On The Orders of Primitive Groups

Attila Maróti *

School of Mathematics and Statistics, University of Birmingham
Birmingham B15 2TT, England

21th of February 2002

Abstract

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, 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 is established, where M_{12} turns out to be the "largest" primitive group. For an application a bound on the orders of permutation groups without large alternating composition factors is given. This sharpens a lemma of Babai, Cameron, Pálfy and generalizes a theorem of Dixon.

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 [4] (see also [9] or [19]): 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 [20] of bounding the orders of Sylow subgroups Praeger and Saxl [16] 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 [1] 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

*On leave from University of Szeged, Hungary; research partially supported by the Hungarian National Foundation for Scientific Research Grant TO34878.

$n^{32\log^2 n}$ bound for $n > 400$ in [17] by an elementary argument (using some ideas of [2]). Apart from $O(\log n)$ factors in the exponents, the former two estimates are asymptotically sharp. To do better, one has to use the 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 [5], while an $n^{9 \log_2 n}$ estimate follows from Liebeck [13]. 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 1.1. *Let G be a primitive permutation group of degree n. Then one of the following holds.*
(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 1.1. *Let G be a primitive subgroup of S_n.*
(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 [5]. The estimate in (i) is asymptotically sharp for uniprimitive groups of case (i) of theorem 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 1.1 also leads to a sharp exponential bound.

Corollary 1.2. *If G is a primitive subgroup of S_n not containing A_n, then $|G| < 3^n$. Moreover, if $n > 24$, then $|G| < 2^n$.*

This improves the Praeger-Saxl [16] 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 1.3. *If G is a primitive subgroup of S_n not containing A_n, then $|G|$ is 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 [11]. 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 refered to in [15]. (Note that the Kleidman-Wales list can also be deduced by a similar argument.)

Corollary 1.4. *Let G be a primitive permutation group of degree n not containing 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 [14] 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 [18] by Pyber. Improving restrictions on the composition factors of permutation groups one can bound their order. For example, Dixon [7] proved that a solvable permutation group of degree n has order at most $24^{(n-1)/3}$, and Babai, Cameron, Pálfy [3] 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 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 $|G| \leq d!^{(n-1)/(d-1)}$.*

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 [15], and for an alternative approach to dealing with nonabelian alternating composition factors see the paper [10] by Holt and Walton.

2 Proof of theorem 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 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 [5], 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 $|G| \leq |H \text{ wr } S_r| < n^{[\log_2 n]}$. Otherwise $|G| \leq |H \text{ wr } S_r| < (t^{1+[\log_2 t]})^r \cdot r!$ 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 [12], 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 [12], 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 [12], 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 [12], 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 [13] 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 [8], 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 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 [6] 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 [6].

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 1 or it is of type (i) with $r = k = 1$. This is proved below.

Lemma 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 1.1.

B. It may be assumed that both t and q are greater than 2. For if $q = 2$, then G is permutation isomorphic 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 staightforward 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 Corollaries

Corollaries 1.1-4 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 1.1.

Lemma 3.1. *Let G be a primitive group of degree n not of case (iii) of theorem 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 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 3.2. *If G is a primitive subgroup of S_n not containing A_n, then $|G| \leq |M_{12}|^{\frac{n}{12}} < 3^n$.*

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 1.1 and 1.2. The proof of corollary 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 [8] 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 isomorphic 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 Corollary 1.2 and 1.1 (i).

Lemma 3.3. *Let G be primitive of degree n not containing A_n.*
(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 isomorphic to one of the groups in the list of Corollary 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 isomorphic to one of the groups in the list of Corollary 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 1.1 (ii) follows from lemma 3.3 (ii).

For the proof of Corollary 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 [6]. 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.

4 An application

Corollary 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 3.2 for $n \geq 12$, and holds also for $4 < n < 12$ by inspection.) If G is transitive with k-element blocks of imprimitivity then

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

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

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

Acknowledgements

The author is grateful to Laci Pyber for his generous help and encouragement.

References

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

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

[3] 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.

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

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

[6] 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.

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

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

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

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

[11] 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.

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

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

[14] 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.

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

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

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

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

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

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