup of G, then one of the following holds:

(i) H is a known group (and $H \cap G_0$ has well-described (projective) action on V);

(ii) $|H| < q^{3n}$.

The known groups in (i) are groups of the following general types: stabilizers of subspaces, or of sets of subspaces of V; stabilizers of decompositions $V = V_1 \otimes \ldots \otimes V_r$; normalizers of classical groups over subfields or extension fields of $GF(q)$; or A_c or S_c in a representation of smallest degree over $GF(q)$ ($n \in \{c-1, c-2\}$). These subgroups are described in more detail in paragraphs 3 and 4 of [40], or in the book [37].

Let $F(B)$ be the Fitting subgroup of B. Notice that $B/F(B)$ can be considered as a factor group of a subgroup of $PGL(n, q)$. Hence we can use Theorem 4.2.2 repeatedly to describe the group $B/F(B)$. We see that there are four possibilities for $B/F(B)$. These are the following.

- $B/F(B)$ is solvable;
- $B/F(B)$ has a minimal normal subgroup, $M/F(B)$ isomorphic to a direct product of $1 \leq \ell \leq tr$ copies of a non-abelian finite simple classical group, T of dimension x over the field of y elements so that $|B/M| \leq |Out(T)|^{\ell}$;
- $B/F(B)$ is a factor group of a permutation group of degree at most $(n_0 + 2)rt \leq n + 2rt \leq 2n$;
- $|B/F(B)| \leq q^{3n}$.

(Note that if K is a subgroup of T^{tr} where T is as above, so that K projects naturally onto each direct factor of T^{tr}, then $K = T^{\ell}$ for some $1 \leq \ell \leq tr$. This explains the structure of the groups $M/F(B)$ and hence of the groups $B/F(B)$ of the second type above.)

Next we state two rather crude bounds for $|\mathrm{Out}(T)|$ where T is a finite simple classical group.

Lemma 4.2.1. *Let T be a finite simple classical group as above. If $T \neq PSL(x,y)$,* yx1
then we have

$$|Out(T)| \leq \frac{y^{2.5x}}{6^{x/2}}.$$

If $T = PSL(x,y)$, then

$$|Out(T)| \leq \frac{y^{2x}}{(y-1)}.$$

Proof. The exact values for $|\mathrm{Out}(T)|$ are found on page 170 of [37]. We use those. If $T = PSL(x,y)$, then we have

$$|\mathrm{Out}(T)| \leq 2 \cdot y^2 \leq y^{2x-1} < \frac{y^{2x}}{(y-1)}.$$

So from now on, suppose that $T \neq PSL(x,y)$.

If $y = 2$, then

$$|\mathrm{Out}(T)| \leq 6 < \frac{2^{2.5x}}{6^{x/2}}$$

unless $x = 2$ in which case T is not simple.

Let $y = 3$. In this case we have

$$|\mathrm{Out}(T)| \leq 24 < \frac{3^{2.5x}}{6^{x/2}}$$

for all $x \geq 2$.

Finally, if $y \geq 4$, then we see that

$$|\mathrm{Out}(T)| \leq 6 \cdot (y+1) \cdot (y-1) < 6 \cdot y^2 < \frac{y^{2.5x}}{6^{x/2}}$$

for all $x \geq 2$. □

At this point and once in a later section we need an elementary result from [24] and a theorem from [42].

Lemma 4.2.2 (Gallagher, [24]). *If G is a finite group and H is a subgroup of G, then* yx2

$$k(H)/(G:H) \leq k(G) \leq (G:H) \cdot k(H),$$

where $(G:H)$ denotes the index of H in G.

Theorem 4.2.3 (Liebeck, Pyber, [42]). *Let G be a finite simple group of Lie type* yx3 *over $GF(q)$. If $\ell = rk(G)$, then*

$$k(G) \leq (6q)^{\ell}.$$

We are now in the position to prove the following.

Lemma 4.2.3. *If $B/F(B)$ is a group of any of the four types above, then we have* yx4 *$k(B/F(B)) \leq q^{3n}$.*

Proof. This is trivial in the fourth case. Also, if $B/F(B)$ is solvable, then so is B. Since B is a normal subgroup in G, it is completely reducible, hence we have $|B| \leq q^{3n}$ by the Pálfy-Wolf theorem [59], [71]. This proves the lemma in the first case. By Theorem 4.1.2, the number of conjugacy classes and so the number of complex irreducible characters of a finite permutation group, K of degree at most $2n$ is at most $2^{2n} < q^{3n}$, hence any factor group of K has at most q^{3n} conjugacy classes. This gives the result in the third case.

Suppose that $B/F(B)$ and T are of the second type above. By Lemma 4.1.1, we have

$$k(B/F(B)) \leq k(M/F(B)) \cdot k(B/M) \leq k(T)^{tr} \cdot |\mathrm{Out}(T)|^{tr}.$$

If $T \neq PSL(x,y)$, then by Theorem 4.2.3 and by Lemma 4.2.1, we have

$$k(B/F(B)) \leq y^{3xtr} \leq q^{3n_0 tr} \leq q^{3n}.$$

Let $T = PSL(x, y)$. In this case we may apply Lemma 4.2.2 to the estimate $k(GL(x, y)) < y^x$ of Lemma 5.9 (ii) of [46] to conclude that $k(T) < y^x \cdot (y - 1)$. Hence by Lemma 4.2.1, we again get that

$$k(B/F(B)) \leq q^{3n}.$$

This completes the proof of the lemma. □

Now $F(B)$ is a nilpotent characteristic subgroup of B, hence it is normal in G. Since G is irreducible, $F(B)$ is a completely reducible nilpotent group by Clifford's theorem. By Theorem 1.6 (a) of [71], we conclude that $k(F(B)) \leq |F(B)| \leq q^{1.6n}$.

From this and by Lemma 4.2.3 we have that

$$k(B) \leq k(B/F(B)) \cdot k(F(B)) \leq q^{4.6n}.$$

If $1 < n_0 \leq 4$, then $|B| \leq q^{4n}$, and hence by Theorem 4.1.2, we have

$$k(G) \leq k(B) \cdot k(G/B) \leq q^{4n} \cdot 2^{tr} \leq q^{4.5n} < q^{5n}.$$

Otherwise, if $n_0 \geq 5$, then again by Theorem 4.1.2, we get

$$k(G) \leq k(B) \cdot k(G/B) \leq q^{4.6n} \cdot 2^{tr} \leq q^{4.8n} < q^{5n}.$$

This completes the proof of Theorem 4.2.1. □

This sharpens Corollary 5 of [42] which was used (see [42]) to extend a result of Arregi and Vera-Lopez [2]. By Theorem 4.2.1 we may sharpen a little on Corollary 6 of [42] as follows.

Theorem 4.2.4. *Any subgroup of $GL(n, q)$ has at most $q^{(2n^2+31n)/6}(n-1)! \cdot 2^{n-1}$ conjugacy classes.*

Proof. (Liebeck, Pyber, [42]) If G is any subgroup of $GL(n,q)$ ($q = p^f$), then $G/O_p(G)$ may be viewed as a completely reducible linear group acting on the direct sum of the composition factors of the natural module for G. By Theorem 4.2.1, $k(G/O_p(G)) \leq q^{5n}$ holds. By a result of Arregi and Vera-Lopez [2], any p-subgroup of $GL(n,q)$ has at most $q^{(2n^2+n)/6}(n-1)! \cdot 2^{n-1}$ conjugacy classes. Hence, by Lemma 4.1.1, we get

$$k(G) \leq k(O_p(G)) \cdot k(G/O_p(G)) \leq q^{(2n^2+31n)/6}(n-1)! \cdot 2^{n-1}$$

as required. □

4.3 Primitive permutation groups

In this section we prove some upper bounds for the number of conjugacy classes of a normal subgroup of a primitive permutation group. Our main result is Theorem 4.3.3. This result is necessary to deduce our general $k(G) \leq 3^{(n-1)/2}$ bound for arbitrary permutation groups G of degree $n > 2$.

We note here that this section is not entirely self-contained. The actual lower bound we use for the partition function, $p(n)$ is deduced only in Chapter 3. However, this should not cause much inconvenience for the reader, since we provide some supporting evidence and explanation at that point.

Let us start by reminding the reader what a primitive permutation group is. There are two equivalent definitions both of which we make use of. Usually, we think of a primitive permutation group as a transitive group having no non-trivial block of imprimitivity. This is equivalent to saying that any one-point stabilizer of the transitive group is maximal. For example, a 2-transitive group is always primitive.

As for 2-transitive groups, the structure of primitive permutation groups is described via their minimal normal subgroups. The ultimate structure theorem is the so-called O'Nan-Scott-Aschbacher theorem. It is complicated to state and we do not

need it in its full glory.

The group, S generated by all minimal normal subgroups of the primitive group, G is called the socle of G. This is a characteristic subgroup of G isomorphic to a direct power of, say r copies of a simple group, L. Since each nontrivial normal subgroup of a primitive group is transitive, S is also transitive.

If L is abelian, then S is an (elementary) abelian group and is the unique minimal normal subgroup of G. In fact, S acts regularly on the underlying set. It is not hard to see that in this case G/S (or a one-point stabilizer of G) may be viewed as an irreducible subgroup of $GL(r,p)$ where $|L| = p$. Hence, for all nontrivial normal subgroups, N of G, the factor group N/S can be viewed as a completely reducible subgroup of $GL(r,p)$. (This is why we needed to deal with completely reducible groups in the previous section.) Primitive permutation groups with an (elementary) abelian regular socle are called affine.

If L is not abelian, then the situation is much more complicated. The group, G can be almost simple if $r = 1$, or it can be of simple diagonal type, of product type or of twisted wreath type if $r > 1$ holds. By an almost simple primitive group, G with socle, L we mean a primitive permutation group containing L and contained in $Aut(L)$. We need not explain what the other types of primitive permutation groups are.

On the bottom of page 553 of [42] it is noted that whenever L is a non-alternating, non-abelian finite simple group, then the number of conjugacy classes, $k(L)$ of L satisfies $k(L) \leq P(L)^4$ where $P(L)$ denotes the minimal degree of a faithful permutation representation for L. Using Theorem 1 of [42] and the bounds for the minimal degrees $P(L)$ listed in the proof of Proposition 1.9 of [42] and in [16], it is easy to improve on this estimate.

Lemma 4.3.1. *If L is a non-alternating, non-abelian finite simple group, then we have $k(L) \leq P(L)^{3.6}$ where $P(L)$ denotes the minimal degree of a faithful permutation representation for L.*

To obtain information on the number of conjugacy classes of an almost simple group, we need another technical lemma, this time on the orders of the outer automorphism groups of simple groups. A weak version of Lemma 8.6 of [29] is the following.

Lemma 4.3.2 (Guralnick, Pyber, [29]). *If L is a non-abelian finite simple group, then $|Out(L)| \leq P(L)^{0.82}$ where $P(L)$ denotes the minimal degree of a faithful permutation representation for L.* 13

We also need Lemma 2.13 from [42]. For a group G we denote the smallest degree of a faithful transitive permutation representation of G by $P^t(G)$.

Lemma 4.3.3 (Liebeck, Pyber, [42]). *If $S_1, \ldots, S_r$ are non-abelian simple groups, then* 14

$$P^t(S_1 \times \ldots \times S_r) \geq \prod_{i=1}^{r} P^t(S_i).$$

The following is a strong version of Lemma 2.14 of [42].

Lemma 4.3.4. *Let $N \neq \{1\}$ be a normal subgroup of a primitive permutation group G of degree n. Suppose that G has a non-abelian socle. Then there exists a minimal normal subgroup M of G contained in N and a normal subgroup K of N containing M, so that $|K/M| \leq n^{0.82}$ and that N/K has an embedding into S_r with $r \leq log_5 n$.* 15

Proof. Let M be a minimal normal subgroup of G contained in N. By the Aschbacher-O'Nan-Scott theorem, we know that M is a direct power of a non-abelian simple group, say $M = L^r$. We also know that M is transitive. By Lemma 4.3.3, we have $P^t(L)^r \leq n$. It follows that $r \leq log_5 n$. Now N acts on the direct factors of M by conjugation. The kernel K of this action has an embedding into $\mathrm{Aut}(L)^r$, and $N/K \leq S_r$. Finally, by Lemma 4.3.2, we have $|\mathrm{Out}(L)| \leq (P^t(L))^{0.82}$. This gives us

$$|K/M| \leq |\mathrm{Out}(L)|^r \leq (P^t(L))^{0.82r} \leq n^{0.82}.$$

□

Now we are in the position to give a polynomial bound for the number of conjugacy classes of a certain primitive permutation group.

Theorem 4.3.1. *Let G be a primitive subgroup of S_n, and let N be a normal subgroup of G. If the socle of G is isomorphic to a direct power of A_6, or is not a direct product of non-abelian alternating groups, then $k(N) \leq n^6$.* t6

Proof. Let G be a primitive permutation group of degree n with socle isomorphic to a direct power of L where L is a simple group. Let N be a normal subgroup of G different from $\{1\}$. Suppose that L is isomorphic to A_6, or is non-abelian and non-alternating. By Lemma 4.3.4, we know that there exists a minimal normal subgroup $M \cong L^r$ of G contained in N and a normal subgroup K of N containing M, so that $|K/M| \leq n^{0.82}$ and that N/K has an embedding into S_r with $r \leq log_5 n$. By Lemma 4.1.1, Lemma 4.3.4 and Theorem 4.1.2, we have $k(N/M) \leq k(K/M) \cdot k(N/K) \leq n^{0.82} \cdot 2^{r-1} \leq n^{1.32}$. By Lemma 4.3.1 and by inspection for the case $L = A_6$, it follows that if L is isomorphic to A_6, or is non-abelian and non-alternating, then by Lemma 4.1.1 and by Lemma 4.3.3 we have $k(N) \leq k(N/M) \cdot k(M) \leq n^{1.32} \cdot n^{3.6} < n^5$. Hence we reduced the proof of the theorem to the case where the primitive permutation group G is of affine type, that is, if it has an abelian socle S. In this case N contains S, and N/S may be considered as a completely reducible subgroup of $GL(m, p)$ where p is a prime and $p^m = n$. By Lemma 4.1.1 and Theorem 4.2.1 we get $k(N) \leq k(N/S) \cdot k(S) \leq p^{5m} \cdot n = n^6$, which completes the proof of the theorem. □

This sharpens part (ii) of Corollary 2.15 of [42].

But what happens if the socle of a primitive group is a direct product of isomorphic copies of a non-abelian alternating group of degree different from 6? Well, the number of conjugacy classes of the symmetric group S_n is equal to the number of partitions, $p(n)$ of the integer n. Let us try to think along this line.

First we prove a lemma.

Lemma 4.3.5. *For any integers $r \geq 2$ and $m \geq 5$, we have* yx5

$$p(m)^r \cdot 2^{r-1} < p(m^r).$$

Proof. Let $r = 2$. By [26], we may and do suppose that $m \geq 13$. To prove the inequality for $r = 2$, it is sufficient to give

$$p(m) \cdot p(m+6) + p(m) \cdot p(m+2) > 2 \cdot p(m)^2$$

number of different partitions of m^2.

Let Π_1 be the set of all partitions of m^2 of the following form. Take any partition, π_1 of m and multiply each part by $m-3$. Then combine this new partition with an arbitrary partition, π_1' of $m+6$ together with two parts of lengths $m-3$ each. There are $p(m)$ choices for π_1 and $p(m+6)$ choices for π_1'. Hence $|\Pi_1| \leq p(m) \cdot p(m+6)$. We claim that $|\Pi_1| \geq p(m) \cdot p(m+6)$. Suppose that $\pi \in \Pi_1$. We must show that there is a unique partition, π_1 of m and a unique partition, π_1' of $m+6$ so that π is obtained by the above construction from π_1 and π_1'. Since $m \geq 13$, any partition of $m-6$ can contain at most one part of length divisible by $m-3$, possibly a part equal to $m-3$. Hence π_1' is uniquely defined; it consists of all parts of π not divisible by $m-3$ possibly together with a part of length $m-3$. The partition, π_1 is uniquely defined as well. It consists of all parts of π divisible by $m-3$ except two or possibly three parts of lengths $m-3$ each. This completes the proof of our claim. We get $|\Pi_1| = p(m) \cdot p(m+6)$.

Now let Π_2 be the set of all partitions of m^2 of the following form. Take any partition, π_2 of m and multiply each part by $m-2$. Then combine this new partition with an arbitrary partition, π_2' of $m+2$ together with a part of length $m-2$. There are $p(m)$ choices for π_2 and $p(m+2)$ choices for π_2'. Hence $|\Pi_2| \leq p(m) \cdot p(m+2)$. We claim that $|\Pi_2| \geq p(m) \cdot p(m+2)$. Suppose that $\pi \in \Pi_2$. We must show that there is a unique partition, π_2 of m and a unique partition, π_2' of $m+2$ so that π is obtained

by the above construction from π_2 and π_2'. Since $m \geq 13$, the partition, π_2' is uniquely defined; it consists of all parts of π not divisible by $m-2$ possibly together with a part of length $m-2$. The partition, π_2 is uniquely defined too. It consists of all parts of π divisible by $m-2$ except one or possibly two parts of lengths $m-2$ each. This proves our claim, and we get $|\Pi_2| = p(m) \cdot p(m+2)$.

Since $m-2$ and $m-3$ are relatively prime, it is easy to see that $\Pi_1 \cap \Pi_2 = \emptyset$. Hence $|\Pi_1 \cup \Pi_2| = p(m) \cdot p(m+6) + p(m) \cdot p(m+2)$, and this proves the lemma for $r = 2$.

Now let $r \geq 3$. It is sufficient to show

$$2 \cdot p(m) \cdot p(m^{r-1}) < p(m^r).$$

Let Π be the set of all partitions of m^r of the following form. Take any partition of m^{r-1} and multiply each part by $m-1$. Combine this with a partition of m. Hence we get a partition π of $m^{r-1} \cdot (m-1) + m$. Combine π either with a part of length $2m$ together with $m^{r-2} - 3$ number of parts each of lengths m, or with two parts each of length $2m$ and $m^{r-2} - 5$ number of parts each of lengths m. By a similar argument as above, it is possible to show that $|\Pi| = 2 \cdot p(m) \cdot p(m^{r-1})$. Since the partition (m^r) is not in Π, we have $2 \cdot p(m) \cdot p(m^{r-1}) < p(m^r)$.

The proof of the lemma is now complete. □

Theorem 4.3.2. *Let $m \geq 5$, or $m \geq 2$ and $r = 1$. If $(A_m)^r \leq G \leq S_m$ wr S_r, then* t7
$k(G) \leq p(m^r)$, with equality if and only if $r = 1$ and $G = S_m$, or $r = 1$, $m = 3$ and $G = A_3$.

Proof. Put $n := m^r$. Let $r = 1$. In this case, we may and do suppose that $G = A_n$. The conjugacy classes of S_n can be naturally associated with the partitions of n. We will now associate the conjugacy classes of A_n with some partitions of n. If the conjugacy class of S_n associated with the partition π is a unique conjugacy class in A_n, then

associate this class with π. Otherwise, if the conjugacy class of S_n associated with π is the union of at least two conjugacy classes of A_n, then it must be the union of precisely two and π must be a partition of n with pairwise different odd parts. In this case associate one conjugacy class of A_n with π, and associate the other with the partition of n obtained from π by replacing the (unique) greatest odd part k by the parts 1 and $k-1$. It is easy to see that this map is an injection from the set of conjugacy classes of A_n to the set of partitions of n. If n is even or $n > 3$ is odd, then no conjugacy class of A_n is associated with the partition $\pi = (n)$ or $\pi = (n-3, 3)$, respectively. Finally, the statement of the theorem is true for $n = 2$ and $n = 3$. We conclude that the result is true for $t = 1$.

Now let $r \geq 2$ and $m \geq 5$. Then by Lemma 4.1.1 and by Theorem 4.1.2, we can write $k(G) \leq p(m)^r \cdot 2^{r-1}$. Finally, an application of Lemma 4.3.5 finishes the proof of the theorem. □

Notice that so far we nearly proved the following. If $N \neq \{1\}$ is a normal subgroup of a primitive group G of degree n with socle isomorphic to $(A_m)^r$ where A_m is a non-abelian alternating group different from A_6, then $k(N) \leq p(n)$ with equality if and only if $N = S_n$. By Lemma 4.3.4, the Aschbacher-O'Nan-Scott theorem and by Theorem 4.3.2, there exists a normal subgroup K of N so that $k(K) \leq p(m)^r$ and that N/K has an embedding into S_r. Now, by Lemma 4.1.1 and by Theorem 4.1.2, we see that $k(N) \leq k(K) \cdot k(N/K) \leq p(m)^r \cdot 2^{r-1}$. From this and by Lemma 4.3.5, we have $k(N) < p(m^r)$ unless $r = 1$. In case $r = 1$, Theorem 4.3.2 gives $k(N) \leq p(m)$. Finally, $m^r \leq n$ follows from Lemma 4.3.3 and hence we get $k(N) \leq p(n)$, since the partition function is strictly increasing.

We are now in the position to state the main result of this section.

Theorem 4.3.3. *Let G be a primitive subgroup of S_n, and let N be a normal subgroup of G. Then $k(N) \leq p(n)$, where $p(n)$ denotes the number of partitions of the integer n, with equality if and only if $N = S_n$ or if $n = 3$ and $N = A_3$.* t8

Proof. By the remark after Theorem 4.3.2, we may (and do) assume that $N \neq \{1\}$ is a normal subgroup of a primitive group G of degree n with socle $S = L^r$ where L is isomorphic to A_6 or is abelian or a non-alternating simple group.

By Theorem 4.3.1 we have $k(N) \leq n^6$.

Later, in Theorem 3.4.2, we give the lower bound $e^{2.5\sqrt{n}}/13n < p(n)$ for the partition function holding for all positive integers n. We use this to complete the proof of the claim.

It is easy to check that $n^6 < e^{2.5\sqrt{n}}/13n < p(n)$ for $n \geq 284$. Moreover, by the computer package [26] it is easily checked that $n^6 < p(n)$ holds for $252 \leq n \leq 284$, while $n^6 > p(n)$ for $n < 252$. So in order to establish the claim, we may (and do) suppose that $n < 252$. Now [26] contains a list of all primitive permutation groups G of degree less than 252 (up to permutation isomorphism) where L is isomorphic to A_6 or is abelian or a non-alternating simple group. From this list it is not too difficult to deduce the list of all normal subgroups, N. It is checked that we always have $k(N) < p(n)$ unless $N = S_6$ if $n = 6$, or if $N = A_3$ when $n = 3$. □

This sharpens part (i) of Corollary 2.15 of [42].

It is important for the reader to believe the proof of Theorem 4.3.3. For sufficiently large n there is no problem (this is part (i) of Corollary 2.15 of [42]) if one compares the asymptotic formula of $p(n)$ with the bound in part (iii) of Theorem 3.1.1. The concern is with the case when n is small. Currently, through work of Fulman and Guralnick [23], Guralnick and the author are working on improving the bounds in Lemma 4.3.1 and Theorem 4.2.1. It is possible that 'almost all' almost simple groups of degree n have at most $n + 3$ conjugacy classes. Moreover, it is conjectured that a completely reducible subgroup of $GL(n, q)$ has at most q^n conjugacy classes. If one could prove these, then we could sharpen the $k(N) \leq n^6$ bound in Theorem 4.3.1 to something like $k(N) \leq 2n$. This would give a much more elegant proof for Theorem 4.3.3.

4.4 The general bound

In this section we prove Theorem 4.1.3.

We start with a couple of rather technical lemmas.

The first one helps us to start the induction in proving Theorem 4.1.3.

Lemma 4.4.1. *If G is a subgroup of S_n with $n \leq 12$, then $k(G) \leq 5^{n/4}$.* 16

Proof. Use induction on n. If G is intransitive and has an orbit Δ of length $k < n$, then by induction and by Lemma 4.1.1, we have $k(G) \leq k(G/K) \cdot k(K) \leq 5^{k/4} \cdot 5^{(n-k)/4} = 5^{n/4}$ where K is the kernel of the action of G on Δ. For transitive groups this can easily be read off from the library of transitive permutation groups of the computer package [26]. □

Note that the bound in Lemma 4.4.1 is sharp for direct products of ℓ isomorphic copies of either S_4 or D_8 acting naturally on $n = 4\ell$ letters.

We also need to give an upper estimate for the number of partitions of the integer n. Explicit upper bounds appear in [21] and [68] for example, but we prefer a much weaker estimate in a different form.

Lemma 4.4.2. *For $n > 12$ we have $p(n) < c \cdot (3/2)^n$ where $c = (2 \cdot \sqrt{3})^{-\frac{1}{2}}$.* 17

Proof. For $n \geq 50$ we have $p(n) \leq e^{\pi\sqrt{2n/3}}$ by [21], and the right hand side is smaller than $c \cdot (3/2)^n$. For $12 < n < 50$ the statement is checked easily. □

Another technical lemma we need is

Lemma 4.4.3. *If $G \leq S_n$ is primitive with $7 \leq n \leq 12$ and N is a normal subgroup of G of order prime to 7, then $k(N) \leq 2^{(n-1)/2}$.* 18

Proof. This is checked easily by [26]. □

In certain cases in proving our general bound (for small degrees) Lemma 4.1.1 is not sufficient. We need a more careful estimate. The following result is taken from page 447 of [38].

Lemma 4.4.4 (Kovács, Robinson, [38]). *Let N be a normal subgroup of an arbitrary finite group G. If every subgroup of G/N has at most t conjugacy classes, then $k(G) \leq t \cdot \#\{G$ -conjugacy classes of $N\}$.*

We now begin the proof of Theorem 4.1.3.

Choose a counterexample G with n minimal. We may suppose that G is transitive. For if G was intransitive with an orbit Δ of length $k < n$, then by assumption we would have $k(G) \leq k(G/K) \cdot k(K) \leq 3^{(k-1)/2} \cdot 3^{(n-k-1)/2} < 3^{(n-1)/2}$ where K is the kernel of the action of G on Δ. Moreover, we may also assume that G has no blocks of imprimitivity of size greater than 2 and less than $n/2$. For if G had a block Δ of size $2 < k < n/2$, then we would have $k(G) \leq k(G/B) \cdot k(B) \leq 3^{((n/k)-1)/2} \cdot (3^{(k-1)/2})^{(n/k)} = 3^{(n-1)/2}$ where B is the kernel of the action of G on the blocks of imprimitivity associated to Δ.

Let H be the point stabilizer of the transitive group G. By the observations above and by Theorem 1.5.A of [20] we have four possibilities to consider for subgroups of G containing H. These were also given in [38], so for simplicity, from now on we use the notations of that paper.

(i) H max G.

(ii) H max K max G for some subgroup K of G with $(G : K) = 2$.

(iii) H max K max G for some subgroup K of G with $(K : H) = 2$.

(iv) H max K max L max G for some subgroups K, L of G with $(K : H) = (G : L) = 2$.

By Lemma 4.4.1, we may suppose that $n \geq 13$.

Case (i). By Theorem 4.3.3 and Lemma 4.4.2, we have $k(G) \leq p(n) < c \cdot (3/2)^n \leq 3^{(n-1)/2}$.

Case (ii). Let $(K : H) = a$. We may suppose that $a \geq 7$ (since $n \geq 13$). Let $C = core_K(H)$. For any x in $G \backslash K$ we have $C \cap C^x = \{1_G\}$, as $core_G(H)$ is trivial. Now K/C

and K/C^x are both isomorphic to primitive permutation groups of degree a, and CC^x is normal in K, so by Theorem 4.3.3, we have $k(K/C) \leq p(a)$ and $k(CC^x/C^x) \leq p(a)$. Hence $k(K) \leq k(K/C) \cdot k(C/C \cap C^x) \leq p(a)^2$. Now $k(G) \leq 2 \cdot k(K) \leq 2 \cdot p(a)^2$. But we are assuming that $k(G) > 3^{(2a-1)/2}$, so we have $2 \cdot p(a)^2 > 3^{(2a-1)/2}$. This is checked to be false for $7 \leq a \leq 12$. Else if $a > 12$, we get $c \cdot (3/2)^a > 3^{(2a-1)/2}$ by Lemma 4.4.2, which is also a contradiction.

Case (iii). Let $(G : K) = a$ and $C = core_G(K)$. Then C is an elementary abelian 2-group of order at most 2^a, and G/C is isomorphic to a primitive permutation group of degree a. Suppose first that $a > 12$. By Lemma 4.4.2 and by our assumption, we have $c \cdot (3/2)^a \cdot 2^a > p(a) \cdot 2^a \geq k(G) > 3^{(2a-1)/2}$, which is a contradiction. By Lemma 4.4.1 and by the above argument, we may assume that $7 \leq a \leq 12$. If the primitive group G/C of degree a has order not divisible by 7, then by Lemma 4.4.3, we have $k(G/C) \leq 2^{(a-1)/2}$. Hence we get $2^{(3a-1)/2} \geq k(G) > 3^{(2a-1)/2}$, which is also a contradiction. So we may suppose that G/C has an element of order 7. By Lemma 4.4.1, every subgroup of G/C has at most $5^{a/4}$ conjugacy classes, so by Lemma 4.4.4 we get $k(G) \leq ((2^a - 2 \cdot 2^{a-7})/7 + 2 \cdot 2^{a-7}) \cdot 5^{a/4}$. By assumption we have $3^{(2a-1)/2} < ((2^a - 2 \cdot 2^{a-7})/7 + 2 \cdot 2^{a-7}) \cdot 5^{a/4}$, which is also false.

Case (iv). Let $(L : K) = a$. Let $C = core_L(H)$ and $D = core_L(K)$. For any x in $G \setminus L$ we have $C \cap C^x = \{1_G\}$. Then L/D is isomorphic to a primitive permutation group of degree a, and D/C is an elementary abelian 2-group of order at most 2^a. By Theorem 4.3.3, $k(L/D) \leq p(a)$, so that $k(L/C) \leq 2^a \cdot p(a)$. Now set $M = CC^x$. Then $k(MD^x/D^x) \leq p(a)$ by Theorem 4.3.3, so $k(M/M \cap D^x) \leq p(a)$. Hence $k(M/C^x) \leq k(M/M \cap D^x) \cdot k(M \cap D^x/C^x) \leq 2^a \cdot p(a)$, so that $k(C) \leq 2^a \cdot p(a)$, $k(L) \leq 2^{2a} \cdot p(a)^2$, and $k(G) \leq 2 \cdot 4^a \cdot p(a)^2$. Suppose first that $a > 12$. By Lemma 4.4.2 and by our assumption, we have $3^{(4a-1)/2} < 2 \cdot 2^{2a} \cdot c^2 \cdot (3/2)^{2a}$, which is false. By Lemma 4.4.1 and by the previous argument, we may suppose that $4 \leq a \leq 12$. First, let $a \geq 7$. If L/D does not contain A_a, then we have $k(L/C) \leq 2^a \cdot 2^{(a-1)/2}$ by Lemma 4.4.3.

Moreover, $k(MD^x/D^x) \leq 2^{(a-1)/2}$, so $k(C) = k(M/C^x) \leq 2^{(3a-1)/2}$. This means that $k(L) \leq 2^{3a-1}$, and so $k(G) \leq 8^a$. By assumption we have $8^a > 3^{(4a-1)/2}$, which is a contradiction. Else if the primitive group L/D of degree a contains A_a, then $k(L/C) \leq ((2^a - 2 \cdot 2^{a-7})/7 + 2 \cdot 2^{a-7}) \cdot 5^{a/4}$ by Lemma 4.4.4. So this way we get $k(G) \leq 2^a p(a) \cdot ((2^a - 2 \cdot 2^{a-7})/7 + 2 \cdot 2^{a-7}) \cdot 5^{a/4}$ which is checked to be smaller than $3^{(4a-1)/2}$. (Applying the inequality $p(a) \leq 2^{(a+1)/2}$ suffices to show this.) This is a contradiction. Let $a = 4$. Now L/D is a primitive group of order divisible by 3, so by Lemma 4.4.4 we get $k(L/C) \leq ((2^4 - 4)/3 + 4) \cdot 5 = 40$. Similarly, we get $k(C) = k(M/C^x) \leq 40$. This sums up to $k(G) \leq 2 \cdot k(L) \leq 3200$, which is again a contradiction. Let $a = 5$. By Lemma 4.4.4, we get $k(L/C) \leq ((2^5 - 2)/5 + 2) \cdot 7 = 56$. Similarly $k(M/C^x) \leq 56$. This means that $k(G) \leq 2 \cdot 56^2 = 6272$, which yields another contradiction. Finally, let $a = 6$. All primitive groups of degree 6 contain a 5-cycle, so by Lemma 4.4.4, we can put $k(L/C) \leq ((2^6 - 4)/5 + 4) \cdot 11 = 176$. Similarly we see that $k(M/C^x) \leq 176$. So we have $k(G) \leq 2 \cdot 176^2$, which is a contradiction.

4.5 Groups with no composition factor of order 2

To improve on the $3^{(n-1)/2}$ general bound, the next step would probably be to show that $k(G) \leq 5^{(n-1)/3}$ holds for all permutation groups G of degree $n > 3$. This would be sharp in case $G = D_8$ or $G = S_4$ when $n = 4$. A careful modification of the proof of Theorem 4.1.3 makes it possible to attain the $5^{(n-1)/3}$ bound but only for permutation groups with no composition factor isomorphic to C_3 provided that $k(H) \leq 5^{n/4}$ holds for $n \leq 31$ whenever H is a (transitive) group of degree n. If we allow G to possess composition factors isomorphic to C_3, then we have more cases to consider which are not discussed by the proof of Theorem 4.1.3.

Next we restrict our attention to some of these additional cases and make a step in developing the method to deal with groups having C_3 as a composition factor. To keep the argument reasonably short, we restrict the structure of G (by excluding C_2

from the set of composition factors of G) but in exchange we prove a sharper bound than the proposed $k(G) \leq 5^{(n-1)/3}$.

Theorem 4.5.1. *If G is a subgroup of S_n with no composition factor isomorphic to C_2, then $k(G) \leq (5/3)^n$.* t4.5

We start with the following

Lemma 4.5.1. *If G is a transitive permutation group of degree n with $5 \leq n \leq 9$ such that no composition factor of G is isomorphic to C_2, then $k(G) \leq k(A_n)$.* l10

Proof. This is easily checked by [26]. □

To prove Theorem 4.5.1, it is sufficient to see that if G is a permutation group of degree $n > 4$ with no composition factor isomorphic to C_2, then $k(G) \leq (5/3)^{n-1}$.

Let G be a counterexample to the previous statement with n minimal. As in the beginning of the previous section, we may assume that G is transitive. Let Δ be a block of imprimitivity for G, and let B be the kernel of the action of G on the system of blocks associated with Δ. Again, by the argument at the beginning of the previous section, we may suppose that $|\Delta| = 1$, 2, 3, 4, $n/4$, $n/3$, $n/2$ or n. Now $|\Delta|$ cannot be 2 or 4, since in this case the normal subgroup B is solvable of even order. Moreover, $|\Delta|$ can not be $n/4$ or $n/2$ since in this case the factor group G/B is solvable of even order.

By these observations and by Theorem 1.5.A of [20], we have four possibilities to consider for proper subgroups K, L of G strictly containing the point-stabilizer H. These are the following.

(i) H max G.

(ii) H max K max G for some subgroup K of G with $(G : K) = 3$.

(iii) H max K max G for some subgroup K of G with $(K : H) = 3$.

(iv) H max K max L max G for some subgroups K, L of G with $(K : H) = (G : L) = 3$.

By Lemma 4.4.1, we may suppose that $n \geq 13$.

Case (i). By Theorem 4.3.3 and by Lemma 4.4.2, we have $k(G) \leq p(n) < c \cdot (3/2)^n \leq (5/3)^{n-1}$ which is a contradiction.

Case (ii). Observe that K is normal in G. Let $(K : H) = a$, and let $C = core_K(H)$. For any x in $G \setminus K$ we have $C \cap C^x \cap C^{x^2} = \{1_G\}$, as $core_G(H)$ is trivial. Now K/C^x and K/C^{x^2} are both isomorphic to primitive permutation groups of degree a, and both CC^x and $(C^x \cap C)C^{x^2}$ are normal in K, so by Theorem 4.3.3, we have $k(K/C^x) \leq p(a)$, $k(CC^x/C^x) \leq p(a)$ and $p(a) \geq k((C^x \cap C)C^{x^2}/C^{x^2}) = k(C^x \cap C)$. Hence $k(K) \leq k(K/C) \cdot k(C) \leq k(K/C) \cdot k(C/C^x \cap C) \cdot k(C^x \cap C) \leq k(K/C) \cdot k(CC^x/C^x) \cdot k(C^x \cap C) \leq p(a)^3$. Now $k(G) \leq 3 \cdot k(K) \leq 3 \cdot p(a)^3 = 3 \cdot p(n/3)^3$. By Lemma 4.4.2 we have $k(G) \leq 3c^3 \cdot (3/2)^n < (5/3)^{n-1}$ for $n > 36$. So we must have $15 \leq n \leq 36$. It is checked by [26] that in this case we again have $k(G) \leq 3 \cdot p(n/3)^3 < (5/3)^{n-1}$. This is a contradiction.

Case (iii). Let $(G : K) = a$, and let $C = core_G(K)$. Since C has no composition factor isomorphic to C_2, we have $k(C) \leq |C| \leq 3^{n/3}$. On the other hand, G/C is isomorphic to a primitive permutation group of degree a, so we have $k(G/C) \leq p(a)$ by Theorem 4.3.3. This yields $k(G) \leq k(C) \cdot k(G/C) \leq 3^{n/3} \cdot p(n/3)$. By Lemma 4.4.2, we have $k(G) \leq 3^{n/3} \cdot c \cdot (3/2)^{n/3} < (5/3)^{n-1}$ for $n > 36$. So we must have $15 \leq n \leq 36$. For $n = 30$, 33 and 36 it is checked by [26] that $k(G) \leq 3^{n/3} \cdot p(n/3) < (5/3)^{n-1}$. Finally since G/C is a primitive permutation group with no composition factor isomorphic to C_2, by Lemma 4.5.1 we can definitely replace $p(a)$ by $k(A_a)$ in the above estimate for $5 \leq a \leq 9$. Hence $k(G) \leq 3^{n/3} \cdot k(A_{n/3}) < (5/3)^{n-1}$ for $15 \leq n \leq 27$. This is a contradiction.

Case (iv). Observe that L is normal in G. Let $(L : K) = a$. Moreover let $C = core_L(H)$ and $D = core_L(K)$. For any x in $G \setminus L$ we have $C \cap C^x \cap C^{x^2} = \{1_G\}$,

as $core_G(H)$ is trivial. Now L/D is isomorphic to a primitive group of degree a. Since D/C has no composition factor isomorphic to C_2, it is an elementary abelian 3-group of order at most 3^a. So from these, we have $k(L/C) \leq k(L/D) \cdot k(D/C) \leq 3^a \cdot p(a)$. Let $M = CC^x$. Since MD^x is normal in L, by Theorem 4.3.3 we have $p(a) \geq k(MD^x/D^x) = k(M/M \cap D^x)$. This yields $k(C/C^x \cap C) = k(M/C^x) \leq k(M/M \cap D^x) \cdot k(M \cap D^x/C^x) \leq p(a) \cdot 3^a$. We next bound $k(C^x \cap C)$. Since $(C^x \cap C)D^{x^2}/D^{x^2}$ is a normal subgroup of the primitive group L^{x^2}/D^{x^2} of degree a, by Theorem 4.3.3 we see that $k(C^x \cap C/D^{x^2} \cap C^x \cap C) = k((C^x \cap C)D^{x^2}/D^{x^2}) \leq p(a)$. Since $D^{x^2} \cap C^x \cap C$ is isomorphic to a subgroup of D^{x^2}/C^{x^2}, it has order at most 3^a. So we have $k(C^x \cap C) \leq k(C \cap C^x/D^{x^2} \cap C^x \cap C) \cdot k(D^{x^2} \cap C^x \cap C) \leq p(a) \cdot 3^a$. Putting our results together we get $k(G) \leq 3 \cdot k(L) \leq 3 \cdot k(L/C) \cdot k(C) \leq 3^{a+1} \cdot p(a) \cdot k(C) \leq 3^{a+1} \cdot p(a) \cdot k(C/C^x \cap C) \cdot k(C^x \cap C) \leq 3^{3a+1} \cdot p(a)^3 = 3 \cdot 3^{n/3} \cdot p(n/9)^3$. By Lemma 4.4.2, we have $k(G) \leq 3 \cdot 3^{n/3} \cdot p(n/9)^3 < 3 \cdot 3^{n/3} \cdot c^3 \cdot (3/2)^{n/3} < (5/3)^{n-1}$ for $n > 108$. For $n = 90$, 99 and 108, it is checked by [26] that $k(G) \leq 3 \cdot 3^{n/3} \cdot p(n/9)^3 < (5/3)^{n-1}$. For $n = 45$, 54, 63, 72 and 81, notice that by Lemma 4.5.1, we can write $k(G) \leq 3 \cdot 3^{n/3} \cdot k(A_{n/9})$, which is checked to be smaller than $(5/3)^{n-1}$. Now $n \neq 18$ or 36, because $a \neq 2$ or 4, since G does not have a composition factor isomorphic to C_2. So we must have $n = 27$. Let Δ be the orbit of K which contains the point stabilized by H. Let B be the base group of the system of imprimitivity associated to Δ. Then B is an elementary abelian 3-group, and G/B is a transitive group of degree 9. Since G/B has no composition factor isomorphic to C_2, by Lemma 4.5.1, we get $k(G/B) \leq k(A_9) = 18$. Hence $k(G) \leq k(B) \cdot k(G/B) \leq 3^9 \cdot 18 < (5/3)^{26}$. This is the final contradiction.

This completes the proof of Theorem 4.5.1.

4.6 Nilpotent groups

The other extreme (and possibly hardest) case to consider in finding the best possible general estimate for $k(G)$ is when the permutation group is a 2-group. The example of

$D_8 \wr C_{n/4}$ for n a power of 2 of [42] shows that a general upper bound for $k(G)$ of the form c^n should satisfy $c \geq 5^{1/4} = 1.495....$ We prove the following

Theorem 4.6.1. *If G is a nilpotent subgroup of S_n, then $k(G) \leq 1.52^n$.* t5.5

Proof. Let G be a counterexample with n minimal. We may suppose that G is transitive. For if G is intransitive with an orbit Δ of length $k < n$, then $k(G) \leq k(G/K) \cdot k(K) \leq 1.52^k \cdot 1.52^{n-k}$ where K is the kernel of the action of G on the set Δ.

We may suppose that G is a p-group by Theorem 1 on page 30 of [**?**]. For otherwise, we may consider G as a subgroup of S_Ω where $|\Omega| = n = {p_1}^{k_1}...{p_t}^{k_t}$ with $t \geq 2$ and ${p_i}^{k_i}$ distinct prime powers. (Note that $|G|$ and n have the same set of prime divisors.) We may take $\Omega = X_1 \times X_2 \times ... \times X_t$ where $|X_i| = {p_i}^{k_i}$ for all $1 \leq i \leq t$ such that the Sylow p_i-subgroup of G acts transitively on X_i for all $1 \leq i \leq t$. Now by the assumption on the minimality of n, we get $k(G) \leq 1.52^{\sum_{i=1}^{t} {p_i}^{k_i}} \leq 1.52^n$.

The following lemma shows that G can be taken to be a 2-group.

Lemma 4.6.1. *If G is a p-group of S_n with $p > 2$, then $k(G) \leq 5^{n/4}$.*

Proof. We may and do assume that $p = 3$. For if $p > 3$, then $k(G) \leq |G| \leq 5^{(n-1)/4}$. We claim that if G is a 3-subgroup of S_n where $n \leq 27$, then $k(G) \leq 1.45^n$. By the argument at the beginning of this section we may suppose that G is transitive. Let $n = 3^t$. If $t = 1$, then $k(G) \leq 3 < 1.45^3$. If $t = 2$, then by [26] we see that $k(G) \leq 17 < 1.45^9$. Let $t = 3$. A Sylow 3-subgroup of S_{27} has order 3^{13} and has 1683 conjugacy classes, by [56]. So if G has order greater than 3^{10} (and at most 3^{13}), then by Lemma 4.2.2, we get $k(G) \leq 9 \cdot 1683 < 1.45^{27}$. Let $|G| \leq 3^{10}$. Since $Z(G)$ is an abelian permutation group of degree 27, we have $|Z(G)| \leq 3^3$. Moreover, any conjugacy class of G not contained in $Z(G)$ has order at least 3. From this we get

$$k(G) \leq 3^3 + ((3^{10} - 3^3)/3) < 1.45^{27},$$

which proves our claim. To finish the proof of the lemma, it is sufficient to show that if

G is a transitive 3-subgroup of S_n where $n = 3^t$, then $k(G) \leq 5^{n/4}$. Let us prove this by induction on t. This is true for $t \leq 3$. Let $t > 3$ and let Δ be a block of imprimitivity for G of size 27. Let the base group of the system of imprimitivity associated to Δ be B. Then, by Lemma 4.1.1 and by our inductive hypothesis, we get

$$k(G) \leq k(B) \cdot k(G/B) \leq 1.45^n \cdot 5^{n/108} \leq 5^{n/4}.$$

□

So, let G be a transitive 2-group of degree $n = 2^k$. If $k \leq 4$, then $k(G) \leq k(\mathrm{Syl}_2(S_n)) \leq 5^{n/4} < 1.52^n$ by the [26] library of transitive permutation groups. Let $k = 5$. Take a block Δ_0 of order 16. This block induces a system of imprimitivity Σ. Let the kernel of the action of G on Σ be K, and let the kernel of the action of K on Δ_0 be K_0. Now K_0 is faithful on the set $\Omega \setminus \Delta_0$ with orbits of size at most 16, so we have $k(K_0) \leq 5^4$. Furthermore, K/K_0 is faithful and transitive on a set of size 16, so $k(K/K_0) \leq k(\mathrm{Syl}_2(S_{16})) = 230$. This means that $k(G) \leq 2 \cdot 5^4 \cdot 230 = 287500 < 5^8 < 1.52^n$. Let $k = 6$. Take a block Δ_0 of order 32. Let Σ be the system of imprimitivity induced by this block, and let the kernel of the action of G on Σ be K. Now let the kernel of the action of K on Δ_0 be K_0. The group K_0 is faithful on the set $\Omega \setminus \Delta_0$ with orbits of size at most 32. By the results obtained in case $k = 5$, we get $k(G) \leq 2 \cdot k(K/K_0) \cdot k(K_0) \leq 2 \cdot 287500 \cdot 5^8 < 1.51^n$. Finally, let $k \geq 7$. Again take a block Δ_0 of order 64. Let the induced system of imprimitivity be Σ, and let the kernel of the action of G on Σ be K. Since K has orbits of length at most 64, we have $k(K) \leq 1.51^n$. Furthermore, we have $k(G/K) \leq 1.52^{n/64}$ by induction. This gives $k(G) \leq 1.51^n \cdot 1.52^{n/64} < 1.52^n$, which is the final contradiction.

The proof of Theorem 4.6.1 is now complete. □

Note that the bound in Theorem 4.6.1 is 'close' to best possible. The direct product of ℓ isomorphic copies of D_8 acting naturally on $n = 4\ell$ letters has precisely $5^{n/4}$

conjugacy classes.

The above proof uses the fact that if G is a transitive 2-group of degree n, then $k(G) \leq k(Syl_2(S_n)) \leq p(n)$ provided that $n \leq 16$. However, the $D_8 \wr C_{n/4}$ example in [42] and the asymptotic estimate for the number of conjugacy classes of the symmetric 2-group of [56] shows that this is definitely not the case for all 2-powers, n. Little computer search suggests that the group $D_8 \wr E(8)$ has the maximal number of conjugacy classes among transitive 2-groups of degree 32 where $E(8)$ is the elementary abelian 2-group in its regular action. So we ask the following.

Question 4.6.1. *Let G be a transitive 2-group of degree 2^t with the property that $k(G)$ is maximal among all transitive 2-groups of degree 2^t. Then, is it true that we have one of the following?*

(i) If $t \leq 4$, then G is a Sylow subgroup of S_{2^t} and $k(G) \leq p(n)$.

(ii) If $t \geq 5$, then G is permutation isomorphic to the permutation group $D_8 \wr E(2^{t-2})$ where $E(2^{t-2})$ is the elementary abelian 2-group of order 2^{t-2} with its regular action, and $k(G) > p(n)$.

Finally, we note that it is very likely that $k(G) \leq 5^{n/4}$ should be the best possible estimate even for arbitrary subgroups G of S_n. However, we believe that a proof for this conjecture is out of reach at the time of writing.

Chapter 5

Covering the symmetric groups with proper subgroups

5.1 Introduction

Let G be a group that is a set-theoretic union of finitely many proper subgroups. Cohn [15] defined the function $\sigma(G)$ to be the least integer m such that G is the union of m of its proper subgroups. (A result of Neumann [54] states that if G is the union of m proper subgroups where m is finite and small as possible, then the intersection of these subgroups is a subgroup of finite index in G. Hence in investigating σ we may assume that G is finite.) It is an easy exercise that $\sigma(G)$ can never be 2; it is at least 3. Groups that are the union of three proper subgroups, as $C_2 \times C_2$ is for example, are investigated in the papers [64], [31], and [12]. Moreover, $\sigma(G)$ can be 4, 5, and 6 too, as the examples, $C_3 \times C_3$, A_4, and $C_5 \times C_5$ show. However, Tomkinson [67] proved that there is no group G with $\sigma(G) = 7$. Cohn [15] showed that for any prime power p^a there exists a solvable group G with $\sigma(G) = p^a + 1$. In fact, Tomkinson [67] established that $\sigma(G) - 1$ is always a prime power for solvable groups G. He also pointed out that it would be of interest to investigate σ for families of simple groups.

Indeed, the situation for nonsolvable groups seems to be totally different. Bryce, Fedri, Serena [13] investigated certain nonsolvable 2-by-2 matrix groups over finite fields, $((P)G(S)L(2,q))$ and obtained the formula $\frac{1}{2}q(q+1)$ for even prime powers $q \geq 4$, and the formula $\frac{1}{2}q(q+1)+1$ for odd prime powers $q \geq 5$. Moreover, Lucido [44] found that $\sigma(Sz(q)) = \frac{1}{2}q^2(q^2+1)$ where $q = 2^{2m+1}$. There are partial results due to Bryce and Serena for determining $\sigma((P)G(S)L(n,q))$.

In this paper the following is established.

Theorem 5.1.1. *Let $n > 3$, and let S_n and A_n be the symmetric and the alternating group respectively on n letters.* t11

(1) We have $\sigma(S_n) = 2^{n-1}$ if n is odd unless $n = 9$, and $\sigma(S_n) \leq 2^{n-2}$ if n is even.

(2) If $n \neq 7, 9$, then $\sigma(A_n) \geq 2^{n-2}$ with equality if and only if n is even but not divisible by 4.

In the following sections we will prove more than what is stated in Theorem 5.1.1. We will obtain exact or asymptotic formulas in all (infinite) cases (possibly) except for $\sigma(A_p)$ where p is a prime of the form $(q^k-1)/(q-1)$ where q is a prime power and k is a positive integer.

For the groups S_9, S_{12}, A_7, and A_9 we only prove $172 \leq \sigma(S_9) \leq 256$, $\sigma(S_{12}) \leq 761$, $\sigma(A_7) \leq 31$, and $\sigma(A_9) \geq 80$. Notice that the numbers 761 and 31 are primes not of the form $q+1$ where q is a prime power. We prove that $\sigma(G)$ can indeed be such a prime.

Proposition 5.1.1. *For the smallest Mathieu group we have $\sigma(M_{11}) = 23$.* prop11

This result was also proved (independently) by Holmes in [32]. In her paper many interesting results are found about sporadic simple groups. It is proved that $\sigma(M_{22}) = 771$, $\sigma(M_{23}) = 41079$, $\sigma(O'N) = 36450855$, $\sigma(Ly) = 112845655268156$, $5165 \leq \sigma(J_1) \leq 5415$, and that $24541 \leq \sigma(McL) \leq 24553$.

At this point we note that Tomkinson [67] conjectured that $\sigma(G)$ can never be 11 nor 13.

In Section 6 we investigate the relationship between some of the known infinite series of σ.

The commuting graph Γ of a group G is as follows. Let the vertices of Γ be the elements of G and two vertices g, h of Γ are joined by an edge if and only if g and h commute as elements of G. (The commuting graph is used to measure how abelian the group is. See [22], and [62].) Several people have studied $\alpha(G)$, the maximal cardinality of an empty subgraph of Γ and $\beta(G)$, the minimal cardinality of a covering of the vertices of Γ by complete subgraphs. (See the papers [22], [52], and [58].) Brown investigated the relationship between the numbers $\alpha_n = \alpha(S_n)$ and $\beta_n = \beta(S_n)$. In [10] it is shown that these numbers are surprisingly close to each other, though for $n \geq 15$, they are never equal [11].

As an application of Theorem 5.1.1, we prove that if we add 'more' edges to the commuting graph of the symmetric group, then the corresponding numbers will be equal in infinitely many cases. Let G be a group. Define a graph Γ' on the elements of G with the property that two group elements are joined by an edge if and only if they generate a proper subgroup of G. Similarly as for the commuting graph, we may define $\alpha'(G)$ and $\beta'(G)$ for our new graph, Γ'. Put $\alpha'_n = \alpha'(S_n)$ and $\beta'_n = \beta'(S_n)$. The theorem can now be stated.

Theorem 5.1.2. *There is a subset S of density 1 in the set of all primes, so that $\alpha'_n = \beta'_n$ holds for all $n \in S$.* t12

The equality $\alpha'_n = \beta'_n$ is valid for very small values of n also. Does it hold for all n?

We note that the problem of covering groups by subgroups has found interest for many years. The first reference the author is aware of is the 1926 work of Scorza [64]. Probably Neumann [54], [55] was the first to study the number of (abelian) subgroups needed to cover a (not necessarily finite) group G in relation to the index of the center

of G. For a survey of this area see [65]. On the other hand, for an extensive account of work in (packing and) covering groups with (isomorphic) subgroups (or of subgroups of a specified order) the reader is referred to [35].

5.2 Preliminaries

Let G be S_n or A_n, the symmetric or the alternating group on n letters. Let Π be a set of permutations of G. Define $\sigma(\Pi)$ to be the least integer m such that Π is the subset of the set-theoretic union of m proper subgroups of G. It is straightforward that $\sigma(\Pi) \leq \sigma(G)$. We will say that a set $\mathcal{H} = \{H_1, \ldots, H_m\}$ of m proper subgroups of G is *definitely unbeatable* on Π if $\Pi \subseteq \bigcup_{i=1}^{m} H_i$; if $\Pi \cap H_i \cap H_j = \emptyset$ for all $i \neq j$; and if $|S \cap \Pi| \leq |H_i \cap \Pi|$ holds whenever $1 \leq i \leq m$ and when $S \notin \mathcal{H}$ is a proper subgroup of G. If $\mathcal{H}$ is definitely unbeatable on Π, then $|\mathcal{H}| = \sigma(\Pi) \leq \sigma(G)$.

We will call a permutation an $(i, n-i)$-cycle if it is a product of two disjoint cycles one of length i and one of length $n-i$, and will call a permutation an $(i, j, n-i-j)$-cycle if it is a product of three disjoint cycles one of length i, one of length j, and one of length $n-i-j$.

We will use the list of primitive permutation groups of [19] and the result of the chapter before the previous one stating that a primitive permutation group of degree n not containing A_n has order at most e^n. Sometimes the computer package [26] is also used for computations in symmetric and alternating groups of small degree.

5.3 Symmetric groups

First, let us consider the case where the degree of the symmetric group is odd.

Theorem 5.3.1. *If $n > 1$ is odd, then $\sigma(S_n) = 2^{n-1}$ unless $n = 9$.* t31

Proof. The set-theoretic union of A_n and all maximal intransitive subgroups of S_n is

S_n. This gives

$$\sigma(S_n) \leq 1 + \frac{1}{2} \cdot \sum_{i=1}^{n-1} \binom{n}{i} = 1 + \frac{1}{2}(2^n - 2) = 2^{n-1}.$$

The upper bound is known to be exact for $n = 3$ and $n = 5$ from [15], so assume that $n \geq 7$. Now let Π be the set of all permutations of S_n, which are the products of at most two disjoint cycles. It is sufficient to prove $\sigma(\Pi) \geq 2^{n-1}$.

For $n \geq 11$ the latter inequality is the direct consequence of the fact that the set consisting of A_n and of all maximal intransitive subgroups of S_n is definitely unbeatable on Π. This is proved in two steps.

Claim 5.3.1. *Let H_1 and H_2 be A_n or a maximal intransitive subgroup of S_n. If $H_1 \neq H_2$, then $\Pi \cap H_1 \cap H_2 = \emptyset$.*

Proof. Indeed, $A_n \cap \Pi$ is the set of all n-cycles, while $S_\Delta \times S_{\overline{n}\setminus\Delta} \cap \Pi$ is the set of all permutations of the form $\pi = \delta \cdot \overline{\delta}$ with δ a $|\Delta|$-cycle from S_Δ and $\overline{\delta}$ a $|\overline{n} \setminus \Delta|$-cycle from $S_{\overline{n}\setminus\Delta}$, where $\overline{n}$ denotes the set of n letters on which S_n acts and where Δ is a nontrivial proper subset of $\overline{n}$. □

Claim 5.3.2. *Suppose that $n \geq 11$ is odd. Let H be A_n or a maximal intransitive subgroup of S_n, and let S be any subgroup of S_n different from A_n and different from any maximal intransitive subgroup. Then $|S \cap \Pi| \leq |H \cap \Pi|$.*

Proof. It can be assumed that S is maximal in S_n. First let $n \geq 17$. If S is primitive, then $|S \cap \Pi| \leq |S| \leq e^n$ follows from the chapter before the previous one, while we have $e^n \leq ((n-1)/2)! \cdot ((n-3)/2)! \leq |H \cap \Pi|$. If S is imprimitive, then $|S \cap \Pi| \leq |S| \leq (n/p)!^p \cdot p! \leq ((n-1)/2)! \cdot ((n-3)/2)! \leq |H \cap \Pi|$ holds, where p is the smallest prime divisor of n. If $n = 11$ or 13, then S is primitive and $|S| < ((n-1)/2)! \cdot ((n-3)/2)!$ is checked easily by [19] or the chapter before the previous one. If $n = 15$, then by [19], S is conjugate to a maximal imprimitive group with five blocks of imprimitivity,

to a maximal imprimitive group with three blocks of imprimitivity, or to S_6 acting on the set of distinct pairs of points. In the first and the third case we have $|S| \leq 3!^5 \cdot 5! < 6! \cdot 7! \leq |H \cap \Pi|$. Let S be a maximal imprimitive subgroup of S_{15} with three blocks of imprimitivity. Now in $S \cap \Pi$ the number of 15-, $(5,10)$-, $(3,12)$, and $(6,9)$-cycles are $(5!^3 \cdot 3!)/15$, $72 \cdot 5!^2/5$, $5!^3/2$, and $5!^3/3$, respectively. All together we get $|S \cap \Pi| = 2338560 < 6! \cdot 7!$. □

The remaining cases, $n = 7$, 9, are dealt separately.

Let $n = 7$. We have $\sigma(\Pi) \leq 64$. We will show that $\sigma(\Pi) \geq 64$. Let $\mathcal{L}$ be a set of $\sigma(S_7)$ maximal subgroups of S_7 covering S_7. Since there is exactly one maximal subgroup (an intransitive one) containing a given $(3,4)$- or a given $(2,5)$-cycle, all $\binom{7}{3} + \binom{7}{2} = 56$ maximal intransitive groups which do not stabilize any point are contained in $\mathcal{L}$. The group A_7 is also contained in $\mathcal{L}$. For if it would not, then the subset of all 7-cycles of Π (having 6! elements) could only be covered by 5! maximal primitive groups each conjugate to $AGL(1,7)$. So we would get $\sigma(\Pi) \geq 56+5!$, which contradicts $\sigma(\Pi) \leq 64$. We claim that $\mathcal{L}$ contains all 7 one-point stabilizers as well, hence $\sigma(\Pi) \geq 56 + 1 + 7 = 64$ would follow. To see this, consider the $(1,6)$-cycles of Π. A maximal subgroup of S_7 containing such permutations is either a stabilizer of a point, or is conjugate to the primitive affine group, $AGL(1,7)$. Suppose that $\mathcal{L}$ does not contain the stabilizer of the point α. Then the 6-cycles of $S_{\overline{n}\setminus\{\alpha\}}$ are covered with at least 60 primitive affine groups, which gives the contradiction $\sigma(\Pi) \geq 56 + 60$.

Let $n = 9$. We have $\sigma(\Pi) \leq 256$. Partition Π into three sets. Let Π_1 be the set of $(4,5)$-cycles of S_9, let Π_2 be the set of $(3,6)$-cycles of S_9, and let $\Pi_3 = \Pi \setminus (\Pi_1 \cup \Pi_2)$. We will show that $\sigma(\Pi) \geq \sigma(\Pi_1 \cup \Pi_3) = 172$. There is no subgroup intersecting both Π_1 and Π_3, so we have $\sigma(\Pi_1 \cup \Pi_3) = \sigma(\Pi_1) + \sigma(\Pi_3)$. Since there is exactly one maximal subgroup - a group conjugate to $S_4 \times S_5$ - containing a given $(4,5)$-cycle, we have $\sigma(\Pi_1) = 126$. Now the set $\mathcal{H}$ of subgroups A_9 with all maximal intransitive subgroups of S_9 isomorphic to $S_1 \times S_8$ or $S_2 \times S_7$ is definitely unbeatable on Π_3, since

these subgroups cover Π_3 in a disjoint way, and $|S \cap \Pi_3| \leq 6! \leq |H \cap \Pi_3|$ holds for all subgroups $S \notin \mathcal{H}$, $H \in \mathcal{H}$ of S_9. □

If $n > 2$ is even, then $\sigma(S_n)$ is asymptotically equal to the index of the largest transitive subgroup of S_n, that is to $\frac{1}{2}\binom{n}{n/2}$. However, we prove more than that.

Theorem 5.3.2. *If $n > 2$ is even, then $\sigma(S_n) \sim \frac{1}{2}\binom{n}{n/2}$. More precisely, for any $\epsilon > 0$ there exists N such that if $n > N$, then* t32

$$\frac{1}{2}\binom{n}{n/2} + (\frac{1}{2} - \epsilon)\sum_{i=0}^{[n/3]}\binom{n}{i} < \sigma(S_n) \leq \frac{1}{2}\binom{n}{n/2} + \sum_{i=0}^{[n/3]}\binom{n}{i}.$$

Note that the term $\sum_{i=0}^{[n/3]}\binom{n}{i}$ is considerably smaller than $\frac{1}{2}\binom{n}{n/2}$ for large values of n.

Proof. The set-theoretic union of all maximal imprimitive subgroups conjugate to $S_{n/2}wrS_2$, all maximal intransitive subgroups conjugate to some $S_i \times S_{n-i}$ with $i \leq [n/3]$, and A_n is S_n. This gives

$$\sigma(S_n) \leq \frac{1}{2}\binom{n}{n/2} + \sum_{i=0}^{[n/3]}\binom{n}{i}.$$

Let Π_0 be the set of all n-cycles of S_n. For each $(n-2)/4 < i < [n/3]$ with i odd, let Π_i be the set of all $(i, i+1, n-2i-1)$-cycles of S_n. Moreover, let $\mathcal{H}_0$ be the set of all maximal imprimitive subgroups of S_n conjugate to $S_{n/2}wrS_2$. For each $i > 0$ with Π_i defined above, let $\mathcal{H}_i$ be the set of all maximal intransitive subgroups of S_n conjugate to $S_i \times S_{n-i}$. The following two claims are to show that if n is sufficiently large, then $\mathcal{H}_0$ is definitely unbeatable on Π_0, and for each $i > 0$ the set $\mathcal{H}_i$ is definitely unbeatable on Π_i.

Claim 5.3.3. *With the notations above we have the following.* c33

(i) $\Pi_0 \subseteq \bigcup_{H \in \mathcal{H}_0} H$;

(ii) $\Pi_i \subseteq \bigcup_{H\in\mathcal{H}_i} H$ *for all* $i > 0$*;*

(iii) If H_1, $H_2 \in \mathcal{H}_0$ *and* $H_1 \neq H_2$ *then* $\Pi_0 \cap H_1 \cap H_2 = \emptyset$*;*

(iv) For all i *if* H_1, $H_2 \in \mathcal{H}_i$ *and* $H_1 \neq H_2$, *then* $\Pi_i \cap H_1 \cap H_2 = \emptyset$.

Proof. All statements are checked easily. □

Claim 5.3.4. *Let* $n \geq 14$ *and let* S *be a maximal subgroup of* S_n. *Then* c34

(i) $|S \cap \Pi_0| < |H \cap \Pi_0|$ *for all* $S \notin \mathcal{H}_0$, $H \in \mathcal{H}_0$*;*

(ii) $|S \cap \Pi_i| < |H \cap \Pi_i|$ *for all* i *and all* $S \notin \mathcal{H}_i$, $H \in \mathcal{H}_i$.

Proof.

(i) If S is primitive, then

$$|S \cap \Pi_0| \leq |S| < e^n < \frac{(n/2)!^2 \cdot 2}{n} = |H \cap \Pi_0|$$

follows. If S is imprimitive, then

$$|S \cap \Pi_0| \leq |S| \leq (n/d)!^d \cdot d! < \frac{(n/2)!^2 \cdot 2}{n} = |H \cap \Pi_0|,$$

where d is the smallest divisor of n greater than 2. If S is intransitive, then $S \cap \Pi_0 = \emptyset$.

(ii) Fix an index i. If S is primitive, then

$$|S \cap \Pi_i| \leq |S| < e^n < \frac{([n/3]-2)! \cdot (n-[n/3]+1)!}{[n/3] \cdot (n-2[n/3]+1)} \leq |H \cap \Pi_i|$$

follows. If S is imprimitive, then

$$|S \cap \Pi_i| \leq |S| < (n/d)!^d \cdot d! < \frac{([n/3]-2)! \cdot (n-[n/3]+1)!}{[n/3] \cdot (n-2[n/3]+1)} \leq |H \cap \Pi_i|,$$

where d is the smallest divisor of n greater than 2. Let S be intransitive. If S is contained in a group conjugate to $S_{i+1} \times S_{n-i-1}$, then

$$\frac{|S \cap \Pi_i|}{|H \cap \Pi_i|} = \frac{(i+1)! \cdot (n-i-1)!}{i! \cdot (n-i)!} < 1.$$

If S is contained in a group conjugate to $S_{n-2i-1} \times S_{2i+1}$, then

$$\frac{|S \cap \Pi_i|}{|H \cap \Pi_i|} = \frac{(n-2i-1)! \cdot (2i+1)!}{i! \cdot (n-i)!} = \frac{\binom{n}{i}}{\binom{n}{2i+1}} < 1.$$

Finally, if S is contained neither in a group conjugate to $S_{i+1} \times S_{n-i-1}$, nor in a group conjugate to $S_{n-2i-1} \times S_{2i+1}$, then $S \cap \Pi_i = \emptyset$. □

Now let $\Pi = \Pi_0 \cup \bigcup_i \Pi_i$. Let $\mathcal{H}$ be a set of $\sigma(\Pi)$ maximal subgroups of S_n covering Π.

Claim 5.3.5. *With the notations above, we have $\mathcal{H} = \mathcal{H}_0 \cup \bigcup_i \mathcal{H}_i$ whenever $n \geq 14$.* c35

Proof. Let $\mathcal{H}'$ be the set of all intransitive groups in $\mathcal{H}$ together with all maximal imprimitive subgroups of $\mathcal{H}$ conjugate to $S_{n/2} wr S_2$. For each $S \in \mathcal{H}'$, there exists a unique j such that $S \cap \Pi_j \neq \emptyset$. Moreover, for all i and all $S \in \mathcal{H}'$, $H_i \in \mathcal{H}_i$, we have $|S \cap \Pi_i| \leq |H_i \cap \Pi_i|$. This means that the union of all subgroups in $\mathcal{H}'$ does not contain at least

$$(|\mathcal{H}_0 \cup \bigcup_i \mathcal{H}_i| - |\mathcal{H}'|) \cdot min\{\frac{(n/2)!^2 \cdot 2}{n}, \frac{([n/3]-2)! \cdot (n-[n/3]+1)!}{[n/3] \cdot (n-2[n/3]+1)}\}$$

elements of Π. If this expression is 0, then by Claims 5.3.3 and 5.3.4 we are finished. Otherwise, these elements can be covered by at most $|\mathcal{H}_0 \cup \bigcup_i \mathcal{H}_i| - |\mathcal{H}'|$ transitive groups neither of which is conjugate to $S_{n/2} wr S_2$. But this is impossible since

$$max\{e^n, (n/d)!^d \cdot d!\} < min\{\frac{(n/2)!^2 \cdot 2}{n}, \frac{([n/3]-2)! \cdot (n-[n/3]+1)!}{[n/3] \cdot (n-2[n/3]+1)}\},$$

where d is the smallest divisor of n with d greater than 2. $\square$

The following claim nearly finishes the proof of the theorem.

Claim 5.3.6. *If $n \geq 14$, then*

$$\frac{1}{2}\binom{n}{n/2} + \sum_{\substack{(n-2)/4<i<[n/3] \\ i \text{ odd}}} \binom{n}{i} = \sigma(\Pi) < \sigma(S_n) \leq \frac{1}{2}\binom{n}{n/2} + \sum_{i=0}^{[n/3]} \binom{n}{i}.$$

Proof. The first equality is a consequence of Claim 5.3.5. $\sigma(\Pi) < \sigma(S_n)$ follows from the fact that $\sigma(\Pi) \neq \sigma(S_n)$, since the union of all subgroups of $\mathcal{H}_0 \cup \bigcup_i \mathcal{H}_i$ does not contain all even permutations. The upper bound was already established. $\square$

Finally, we need to show that for any fixed $0 < \epsilon < 1/2$, there exists an integer N, so that

$$(\frac{1}{2} - \epsilon) \sum_{i=0}^{[n/3]} \binom{n}{i} < \sum_{\substack{(n-2)/4<i<[n/3] \\ i \text{ odd}}} \binom{n}{i}$$

holds whenever $n > N$. Indeed, for a fixed real number $0 < \epsilon < 1/2$, a suitable N is an integer with the property that whenever $n > N$, then both

$$\sum_{(n-2)/4<i<[n/3]} \binom{n}{i} \leq (2 + 2\epsilon) \sum_{\substack{(n-2)/4<i<[n/3] \\ i \text{ odd}}} \binom{n}{i}$$

and

$$\sum_{0\leq i\leq(n-2)/4} \binom{n}{i} \leq 2\epsilon \sum_{\substack{(n-2)/4<i<[n/3] \\ i \text{ odd}}} \binom{n}{i}$$

hold. $\square$

By Theorems 5.3.1 and 5.3.2, to complete the proof of part (1) of Theorem 5.1.1,

we only need to show $\sigma(S_n) \leq 2^{n-2}$ for $4 \leq n \leq 12$ and n even, since if $n \geq 14$ we have

$$\frac{1}{2}\binom{n}{n/2} + \sum_{i=0}^{[n/3]} \binom{n}{i} < 2^{n-2}.$$

If $n = 4$, then $\sigma(S_4) \leq 4$, since S_4 is the union of A_4 and the three Sylow 2-subgroups of S_4. For $n = 6$, we have $\sigma(S_6) \leq 16$, since S_6 is the union of all imprimitive subgroups conjugate to $S_3 wr S_2$ and all intransitive subgroups conjugate to $S_1 \times S_5$. If $n = 8$, then S_8 is the union of all imprimitive subgroups conjugate to $S_4 wr S_2$, all intransitive subgroups conjugate to $S_2 \times S_6$ and A_8, hence $\sigma(S_8) \leq 64$. For $n = 10$ we have $\sigma(S_{10}) \leq 256$, since S_{10} is the union of all imprimitive subgroups conjugate to $S_5 wr S_2$, all intransitive subgroups conjugate to $S_1 \times S_9$ and all intransitive subgroups conjugate to $S_3 \times S_7$. Finally, $\sigma(S_{12}) \leq 761$, since S_{12} may be written as the union of all imprimitive subgroups conjugate to $S_6 wr S_2$, all intransitive subgroups conjugate to $S_1 \times S_{11}$, $S_2 \times S_{10}$, or $S_3 \times S_9$, and A_{12}.

5.4 Alternating groups

Theorem 5.4.1. *Let $n > 2$ be even. If n is not divisible by 4, then $\sigma(A_n) = 2^{n-2}$. While if n is divisible by 4, then*

$$\binom{(3n/4)-1}{(n/4)-1} \leq \sigma(A_n) - 2^{n-2} \leq \frac{1}{2}\binom{n}{n/2},$$

that is $\sigma(A_n) \sim 2^{n-2}$.

Proof. The set-theoretic union of all maximal imprimitive subgroups of A_n conjugate to $(S_{n/2} wr S_2) \cap A_n$, and all maximal intransitive subgroups of A_n conjugate to some

$(S_i \times S_{n-i}) \cap A_n$ with $1 \leq i \leq (n/2) - 1$ odd is A_n. This gives

$$\sigma(A_n) \leq \frac{1}{2}\binom{n}{n/2} + \sum_{\substack{i=1 \\ i \text{ odd}}}^{(n/2)-1} \binom{n}{i}.$$

The right-hand-side of the former inequality is equal to 2^{n-2} if n is not divisible by 4, and is $\frac{1}{2}\binom{n}{n/2} + 2^{n-2}$ if n is divisible by 4.

First suppose that n is not divisible by 4. We have $\sigma(A_n) \leq 2^{n-2}$. It is proved below that this estimate is exact. The upper bound is known to be exact for $n = 6$ by [13], so assume that $n \geq 10$. Now let Π be the set of all permutations of A_n which are the product of exactly two disjoint cycles of odd lengths. We will show that the set $\mathcal{H}$ of all maximal imprimitive subgroups of A_n conjugate to $(S_{n/2} wr S_2) \cap A_n$, and all maximal intransitive subgroups of A_n conjugate to some $(S_i \times S_{n-i}) \cap A_n$ with $1 \leq i \leq (n/2) - 1$ odd is definitely unbeatable on Π if $n \geq 10$, that is $\sigma(\Pi) \geq 2^{n-2}$ for $n \geq 10$ and not divisible by 4.

Claim 5.4.1. *Let $\mathcal{H}$ be as above. If $n \geq 10$ is not divisible by 4, then*

(i) $\Pi \subseteq \bigcup_{H \in \mathcal{H}} H$;

(ii) If H_1, $H_2 \in \mathcal{H}$ *and* $H_1 \neq H_2$, *then* $\Pi \cap H_1 \cap H_2 = \emptyset$;

(iii) $|S \cap \Pi| \leq |H \cap \Pi|$ *for all* $S \notin \mathcal{H}$, $H \in \mathcal{H}$.

Proof.

(i) This was established above.

(ii) This is checked easily.

(iii) First suppose that $n \geq 14$. Let $H \cong (S_k \times S_{n-k}) \cap A_n$ for some k, and let d be the smallest divisor of n greater than 2. If S is transitive, then

$$|S \cap \Pi| \leq |S| \leq max\{e^n, \frac{(n/d)!^d \cdot d!}{2}\} \leq (k-1)! \cdot (n-k-1)! = |H \cap \Pi|$$

holds. If S is intransitive, then it is either a subgroup of a subgroup in $\mathcal{H}$, or $S \cap \Pi = \emptyset$. Now let $n = 10$. For any maximal subgroup $S \notin \mathcal{H}$, the set $S \cap \Pi$ is either empty, or it contains only $(5,5)$-cycles. In the latter case, S is either permutation isomorphic to $(S_2 wr S_5) \cap A_{10}$, or is a proper primitive subgroup of A_{10}. There are 96 Sylow 5-subgroups in $(S_2 wr S_5) \cap A_{10}$, and there are at most 36 Sylow 5-subgroups (all of order 5) in a proper primitive subgroup of A_{10}, hence $|S \cap \Pi| \leq 384$. On the other hand, we have $|H \cap \Pi| \geq 576$ whenever $H \in \mathcal{H}$. □

Now let n be divisible by 4. We have $\sigma(A_n) \leq 2^{n-2} + \frac{1}{2}\binom{n}{n/2}$. It is proved below that

$$2^{n-2} + \binom{(3n/4)-1}{(n/4)-1} \leq \sigma(A_n).$$

This bound is certainly sharp for $n = 4$, since $\sigma(A_4) = 5$ by [15]. So assume that $n \geq 8$. Let Π_1 be the set of all permutations of A_n which are the product of exactly two disjoint cycles of odd lengths. Moreover, let Σ be an arbitrary subset of $(n/4)+1$ letters, and let Π_2 be the set of all permutations of A_n which are the product of exactly two disjoint cycles of equal lengths with one cycle moving all letters of Σ. Finally, let $\Pi = \Pi_1 \cup \Pi_2$. We will show that the set $\mathcal{H}$ of all maximal imprimitive subgroups of A_n conjugate to $(S_{n/2} wr S_2) \cap A_n$ and intersecting Π nontrivially, and all maximal intransitive subgroups of A_n conjugate to some $(S_i \times S_{n-i}) \cap A_n$ with $1 \leq i \leq \frac{n}{2} - 1$ odd is definitely unbeatable on Π if n is divisible by 4 and greater than 12. That is $\sigma(\Pi) \geq 2^{n-2} + \binom{(3n/4)-1}{(n/4)-1}$ for n divisible by 4 and greater than 12.

Claim 5.4.2. *If n is divisible by 4, then*

(i) $\Pi \subseteq \bigcup_{H \in \mathcal{H}} H$;

(ii) If H_1, $H_2 \in \mathcal{H}$ *and* $H_1 \neq H_2$, *then* $\Pi \cap H_1 \cap H_2 = \emptyset$;

(iii) If $n \geq 16$, *then* $|S \cap \Pi| \leq |H \cap \Pi|$ *for all* $S \notin \mathcal{H}$, $H \in \mathcal{H}$.

Proof.

(i) This was established above.

(ii) This is checked easily.

(iii) If $n \geq 14$, then the argument of the proof of Claim 5.3.4 may be applied. $\square$

Let $n = 8$. Any $(3, 5)$-cycle is contained in only one maximal subgroup, in a group permutation isomorphic to $(S_3 \times S_5) \cap A_8$. So if $\mathcal{L}$ is a set of $\sigma(A_8)$ maximal subgroups covering A_8, then $\mathcal{L}$ must contain all 56 maximal subgroups permutation isomorphic to $(S_3 \times S_5) \cap A_8$. Now consider a given $(1, 7)$-cycle. This is contained in either a maximal affine permutation group, or in a one-point stabilizer of A_8. It is checked easily that if $\mathcal{L}$ does not contain all of the 15 maximal affine permutation groups, then the $(1, 7)$-cycles can only be covered with all one-point stabilizers. Conversely, it can also be checked that if $\mathcal{L}$ does not contain all the one-point stabilizers, then it must contain all 15 maximal affine subgroups. In the latter case we have $\sigma(A_8) \geq 56+15 > 69$, where 69 is the lower bound for $n = 8$. For the first case, consider a given $(2, 6)$-cycle. This is contained in either a maximal imprimitive group with two or four blocks of imprimitivity, or in a maximal intransitive group permutation isomorphic to $(S_2 \times S_6) \cap A_8$. It can be checked easily that in all of these groups the number of $(2, 6)$-cycles is at most 192, while the number of $(2, 6)$-cycles in A_8 is exactly 3360. This implies that $\sigma(A_8) \geq 56 + 8 + 17 > 69$.

Finally, let $n = 12$. We have to show that $\sigma(A_{12}) \geq 1052$. For $i = 1$, 3, and 5, let Π_i be the set of all $(i, 12-i)$-cycles (of A_{12}), and let $\mathcal{L}_i$ be the set of all maximal intransitive subgroups of A_{12} permutation isomorphic to $(S_i \times S_{12-i}) \cap A_{12}$. It is easy to see that $\mathcal{L}_i$ is definitely unbeatable on Π_i for each i. (Note that a proper primitive subgroup of A_{12} contains no $(3, 9)$- or $(5, 7)$-cycle, and has order at most 95040.) Moreover, all maximal subgroups of A_{12} intersect at most one of the sets Π_i. This means that $\sigma(\Pi) = \binom{12}{1} + \binom{12}{3} + \binom{12}{5} = 1024$ where $\Pi = \Pi_1 \cup \Pi_2 \cup \Pi_3$. Now let $\mathcal{L}$ be a set of $\sigma(A_{12})$ maximal subgroups covering A_{12}. Since no maximal subgroup different from the subgroups in $\mathcal{L}_5$ intersects Π_5, we have $\mathcal{L}_5 \subseteq \mathcal{L}$. We may suppose that $\mathcal{L}_1 \subseteq$

$\mathcal{L}$. For if $\mathcal{L}$ does not contain $k > 0$ subgroups of $\mathcal{L}_1$, then Π is covered by at least $1024 - k + (10! \cdot k)/95040 > 1052$ subgroups. We may also assume that $\mathcal{L}_3 \subseteq \mathcal{L}$. For suppose that $\mathcal{L}$ does not contain a subgroup H of $\mathcal{L}_3$. Then $H \cap \Pi_3$ is covered by subgroups permutation isomorphic to $(S_4 wr S_3) \cap A_{12}$ or $(S_3 wr S_4) \cap A_{12}$. Since such a group can cover at most 288 permutations of $H \cap \Pi_3$, a covering of $H \cap \Pi_3$ must contain at least $(2! \cdot 8!)/288 = 280$ subgroups. Hence $|\mathcal{L}| \geq 1024 - \binom{12}{3} + 280 > 1052$. So we may suppose that all maximal subgroups permutation isomorphic to $(S_i \times S_{12-i}) \cap A_{12}$ are contained in $\mathcal{L}$ for $i = 1$, 3, and 5. Suppose that A_{12} acts on the set $\{1, \ldots, 12\}$. Let Δ be the set of all $(6,6)$-cycles of A_{12} such that the letters 1, 2, 3, and 4 are in the same 6-cycle. The set Δ is the disjoint union of the subgroups of a certain set, $\mathcal{K}$ consisting of $\binom{8}{2}$ maximal subgroups each permutation isomorphic to $(S_6 wr S_2) \cap A_{12}$. We will show that $\mathcal{K}$ is definitely unbeatable on Δ. Indeed, any element of $\mathcal{K}$ covers 14400 permutations of Δ, while an imprimitive maximal subgroup of A_{12} cannot cover more, a primitive group not isomorphic to M_{12} has order less than 14400, and finally, the number of $(6,6)$-cycles contained by the primitive group M_{12} is only 7920. Since no subgroup in $\mathcal{L}_i$ intersects Δ nontrivially when $i = 1$, 3, or 5, we readily see that $\mathcal{L} \geq 1024 + \binom{8}{2} = 1052$. □

Now we turn to the case when n is odd. The possibilities of n being prime and $n = 9$ are treated separately.

Theorem 5.4.2. *If $n > 9$ is odd and not a prime, then* t42

$$h \leq \sigma(A_n) \leq h + \sum_{i=1}^{[n/3]} \binom{n}{i}$$

where h denotes the index of the largest transitive proper subgroup of A_n. In particular, $\sigma(A_n) \sim h$ and $\sigma(A_n) > 2^{n-2}$.

Proof. Let d be the smallest prime divisor of n, and let $\mathcal{L}$ be the set of all maximal imprimitive subgroups of A_n conjugate to $(S_{n/d} wr S_d) \cap A_n$. Notice that $|\mathcal{L}| = h$. All

subgroups permutation isomorphic to $(S_i wr S_{n-i}) \cap A_n$ for some $1 \leq i \leq [n/3]$ together with all subgroups of $\mathcal{L}$ cover A_n. This yields the upper bound for $\sigma(A_n)$. To verify the lower bound, it is sufficient to show that $\mathcal{L}$ is definitely unbeatable on the set Π of all n-cycles of A_n. It is easy to see that the subgroups of $\mathcal{L}$ cover Π disjointly with each group covering exactly h/n different n-cycles. If S is an imprimitive maximal subgroup of A_n of index k intersecting Π nontrivially, then $|S \cap \Pi| \leq k/n \leq h/n$. Finally, if S is a proper primitive subgroup of A_n, then $|S| \leq e^n < h/n$ follows for $n \geq 21$, and we have $|S| < h/n$ for $n = 15$. (Note that intransitive groups intersect Π trivially.) □

Theorem 5.4.3. *Let $n > 3$ be a prime. If n is not equal to 7, then $\sigma(A_n) > 2^{n-2}$, and $\sigma(A_7) \leq 31$.*

Proof. First let $n > 11$. The alternating group, A_n contains $(n-2)!$ Sylow n-subgroups, while a proper transitive subgroup, H of A_n contains at most $|H|/n$. Hence the set of n-cycles of A_n cannot be covered by less than $n!/(|G| \cdot (n-1))$ subgroups where G is a proper transitive group of A_n of largest possible order. It is sufficient to show that $2^{n-2} < n!/(|G| \cdot (n-1))$, that is $|G| < n!/((n-1) \cdot 2^{n-2})$. Since n is prime, G is primitive. For $n > 17$, we have $|G| < e^n < n!/((n-1) \cdot 2^{n-2})$, while if $n = 13$, then $|G| \leq 5616 < 13!/(12 \cdot 2^{11})$ holds. Now let $n = 11$. Then the number of 11-subgroups contained by A_{11} is 9!, while a proper primitive subgroup contains at most 144. Hence a covering of A_{11} has at least $9!/144 > 2^9$ elements. Let $n = 7$. We will show that A_7 can be covered by at most 31 subgroups. Suppose that A_7 acts on the set Ω of size 7. Let $\alpha \in \Omega$. Let $\mathcal{L}$ be the set of all subgroups conjugate to a copy of $PSL(3,2)$, all intransitive subgroups conjugate to $(S_2 \times S_5) \cap A_7$ satisfying the property that the 2-element orbit does not contain α, and the stabilizer of α in A_7. Notice that $|\mathcal{L}| = 31$, and that the subgroups of $\mathcal{L}$ cover all permutations of the group A_7. Finally, if $n = 5$, then $\sigma(A_5) = 10$ by [15]. □

Theorem 5.4.4. *If $p > 23$ is a prime not of the form $(q^k - 1)/(q - 1)$ where q is a*

prime power and k is an integer, then

$$(p-2)! \leq \sigma(A_p) \leq (p-2)! + \sum_{i=1}^{[p/3]} \binom{p}{i}.$$

Proof. By [27], there are only two conjugacy classes of maximal transitive subgroups of A_p. Both conjugacy classes consist of subgroups isomorphic to the unique subgroup of $AGL(1,p)$ of index 2. Let this set, the set of all maximal transitive subgroups of A_p be denoted by $\mathcal{L}$. Since $\mathcal{L}$ is definitely unbeatable on the set of p-cycles and $|\mathcal{L}| = (n-2)!$, the lower bound for $\sigma(A_p)$ follows. The upper bound is a consequence of the proof of Theorem 5.4.2. □

Later, in Lemma 5.7.1, we will show that there are infinitely many primes of this kind, so $(p-2)!$ is actually an asymptotic estimate for $\sigma(A_p)$ for such primes, p.

Now let $n = 9$. Among all transitive subgroups of A_9, the primitive group $P\Gamma L(2,8)$ contains the most 9-cycles; it contains exactly 3024. Since the number of 9-cycles in A_9 is 8!, at least $8!/3024 = 80$ subgroups are needed to cover all 9-cycles. This gives $\sigma(A_9) \geq 80$.

5.5 A Mathieu group

In this section we prove Proposition 5.1.1. We first show that $\sigma(M_{11}) \leq 23$.

Claim 5.5.1. *The Mathieu group, M_{11} is the set-theoretic union of all 11 one-point stabilizers of its action on 11 letters and of all 12 one-point stabilizers of its action on 12 letters. In particular, $\sigma(M_{11}) \leq 23$.* c51

Proof. By [16], the permutation character of the action of M_{11} on 11 letters is $1_{M_{11}} + \chi_2$, and the permutation character of the action of M_{11} on 12 letters is $1_{M_{11}} + \chi_5$ where χ_2, χ_5 are the irreducible characters of M_{11} indicated in the character table of M_{11}

found in [16]. The character table also shows that for arbitrary $g \in M_{11}$ we cannot have $(1_{M_{11}} + \chi_2)(g) = 0$ and $(1_{M_{11}} + \chi_5)(g) = 0$. □

To prove $\sigma(M_{11}) \geq 23$ it is enough to consider only maximal subgroups whose union is M_{11}.

Claim 5.5.2. c52

(i) The only maximal subgroups of M_{11} containing an element of order 11 are the one-point stabilizers of M_{11} on 12 letters.

(ii) Moreover, let $\mathcal{L}$ be a set of maximal subgroups whose union is M_{11}. Then $\mathcal{L}$ contains all the one-point stabilizers of M_{11} of its action on 12 letters. In particular, $\sigma(M_{11}) \geq 12$.

Proof.

(i) Let G be a maximal subgroup of $M_{11} \leq S_{11}$ containing a permutation of order 11. Then G is transitive and so primitive. A primitive permutation group of degree 11 contained in M_{11} is either a one-point stabilizer of M_{11} of its action on 12 letters, or is affine of order 55. Assume that $G \leq M_{11}$ is affine of order 55 generated by the elements g_1 and g_2 of order 5 and 11, respectively. Represent M_{11} on 12 points. Now $G \leq M_{11} \leq S_{12}$ must be intransitive, since $12 \nmid 55$. This can only be if g_1 and g_2 fixes the same point. Thus G is contained in a one-point stabilizer of $M_{11} \leq S_{12}$.

(ii) Represent M_{11} on 12 letters. For any letter α, there exists a permutation g of M_{11} of order 11 fixing α. By (i), the only maximal subgroup of M_{11} containing g is the one-point stabilizer of α. □

We recall the following fact from [16].

Claim 5.5.3. *A maximal subgroup of M_{11} different from a one-point stabilizer of M_{11} of its action on 11 letters and different from a one-point stabilizer of M_{11} of its action on 12 letters has order at most 144.* c53

By the character table of M_{11} in [16], we see that the set Π of group elements g satisfying $(1_{M_{11}} + \chi_2)(g) = 1$ and $(1_{M_{11}} + \chi_5)(g) = 0$ is exactly the set of 1980 elements of order 8 in M_{11}. By Claim 5.5.3, the set of 11 copies of M_{10} is definitely unbeatable on Π. This, together with Claim 5.5.2, implies $\sigma(M_{11}) \geq 23$. By Claim 5.5.1, we now obtain $\sigma(M_{11}) = 23$ which proves Proposition 5.1.1.

5.6 On some infinite series of σ

We start with a theorem which was conjectured by Ramanujan in 1913 and was confirmed by Nagell [53] in 1960.

Theorem 5.6.1 (Nagell, [53]). *The only solutions to the Diophantine equation* $x^2+7 = 2^n$ *are* $(n, x) = (3, 1)$, $(4, 3)$, $(5, 5)$, $(7, 11)$ *and* $(15, 181)$. t61

This is used to prove

Theorem 5.6.2. *Any positive integer is a member of at most one of the following infinite series.*

(1) $\mathcal{A} = \{2^n\}_{n=5}^{\infty}$;

(2) $\mathcal{B}_p = \{\frac{1}{2}p^n(p^n + 1) + 1\}_{n=1}^{\infty}$ *where* p *is an odd prime;*

(3) $\mathcal{C} = \{\frac{1}{2}2^n(2^n + 1)\}_{n=2}^{\infty}$.

Proof. Suppose that $2^n = \frac{1}{2}p^k(p^k + 1) + 1$ where $n \geq 5$, $k \geq 1$ and p is an odd prime. After multiplying both sides of the equation by 8, we obtain $2^{n+3} = (2p^k + 1)^2 + 7$. By Theorem 5.6.1, we get a contradiction. Suppose that $2^n = 2^{k-1}(2^k + 1)$ where $n \geq 5$ and $k \geq 2$. Notice that the right-hand-side of this equation is divisible by an odd prime, while the left-hand-side is not. Finally, no positive integer is an element of both $\mathcal{B}_p$ and $\mathcal{C}$ for any odd prime p, since the function $\frac{1}{2}x(x+1)$ is strictly increasing on the set of positive integers by a difference of at least 2 whenever $x > 2$. □

5.7 An application

We will show that $\alpha'_n = \beta'_n$ for n a prime greater than 23 and not of the form $(q^k - 1)/(q - 1)$ where q is a prime power and k is an integer. But before we do this, we prove

Lemma 5.7.1. *The set of primes not of the form $(q^k - 1)/(q - 1)$ where q is a prime power and k is an integer has density 1 in the set of all primes.* 171

Proof. The Prime Number Theorem states that there are asymptotically $x/\ln x$ primes less than x. Now let us count the primes less than x which are of the form $(q^k-1)/(q-1)$ for some prime power q and some positive integer k. If $k = 2$, then q has to be a power of 2, and so there are at most $\log_2 x$ such primes. For each $k \geq 3$, there are at most $\sqrt{x}$ such primes. Since k cannot exceed $\log_2 x$, there are at most $(\sqrt{x} + 1)\log_2 x$ such primes in total. We conclude that the sequence

$$\frac{x/\ln x - (\sqrt{x} + 1)\log_2 x}{x/\ln x}$$

tends to 1 as x goes to infinity. □

Now we turn to the proof of Theorem 5.1.2. Let p be a prime greater than 23 and satisfying the condition of Lemma 5.7.1. By part (1) of Theorem 5.1.1, we see that $2^{p-1} = \sigma(S_p) \geq \beta'_p \geq \alpha'_p$. Hence it is sufficient to show that $2^{p-1} \leq \alpha'_p$. Suppose that S_p is acting naturally on a set Ω of size p. For each $1 < i \leq (p-1)/2$ and each subset of Ω of size i, say Δ, choose an $(i, p-i)$-cycle of S_p such that all elements of Δ are moved by the cycle of length i. Let the set of all permutations so obtained be Π_0. Now choose an arbitrary n-cycle, say g. This permutation is contained in a unique copy of $AGL(1, p)$, say in G. Since any $(1, p-1)$-cycle is contained in at most $\varphi(p-1) \cdot p(p-1)$ distinct copies of $AGL(1, p)$ where $\varphi(p-1)$ denotes the Euler function of the integer $p-1$, and since $(p-2)! - 1 > \varphi(p-1) \cdot p^2(p-1)$, it follows that for each $\omega \in \Omega$ we may choose

a $(1, p-1)$-cycle, g_ω fixing ω and not contained in G such that if $\omega \neq \omega'$ are distinct elements of Ω, then there is no subgroup of S_p isomorphic to $AGL(1,p)$ containing both g_ω and $g_{\omega'}$. Now let Π be the set consisting of all elements of Π_0 together with g and all g_ω with $\omega \in \Omega$. Notice that $|\Pi| = 2^{p-1}$. Now it is easy to see that any two distinct permutations of Π generate a transitive subgroup of S_p contained neither in A_p nor in any conjugate of $AGL(1,p)$. So by [27], it follows that any two distinct elements of Π generate S_p. Hence we have $2^{p-1} \leq \alpha'_p$, which completes the proof of Theorem 5.1.2.

Chapter 6

Summary

In Chapter 3 we considered the problem of bounding the order of a primitive permutation group of degree n so that the group does not contain the alternating group of degree n. In our estimates we used the Aschbacher-O'Nan-Scott theorem together with the classification theorem for finite simple groups. We found that "almost all" primitive permutation groups of degree n have order at most $n \cdot \prod_{i=0}^{[\log_2 n]-1}(n-2^i) < n^{1+[\log_2 n]}$, or have socle isomorphic to a direct power of some alternating group. The Mathieu groups in their 4-transitive action, M_{11}, M_{12}, M_{23} and M_{24} are the four exceptions. As a corollary the sharp version of a theorem of Praeger and Saxl was established, where M_{12} turned out to be the "largest" primitive group. In particular, we found that if G is a primitive permutation group of degree n not containing the alternating group of degree n, then $|G|$ is at most $|M_{12}|^{n/12}$. For an application a bound on the orders of permutation groups without large alternating composition factors was given. In particular, we found that if G is a permutation group of degree n, and d is an integer not less than 4, then $|G| \leq d!^{(n-1)/(d-1)}$ whenever G is a group with no composition factor isomorphic to an alternating group of degree greater than d. This sharpened a lemma of Babai, Cameron, Pálfy and generalized a theorem of Dixon. Let G be a primitive subgroup of S_n. We established the inequality $|G| \leq 50 \cdot n^{\sqrt{n}}$ for groups G not containing A_n. This result was applied by J. Araújo, L. Folgado, and J. D. Mitchell

[1] in classifying certain subsemigroups of the semigroup Self(n) of all mappings from an n-element set to itself.

For a finite group G, let $k(G)$ denote the number of conjugacy classes of G. This is also the number of complex irreducible characters of the group G. This invariant is interesting both in group theoretic and representation theoretic points of view. Let V be a finite dimensional FG-module where F is a field of prime order over which the vector space V is defined. The module V (with its additive structure) can be considered as a finite group. We can also consider the semidirect product GV. The so-called $k(GV)$-problem is the following. If G has order co-prime to the order of F, then $k(GV) \leq |V|$. Bounding the number of conjugacy classes of a permutation group is important in this context. In Chapter 4 we proved that if G is a finite permutation group of degree $n > 2$, then $k(G) \leq 3^{(n-1)/2}$. This is an extension of a theorem of Kovács and Robinson and in turn of Riese and Schmid. More distantly but still related to the $k(GV)$-problem, the following is also true. If N is a normal subgroup of a completely reducible subgroup of $GL(n, q)$, then $k(N) \leq q^{5n}$. (Here we note that a normal subgroup of a completely reducible subgroup is again completely reducible.) Similarly, if N is a normal subgroup of a primitive subgroup of S_n, then we found that $k(N) \leq p(n)$ where $p(n)$ is the number of partitions of n. These improve results of Liebeck and Pyber. We proved two more results in Chapter 4 that are worth mentioning here. These are the following. If G is a subgroup of S_n with no composition factor isomorphic to C_2, then $k(G) \leq (5/3)^n$. If G is a nilpotent subgroup of S_n, then $k(G) \leq 1.52^n$. The main result of Chapter 4 (involving the bound $(\sqrt{3})^{n-1}$) was used in a paper by Guralnick and Robinson [30] on the commuting probability of a finite group. These results will also be used in a joint paper of the author and Guralnick [28] on the non–coprime $k(GV)$-problem which is to give an upper bound for $k(GV)$ where V and G are as in the hypotheses of the $k(GV)$-problem with the exception that $|F|$ and $|G|$ need not be co-prime but G is completely reducible on V.

Let G be a group that is a set-theoretic union of finitely many proper subgroups. Cohn defined $\sigma(G)$ to be the least integer m such that G is the union of m proper subgroups. Tomkinson showed that $\sigma(G)$ can never be 7, and that it is always of the form $q+1$ (q a prime power) for solvable groups G. In Chapter 5 we gave exact or asymptotic formulas for $\sigma(S_n)$ where S_n is the symmetric group of degree n. In particular, we showed that $\sigma(S_n) = 2^{n-1}$ if n is odd unless possibly if $n = 9$. When n is even the situation is more complicated. In this case we established the fact that for any $\epsilon > 0$ there exists an integer N so that if n is an integer larger than N, then

$$\frac{1}{2}\binom{n}{n/2} + (\frac{1}{2} - \epsilon)\sum_{i=0}^{[n/3]}\binom{n}{i} < \sigma(S_n) \leq \frac{1}{2}\binom{n}{n/2} + \sum_{i=0}^{[n/3]}\binom{n}{i}.$$

We also investigated the subgroup coverings of the alternating groups. In this case the n even case seemed easier to deal with. We proved that if $n > 2$ is even, then $\sigma(A_n) = 2^{n-2}$ if n is not divisible by 4, while if n is divisible by 4, then

$$\binom{(3n/4)-1}{(n/4)-1}\sigma(A_n) - 2^{n-2} \leq \frac{1}{2}\binom{n}{n/2}.$$

If $n > 9$ is odd and not a prime, then

$$h \leq \sigma(A_n) \leq h + \sum_{i=1}^{[n/3]}\binom{n}{i},$$

where h denotes the index of the largest transitive proper subgroup of A_n. Finally, if n is prime and larger than 7, then we only showed that $\sigma(A_n) > 2^{n-2}$. In Chapter 5 we essentially started the investigation of the function μ. Let G be a 2-generated finite group. Let $\mu(G)$ be the largest integer m so that there exists a subset X of G of order m such that any distinct pair of elements of X generates G. In Chapter 5 we showed that for "most" primes n we have $\sigma(S_n) = \mu(S_n)$. In a beautiful paper Blackburn [7] proved that $\sigma(S_n) = \mu(S_n)$ for almost all odd integers n. In the same paper Blackburn

asked whether is it true that the quotients $\sigma(G)/\mu(G)$ tend to 1 as $|G|$ tends to infinity for any infinite sequence of finite simple groups. The paper [9] is the first step in this direction. We proved two theorems. Let n be a positive integer, q a prime power and V the n-dimensional vector space over the field of q elements. Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. Let b be the smallest prime factor of n, and let $N(b)$ be the number of proper subspaces of V of dimensions not divisible by b. If $n \geq 12$, then

$$\mu(G) = \frac{1}{b}\prod_{\substack{i=1 \\ b\nmid i}}^{n-1}(q^n - q^i) + [N(b)/2].$$

Secondly, let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. Let b be the smallest prime factor of n, let $\binom{n}{k}_q$ be the number of k-dimensional subspaces of the n-dimensional vector space V, and let $N(b)$ be the number of proper subspaces of V of dimensions not divisible by b. Suppose that $n \geq 12$. Then if $n \not\equiv 2 \pmod 4$, or if $n \equiv 2 \pmod 4$, q odd and $G = (P)SL(n,q)$, then

$$\sigma(G) = \mu(G) = \frac{1}{b}\prod_{\substack{i=1 \\ b\nmid i}}^{n-1}(q^n - q^i) + [N(b)/2].$$

Otherwise $\sigma(G) \neq \mu(G)$ and

$$\sigma(G) = \frac{1}{2}\prod_{\substack{i=1 \\ 2\nmid i}}^{n-1}(q^n - q^i) + \sum_{\substack{k=1 \\ 2\nmid k}}^{(n/2)-1}\binom{n}{k}_q + \frac{q^{n/2}}{q^{n/2}+1}\binom{n}{n/2}_q + \epsilon$$

where $\epsilon = 0$ if q is even and $\epsilon = 1$ if q is odd.

Chapter 7

Összefoglaló

A 3. fejezetben az olyan n-ed fokú primitív permutáció csoportok elemszámait becsüljük, amelyek nem tartalmazzák az n-ed fokú alternáló csoportot. A becsléseinkben az Aschbacher-O'Nan-Scott és a véges egyszerű csoportok klasszifikációs tételeit használtuk fel. "Majdnem minden" n-ed fokú primitív permutáció csoport rendje legfeljebb $n \cdot \prod_{i=0}^{[\log_2 n]-1}(n-2^i) < n^{1+[\log_2 n]}$, vagy olyan talppal rendelkezik, amely izomorf valamely alternáló csoport direkt hatványával. A négy, 4-tranzitív Mathieu csoport, M_{11}, M_{12}, M_{23} és M_{24} az egyedüli kivételek. Következményként a Praeger-Saxl tétel egy erősebb verzióját mondtuk ki, ahol az M_{12} csoport "lett" a legnagyobb elemszámú kivétel. Egészen pontosan azt bizonyítottuk, hogy ha G egy n-ed fokú primitív permutáció csoport, amely nem tartalmazza az n-ed fokú alternáló csoportot, akkor $|G|$ legfeljebb $|M_{12}|^{n/12}$. Alkalmazásként egy korlátot adtunk az olyan permutáció csoportok rendjeire, amelyek nem tartalmaztak nagy fokú alternáló csoportot mint kompozíciófaktort. Pontosabban azt igazoltuk, hogy ha G egy n-ed fokú permutáció csoport, d egy olyan egész szám, amely 4-nél nem kisebb, akkor $|G| \leq d!^{(n-1)/(d-1)}$ ha G-nek nincsen d-nél nagyobb fokú alternáló kompozíció faktora. Ez a tétel Babai, Cameron, Pálfy egy lemmáját erősítette és Dixon egy tételét általánosította. Legyen G egy primitív részcsoportja S_n-nek, amely nem tartalmazza A_n-et. Ekkor a következő egyenlőtlenséget igazoltuk. $|G| \leq 50 \cdot n^{\sqrt{n}}$. Ezt az eredményt J. Araújo, L. Folgado,

és J. D. Mitchell [1] felhasználták a Self(n) félcsoport bizonyos részfélcsoportjainak klasszifikációjára.

Egy véges G csoport esetén jelölje $k(G)$ a G csoport konjugáltsági osztályainak számát. Ez a szám egyenlő a csoport komplex karaktereinek számával is. Egy csoport ezen invariánsa érdekes mind csoportelméleti, mind reprezentáció elméleti szemszögből. Legyen V egy F test feletti véges dimenziós vektor tér. Legyen F egy prímtest. Ha G egy véges csoport, akkor V-t tekinthetjük egy FG-modulusnak bizonyos feltételek teljesülése esetén. V, mint modulus tekinthető additív csoportnak is, amelyen G hat. Így definiálhatjuk a GV szemidirekt szorzatot. A $k(GV)$ probléma a következő. Ha $|F|$ nem osztja $|G|$-t, akkor $k(GV) \leq |V|$. Egy tetszőleges permutáció csoport konjugáltsági osztályainak a számának megbecslése ebből a szempontból különösen is érdekes. A 4. fejezetben bizonyítottuk, hogy ha G egy n-ed fokú permutáció csoport és $n > 2$, akkor $k(G) \leq 3^{(n-1)/2}$. Ez Kovács és Robinson, valamint Riese és Schmid egy tételeinek kiterjesztése. A következő állítás szintén igaz. Ha N egy normális részcsoportja a $GL(n, q)$ egy teljesen reducibilis részcsoportjának, akkor $k(N) \leq q^{5n}$. (Itt megjegyezzük, hogy egy teljesen reducibilis csoport normális részcsoportja is teljesen reducibilis.) Hasonlóképpen, ha N az S_n egy primitív részcsoportjának normális részcsoportja, akkor $k(N) \leq p(n)$, ahol $p(n)$ az n szám összes partíciójának száma. Ez Liebeck és Pyber egy eredményét javítotja. Két másik említésre méltó tételt bizonyítottunk be a 4. fejezetben. Ezek a következők. Ha G az S_n egy olyan részcsoportja, amelynek nincsen C_2-vel izomorf kompozíciófaktora, akkor $k(G) \leq (5/3)^n$. Ha G egy nilpotens részcsoportja S_n-nek, akkor $k(G) \leq 1.52^n$. A 4. fejezet fő eredményét, amely a $(\sqrt{3})^{n-1}$ korlátot foglalta magába, Guralnick és Robinson [30] alkalmazta a felcserélhetőségi valószínűségről szóló cikkükben. Ezen kívül ezt az eredményt a szerző egy, a Guralnickkal közös cikkében fogja alkalmazni, amely a nem relatív prím $k(GV)$ problémáról szól, amely egészen pontosan az, mint az eredeti $k(GV)$ problema azzal a kulonbseggel, hogy $|F|$ oszthatja $|G|$-t, viszont G-nek teljesen reducibilisnek kell lennie V-n.

Legyen G egy olyan csoport, amely véges sok valódi részcsoportjának halmazelméleti uniójaként áll elő. Cohn $\sigma(G)$-vel jelölte azt a legkisebb m pozitív egész számot, amelyre az igaz, hogy G előáll m darab valódi részcsoport uniójaként. Tomkinson azt bizonyította, hogy nincs olyan G csoport, amelyre $\sigma(G) = 7$, valamint azt, hogy $\sigma(G)$ mindig $q+1$ alakú ahol q prímhatvány, ha G feloldható. Az 5. fejezetben pontos vagy aszimptotikus formulakat adunk $\sigma(S_n)$-re, ahol S_n az n-ed fokú szimmetrikus csoportot jelöli. Pontosabban, beláttuk, hogy $\sigma(S_n) = 2^{n-1}$ ha n páratlan és 9-től különböző. Ha n páros, akkor a helyzet sokkal komplikáltabb. Ebben az esetben azt bizonyítottuk, hogy bármely pozitív ϵ-ra létezik egy olyan N szám, hogy ha n egy olyan pozitív szám, amely nagyobb, mint N, akkor

$$\frac{1}{2}\binom{n}{n/2} + (\frac{1}{2} - \epsilon)\sum_{i=0}^{[n/3]}\binom{n}{i} < \sigma(S_n) \leq \frac{1}{2}\binom{n}{n/2} + \sum_{i=0}^{[n/3]}\binom{n}{i}$$

teljesül. Az alternaló csoportok részcsoportokkal való lefedésének kérdését is vizsgáltuk. Ebben az esetben a páros n esete könnyebbnek bizonyult. Beláttuk, hogy ha n páros és 2-nél nagyobb, akkor $\sigma(A_n) = 2^{n-2}$ ha n 4-gyel nem osztható, de ha n osztható 4-gyel, akkor

$$\binom{(3n/4)-1}{(n/4)-1}\sigma(A_n) - 2^{n-2} \leq \frac{1}{2}\binom{n}{n/2}.$$

Ha n paratlan, 9-nel nagyobb, es nem prim, akkor

$$h \leq \sigma(A_n) \leq h + \sum_{i=1}^{[n/3]}\binom{n}{i},$$

ahol h jelöli az A_n legnagyobb valódi tranzitív részcsoportjának rendjét. Végül, ha n prím és 7-nél nagyobb, akkor csak azt bizonyítottuk (ilyen általánosságban), hogy $\sigma(A_n) > 2^{n-2}$. Lényegében az 5. fejezetben kezdtük el a μ függvény vizsgálatát. Legyen G egy két elemmel generálható véges csoport. Legyen $\mu(G)$ a legnagyobb olyan m szám, amelyre létezik olyan X részhalmaza G-nek, amelynek rendje m és amelyre igaz az,

hogy bármely két egymastól különböző eleme generálja G-t. Az 5. fejezetben beláttuk, hogy "a legtöbb" n prímre $\sigma(S_n) = \mu(S_n)$. Egy nagyon szép cikkben Blackburn [7] bebizonyította, hogy $\sigma(S_n) = \mu(S_n)$ majdnem minden páratlan n-re. Ugyanebben a cikkben Blackburn megkérdezte, hogy vajon igaz-e az, hogy bármely, véges egyszerű G csoportokból álló végtelen sorozat esetén a $\sigma(G)/\mu(G)$ hányadosok 1-hez tartanak, ha a G csoportok $|G|$ rendjei a végtelenbe tartanak. A [9] cikk az elso lépés ennek a kérdésnek a megválaszolásához. Két tételt bizonyítottunk ebben a cikkben. Legyen n egy pozitív egész szám, q egy prímhatvány, és V egy n dimenziós vektortér a q-elemű test felett. Legyen G a $(P)GL(n,q)$, $(P)SL(n,q)$ csoportok bármelyike. Legyen b az n szám legkisebb prím osztója, és legyen $N(b)$ a V b-vel nem osztható dimenziójú valódi altereinek a száma. Ha $n \geq 12$, akkor

$$\mu(G) = \frac{1}{b}\prod_{\substack{i=1 \\ b\nmid i}}^{n-1}(q^n - q^i) + [N(b)/2].$$

A második tétel pedig a következő. Legyen G a $(P)GL(n,q)$, $(P)SL(n,q)$ csoportok bármelyike. Legyen b az n szám legkisebb prím osztója, és legyen $\binom{n}{k}_q$ a V vektortér k-dimenziós altereinek a száma. Legyen $N(b)$ az, ami az előbb. Legyen $n \geq 12$. Ekkor ha $n \not\equiv 2 \pmod 4$, vagy ha $n \equiv 2 \pmod 4$, q páratlan és $G = (P)SL(n,q)$, akkor

$$\sigma(G) = \mu(G) = \frac{1}{b}\prod_{\substack{i=1 \\ b\nmid i}}^{n-1}(q^n - q^i) + [N(b)/2].$$

Ellenkező esetben, $\sigma(G) \neq \mu(G)$ és

$$\sigma(G) = \frac{1}{2}\prod_{\substack{i=1 \\ 2\nmid i}}^{n-1}(q^n - q^i) + \sum_{\substack{k=1 \\ 2\nmid k}}^{(n/2)-1}\binom{n}{k}_q + \frac{q^{n/2}}{q^{n/2}+1}\binom{n}{n/2}_q + \epsilon$$

ahol $\epsilon = 0$ ha q páros és $\epsilon = 1$ ha q páratlan.

Bibliography

[1] Araújo, J.; Folgado, L.; Mitchell, J. D. A classification of permutation groups that define idempotent generated semigroups. Submitted for publication.

[2] Arregi, J. M.; Vera-Lopez, A. Conjugacy classes in Sylow p-subgroups of $GL(n, q)$. *J. Algebra* **152** (1992), 1–19.

[3] Babai, L. On the orders of uniprimitive permutation groups. *Ann. of Math.* **113**, (1981), 553-568.

[4] Babai, L. On the order of doubly transitive permutation groups. *Invent. Math.* **65**, (1981/82), no. 3, 473–484.

[5] Babai, L.; Cameron, P. J; Pálfy, P. P. On the order of primitive groups with restricted nonabelian composition factors. *J. Algebra* **79**, (1982), 161-168.

[6] Bereczky, Á.; Maróti, A. On solvable semiprimitive groups. Submitted to *J. Algebra.*

[7] Blackburn, S. Sets of elements that generates the symmetric group pairwise. *J. Combinatorial Theory Ser. A.*

[8] Bochert, A. Über die Transitivitätsgrenze der Substitutionengruppen, welche die Alternierende ihres Grades nicht einhalten. *Math. Ann.* **33**, (1889), 572-583.

[9] Britnell, J. R.; Evseev, A.; Guralnick, R. M.; Holmes, P. E.; Maróti, A. Sets of elements that pairwise generate a linear group. To appear in the *Journal of Combinatorial Theory Ser. A.*

[10] Brown, R. Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements. *J. Combin. Theory Ser. A* **49**, (1988), no. 2, 294-307.

[11] Brown, R. Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements. II. *J. Combin. Theory Ser. A* **56**, (1991), no. 2, 285-289.

[12] Bruckheimer, M; Bryan, A. C; Muir, A. Groups which are the union of three subgroups. *Amer. Math. Monthly* **77**, (1970), 52-57.

[13] Bryce, R. A; Fedri, V; Serena, L. Subgroup coverings of some linear groups. *Bull. Austral Math. Soc.* **60**, (1999), no. 2, 227-238.

[14] Cameron, P. J. Finite permutation groups and finite simple groups. *Bull. London Math. Soc.* **13**, (1981), 1-22.

[15] Cohn, J. H. E. On n-sum groups. *Math. Scand.* **75**, (1994), no. 1, 44-58.

[16] Conway, J. H; Curtis, R. T; Norton, S. P; Parker, R. A; Wilson, R. A. Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. *Oxford University Press*, Eynsham, (1985).

[17] Diamond, H. Elementary methods in the study of the distribution of prime numbers. *Bull. Amer. Math. Soc. (N. S.)* **7**, (1982), no. 3., 553-589.

[18] Dixon, J. D. The Fitting subgroup of a linear solvable group. *J. Austral. Math. Soc.* **7**, (1967), 417-424.

[19] Dixon, J. D.; Mortimer, B. The primitive permutation groups of degree less than 1000. *Math. Proc. Camb. Phil. Soc.* **103**, (1988), 213-237.

[20] Dixon, J. D.; Mortimer, B. Permutation groups. *Springer-Verlag, New York* 1996.

[21] Erdős, P. On an elementary proof of some asymptotic formulas in the theory of partitions. *Ann. of Math.* (2) **43** (1942), 437–450.

[22] Erdős, P; Straus, E. G. How abelian is a finite group? *Linear and Multilinear Algebra* **3**, (1975/76), no. 4, 307-312.

[23] Fulman, J.; Guralnick, R. Derangements in simple and primitive groups. *Groups, combinatorics, geometry* (Durham, 2001), 99–121.

[24] Gallagher, P. X. The number of conjugacy classes in a finite group. *Math. Z.* **118** (1970), 175–179.

[25] Gorenstein, D. Finite groups. Second edition. Chelsea Publishing Co., New York, 1980.

[26] The GAP Group, GAP — Groups, Algorithms, Programming, Version 4.2; Aachen, St Andrews, (1999). (http://www-gap.dcs.st-and.ac.uk/gap).

[27] Guralnick, R. M. Subgroups of prime power index in a simple group. *J. Algebra* **81**, (1983), 304-311.

[28] Guralnick, R. M.; Maróti, A. The non-coprime k(GV)-problem for primitive linear groups. In preparation.

[29] Guralnick, R. M.; Pyber, L. Normalizers of primitive permutation groups, in preparation.

[30] Guralnick, R. M.; Robinson, R. G. On the commuting probability of a finite groups. *J. Algebra*.

[31] Haber, S; Rosenfeld, A. Groups as unions of proper subgroups. *Amer. Math. Monthly* **66**, (1959), 491-494.

[32] Holmes, P. E. Subgroup coverings of some sporadic groups, preprint.

[33] Holmes, P. E.; Maróti, A. Pairwise generation of sporadic simple groups. Submitted to *J. Algebra*.

[34] Holt, D. F.; Walton, J. Representing the quotient groups of a finite permutation group. *J. Algebra* **248**, (2002), 307-333.

[35] Jungnickel, D; Storme, L. Packing and covering groups with subgroups. *J. Algebra* **239**, (2001), no. 1, 191-214.

[36] Kleidman, P. B.; Wales, D. B. The projective characters of the symmetric groups that remain irreducible on subgroups. *J. Algebra* **138**, (1991), no. 2, 440–478.

[37] Kleidman, P. B.; Liebeck, M. W. The subgoup structure of the finite classical groups. *London Math. Soc. Lecture Notes, Cambridge Univ. Press* **129**, (1990).

[38] Kovács, L. G.; Robinson, G. R. On the number of conjugacy classes of a finite group. *J. Algebra* **160** (1993), no. 2, 441–460.

[39] Liebeck, M. W. On minimal degrees and base sizes of primitive permutation groups. *Arch. Math.* **43**, (1984), 11-15.

[40] Liebeck, M. W. On the orders of maximal subgroups of the finite classical groups. *Proc. London Math. Soc.* (3) **50** (1985), no. 3, 426–446.

[41] Liebeck, M. W.; Praeger, C. E.; Saxl, J. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. (Ser. A)* **44**, (1988), 389–396.

[42] Liebeck, M. W.; Pyber, L. Upper bounds for the number of conjugacy classes of a finite group. *J. Algebra* **198**, (1997), no. 2, 538–562.

[43] Lubotzky, A.; Segal, D. Subgroup growth, to appear in *Progress in Mathematics, Birkhäuser.*

[44] Lucido, M. S. On the covers of finite groups. *Groups St. Andrews 2001* Vol. II, 395-399, London Math. Soc. Lecture Note Ser., **305**, Cambridge Univ. Press, Cambridge, 2003.

[45] Maróti, A. On the orders of primitive groups. *J. Algebra* **258** (2002), no. 2, 631-640.

[46] Maróti, A. On elementary lower bounds for the partition function. *Integers: Electronic Journal of Combinatorial Number Theory* **3**, (2003). (http://www.integers-ejcnt.org/vol3.html).

[47] Maróti, A. Covering the symmetric groups with proper subgroups. *Journal of Combinatorial Theory Ser. A* **110** (2005), no. 1, 97111.

[48] Maróti, A. Bounding the number of conjugacy classes of a permutation group. *Journal of Group Theory* **8** (2005), no. 3, 273289.

[49] Maróti, A. On generalized blocks for alternating groups. *Journal of Algebra* **297** (2006), no. 2, 400408.

[50] Maróti, A. A proof of a generalized Nakayama conjecture. *Bulletin of the London Mathematical Society* **35** (2006), no. 5, 777785.

[51] Maróti, A. Symmetric functions, generalized blocks, and permutations with restricted cycle structure. *European Journal of Combinatorics* **28** (2007), no. 3, 942963.

[52] Mason, D. R. On coverings of a finite group by abelian subgroups. *Math. Proc. Cambridge Philos. Soc.* **83**, (1978), no. 2, 205-209.

[53] Nagell, T. The Diophantine equation $x^2 + 7 = 2^n$. *Ark. Math.* **4**, (1960), 185-187.

[54] Neumann, B. H. Groups covered by finitely many cosets. *Publ. Math. Debrecen* **3**, (1954), 227-242.

[55] Neumann, B. H. Groups covered by permutable subsets. *J. London Math. Soc.* **29**, (1954), 236-248.

[56] Pálfy, P. P.; Szalay, M. On a problem of P. Turán concerning Sylow subgroups. *Studies in pure mathematics*, 531–542, Birkhäuser, Basel, (1983).

[57] Praeger, C.; Saxl, J. On the order of primitive permutation groups. *Bull. London Math. Soc.* **12**, (1980), 303-308.

[58] Pyber, L. The number of pairwise noncommuting elements and the index of the centre in a finite group. *J. London Math. Soc. (2)* **35**, (1987), no. 2, 287-295.

[59] Pyber, L. Finite groups have many conjugacy classes. J. *London Math. Soc.* (2) **46** (1992), no. 2, 239–249.

[60] Pyber, L. On the orders of doubly transitive permutation groups, elementary estimates. *J. Comb. Theory (A)* **62**, (1993), 361-366.

[61] Pyber, L. Asymptotic results for permutation groups. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science* **11**, (1993), 197-219.

[62] Pyber, L. How abelian is a finite group? The mathematics of Paul Erdős, I, 372-384, *Algorithms Combin.* **13**, Springer, Berlin, 1997.

[63] Riese, U.; Schmid, P. Real vectors for linear groups and the $k(GV)$-problem. *J. Algebra* textbf267 (2003), 725–755.

[64] Scorza, G. I gruppi che possono pensarsi come somma di tre loro sottogruppi. *Boll. Un. Mat. Ital.* **5**, (1926), 216-218.

[65] Serena, L. On finite covers of groups by subgroups. *Advances in group theory* 2002, 173–190, Aracne, Rome, 2003.

[66] Suprunenko, D. A. Matrix groups. *Translations of Mathematical Monographs*, Vol. **45** American Mathematical Society, Providence, R.I., (1976).

[67] Tomkinson, M. J. Groups as the union of proper subgroups. *Math. Scand.* **81**, (1997), 191-198.

[68] van Lint, J. H. Combinatorial Theory Seminar, *Lecture Notes in Mathematics*, Vol. **382** *Springer-Verlag*, Berlin-New York, (1974).

[69] Wielandt, H. Finite Permutation groups. *Acad. Press, New York*, 1964.

[70] Wielandt, H. Permutation groups through invariant relations and invariant functions. *Lecture Notes, Ohio State University, Columbus, Ohio*, 1969.

[71] Wolf, T. R. Solvable and nilpotent subgroups of $GL(n, q^m)$. *Canad. J. Math.* **34** (1982), no. 5, 1097–1111.