Bounding the Number of Conjugacy Classes of a Permutation Group

Attila Maróti *

School of Mathematics and Statistics, University of Birmingham
Birmingham B15 2TT, United Kingdom

4th of February 2004

Abstract

For a finite group G, let $k(G)$ denote the number of conjugacy classes of G. 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. If N is a normal subgroup of a completely reducible subgroup of $GL(n,q)$, then $k(N) \leq q^{5n}$. Similarly, if N is a normal subgroup of a primitive subgroup of S_n, then $k(N) \leq p(n)$ where $p(n)$ is the number of partitions of n. These improve results of Liebeck and Pyber.

1 Introduction.

Let $k(G)$ be the number of conjugacy classes of the finite group G. Kovács and Robinson [8] proved that if G is a subgroup of S_n, then $k(G) \leq 5^{n-1}$, and the proof of a proposed improvement of this to $k(G) \leq 2^{n-1}$ is reduced to the case where G is almost simple. For solvable permutation groups of degree $n > 2$, they obtained $k(G) \leq 3^{(n-1)/2}$. These results are independent of the classification theorem of finite simple groups (CTFSG). To do better, one needs to use CTFSG. Liebeck and Pyber [10] proved the general $k(G) \leq 2^{n-1}$ bound for arbitrary permutation groups. Later, Riese and Schmid [14] extended the Kovács-Robinson estimate of solvable permutation groups to certain p-solvable groups. In general, the following may be shown.

Theorem 1.1. *If G is a subgroup of S_n with $n > 2$, then $k(G) \leq 3^{(n-1)/2}$.*

To prove Theorem 1.1, we will need sharp estimates for the number of conjugacy classes of a normal subgroup of a primitive permutation group. To do this, we first prove the following

Theorem 1.2. *If G is a completely reducible subgroup of $GL(n,q)$, then $k(G) \leq q^{5n}$.*

*Research partially supported by the Hungarian National Foundation for Scientific Research Grant T034878, and the Instituto Italiano Studi Filosofici, Napoli, Italy.

This sharpens Corollary 5 of [10] which was used to extend a result of Arregi and Vera-Lopez [1]. (See Corollary 6 of [10] and its proof on page 554.) So by Theorem 1.2 we may sharpen a little on Corollary 6 of [10] as follows. If G is any subgroup of $GL(n, q)$, then $k(G) \leq q^{(2n^2+31n)/6} \cdot (n-1)! \cdot 2^{n-1}$.

For primitive permutation groups we need

Theorem 1.3. *Let G be a primitive subgroup of S_n, and let N be a normal subgroup of G. Then*

(1) $k(N) \leq p(n)$, 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 $N = A_3$.

(2) If the socle of G is not a direct product of non-abelian alternating groups, then $k(N) \leq n^6$.

This sharpens Corollary 2.15 of [10].

Now Theorem 1.1 is sharp only if $G = A_3$ or S_3 and if $n = 3$. To improve on this $3^{(n-1)/2}$ 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 S_4 when $n = 4$. A careful modification of the proof of Theorem 1.1 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 1.1. Next we restrict our attention on 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 $5^{(n-1)/3}$.

Theorem 1.4. *If G is a subgroup of S_n with no composition factor isomorphic to C_2, then $k(G) \leq (5/3)^n$.*

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 [10] shows that a general upper bound for $k(G)$ of the form c^n should satisfy $c < 5^{1/4} = 1.495....$ We prove the following

Theorem 1.5. *If G is a nilpotent subgroup of S_n, then $k(G) \leq 1.52^n$.*

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.

2 Completely reducible groups and primitive permutation groups.

In this section we deal with Theorems 1.2 and 1.3. First we reduce the proof of part (2) of Theorem 1.3 to the proof of Theorem 1.2. Next we prove Theorem 1.2, and finally, show part (1) of Theorem 1.3.

To do this, we need two basic results. First of all, we will often use the following elementary observation not just in this section but throughout the paper.

Lemma 2.1. *If H is a subgroup, and N is a normal subgroup of the finite group G, then*

(i) $k(H)/(G:H) \leq k(G) \leq k(H) \cdot (G:H)$ and

(ii) $k(G) \leq k(N) \cdot k(G/N)$.

Proof. See for example [5].

□

Now we state a slightly stronger version of Lemma 2.14 of [10].

Lemma 2.2. *Let G be a primitive subgroup of S_n having socle $S = L^r$ where L is a non-abelian simple group and r is an integer. Let N be a normal subgroup of G different from $\{1\}$. There are two possibilities.*

(1) If N contains S, then N has a normal subgroup K containing S, such that $|K/S| \leq n^{0.82}$ and N/K has an embedding into S_r with $r \leq \log_5 n$.

(2) If N does not contain S, then r is even, say $r = 2l$, and N contains a minimal normal transitive subgroup of G, say M, isomorphic to L^l. In this case, N has a normal subgroup K' containing M, such that $|K'/M| \leq n^{0.82}$ and N/K' has an embedding into S_l with $l \leq \log_5 n$.

Proof. Let m be the minimal faithful permutation degree of L. Notice that $m \geq 5$. If N contains S, then by Lemma 2.13 of [10] we see that $m^r \leq n$. Otherwise, if N does not contain S, we have $m^l \leq n$. It follows that $r \leq \log_5 n$ in the first case, and $l \leq \log_5 n$ in the second. Now N acts by conjugation on the direct factors of L^r in the first case, and on the direct factors of L^l in the second. The kernels K and K' of these actions have embeddings into $Aut(L)^r$ and $Aut(L)^l$ in the respective cases. So the groups N/K and N/K' may be considered as subgroups of S_r and S_l, respectively. Finally, it is easily checked from Lemma 8.6 of [7] that $|Out(L)| \leq m^{0.82}$. This gives us $|K/S| \leq |Out(L)|^r \leq m^{0.82 \cdot r} \leq n^{0.82}$ in the first case, and $|K'/M| \leq |Out(L)|^l \leq m^{0.82 \cdot r} \leq n^{0.82}$ in the second.

□

Let G be a primitive permutation group of degree n with socle $S = L^r$ 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. Then we may invoke Lemma 2.2 and use its notation. By part (ii) of Lemma 2.1, by Lemma 2.2 and by Theorem 2 of [10] we have $k(N/S) \leq n^{0.82} \cdot 2^{r-1} \leq n^{1.32}$ if N contains S and $k(N/M) \leq n^{0.82} \cdot 2^{l-1} \leq n^{1.32}$ otherwise. Now using Theorem 1 of [10] and the bounds for the minimal degrees $P(L)$ listed in the proof of Proposition 1.9 of [10] it is straightforward to see that $k(L) \leq P(L)^{3.6}$ holds when L is of Lie type; also if L is sporadic by [2]. It follows that if L is isomorphic to A_6, or is non-abelian and non-alternating, then by part (ii) of Lemma 2.1 and by Lemma 2.13 of [10] we have $k(N) \leq k(N/S) \cdot k(S) \leq n^{1.32} \cdot n^{3.6} < n^5$ if N contains S, and get $k(N) \leq k(N/M) \cdot k(M) \leq n^{1.32} \cdot n^{3.6} < n^5$ otherwise. Hence we reduced the proof of part (2) of Theorem 1.3 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 $p^m = n$. If we prove Theorem 1.2, then we get $k(N) \leq k(N/S) \cdot k(S) \leq p^{5m} \cdot n = n^6$, which would complete the proof of part (2) of Theorem 1.3.

We now turn to the proof of Theorem 1.2.

Let G be a completely reducible subgroup of $GL(n,q)$ acting on V, the n-dimensional vectorspace over $GF(q)$ where q is a fixed prime power. We will show $k(G) \leq q^{5n}$ by induction on n. This is true for $n = 1$ since G is cyclic in this case 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 nontrivial submodules, say of V_1 and of V_2, of dimensions $m < n$ and $n-m$, respectively. Let the kernel of the action of G on the vectorspace V_1 be B. Since B is normal in G, we see that B is completely reducible on V and also on V_2. By induction we have $k(G/B) \leq q^{5m}$ and $k(B) \leq q^{5(n-m)}$, hence we get $k(G) \leq k(B) \cdot k(G/B) \leq q^{5n}$ by part (ii) of Lemma 2.1.

Now the vectorspace V admits an m-space decomposition $V = V_1 \oplus \ldots \oplus V_t$ for some $m \leq n$ and $t \geq 1$ with respect to the irreducible group G. Suppose also that t is 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 part (ii) of Lemma 2.1 and by Theorem 2 of [10] where B denotes the kernel of the action of G on the set of subspaces $\{V_1, \ldots, V_t\}$. If $t < n$ and $m \geq 2$, then let $V = (V_1 \otimes \ldots \otimes V_r) \oplus \ldots \oplus (V_{rl-r+1} \otimes \ldots \otimes V_{rl})$ be a decomposition of the $GF(q)G$-module V such that $rl \geq 1$ is maximal and that $dim(V_i) = n_0 \neq 1$ for all $1 \leq i \leq rl$. Let B be the kernel of the action of G on the set of subspaces $\{V_1, \ldots, V_{rl}\}$. As before, B is normal in G, and so it is completely reducible on V. Let G_0 and B_0 be the images of G and B respectively under the natural homomorphism from $GL(n,q)$ to $PGL(n,q)$. Note that $B_0 \triangleleft G_0$. For each $1 \leq i \leq rl$, let G_i be the subgroup of G_0 stabilizing the vectorspace V_i. Also, let the kernels of these actions be K_i for all $1 \leq i \leq rl$. By the maximality of rl, by repeated use of the main theorem of [9] and by the irreducibility of G, the groups G_i/K_i are isomorphic and either have orders less than q^{3n_0}, or are normalizers of classical groups over a subfield or over an extension field of $GF(q)$, or are subgroups of S_c in a representation of smallest degree $c = n_0 + 1$ or $n_0 + 2$ for all $1 \leq i \leq rl$. In the first case we have $k(B_0) \leq |B_0| \leq q^{3n}$, while in the third we see that $k(B_0) \leq 2^{n+(n/2)} < q^{2n}$ by Theorem 2 of [10] and by repeated use of part (ii) of Lemma 2.1.

Suppose that the second case holds. Let the non-abelian simple normal subgroups of the groups G_i/K_i be isomorphic to the classical group L. We claim that if N is a subnormal subgroup of $Aut(L)$, then $k(N) \leq P(L)^{4.1}$ where $P(L)$ is the minimal degree of a permutation representation of L. If L is not equal to $PSL(2,9)$, $PSL(2,27)$, $PSL(3,4)$ or $PSL(3,16)$, then by Lemma 8.6 of [7] and by $k(L) \leq P(L)^{3.6}$ above, we have $k(N) \leq k(L) \cdot |Out(L)| \leq P(L)^{4.1}$. For the remaining four cases the claim readily follows.

For all $1 \leq j \leq rl$, denote the group $K_1 \cap \ldots \cap K_j$ by $\overline{K}_j$. Also put $\overline{K}_0 = B_0$. We claim that for any index $1 \leq j \leq rl$, the factor group $B_0 \cap \overline{K}_{j-1}/B_0 \cap \overline{K}_j$ may be considered as a subnormal subgroup of the irreducible group G_j/K_j, and hence it is completely reducible on V_j. Indeed. Notice that $B_0 \triangleleft G_j$, and also that $B_0 \cap \overline{K}_{j-1}$ is subnormal in B_0 and hence subnormal in G_j also. Now we have that $(B_0 \cap \overline{K}_{j-1})K_j$ is subnormal in G_jK_j, from which we conclude that $B_0 \cap \overline{K}_{j-1}/B_0 \cap \overline{K}_j \cong (B_0 \cap \overline{K}_{j-1})K_j/K_j$ is subnormal in $G_jK_j/K_j \cong G_j/G_j \cap K_j = G_j/K_j$.

Next we will estimate $k(B_0)$. By repeated applications of part (ii) of Lemma 2.1 and by our two claims above we have $k(B_0) \leq \prod_{j=1}^{rl} k(B_0 \cap \overline{K}_{j-1}/B_0 \cap \overline{K}_j) \leq q^{4.1 \cdot rln_0} \leq q^{4.1 \cdot n}$ in this second case under consideration. But we may also conclude from the above that in all three cases we have $k(B_0) \leq q^{4.1 \cdot n}$.

Now the factor group G_0/B_0 can be considered as a permutation group of degree rl, so by Theorem 2 of [10] we have $k(G_0/B_0) \leq 2^{rl-1}$. Hence, by part (ii) of Lemma 2.1 we get $k(G_0) \leq k(G_0/B_0) \cdot k(B_0) \leq 2^{(n/2)-1} \cdot q^{4.1 \cdot n} \leq q^{5n}/d$ where d is the greatest common divisor of n and $q-1$. Finally, again by part (ii) of Lemma 2.1 we find that $k(G) \leq k(G_0) \cdot d \leq q^{5n}$.

This completes the proof of Theorem 1.2 and of part (2) of Theorems 1.3.

Now we turn to the proof of part (1) of Theorem 1.3.

Lemma 2.3. *Let $m \geq 5$, or $m \geq 4$ and $r = 1$. If $(A_m)^r \leq G \leq S_m$ wr S_r, then $k(G) \leq p(m^r)$, with equality if and only if $G = S_{m^r}$ or $m^r = 3$ and $G = A_3$.*

Proof. Put $n := m^r$. Let $r = 1$. We may take $G = A_n$. 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 summands. In this case associate one conjugacy class of A_n with π, and associate the other one with that partition of n which we get from π by replacing the (unique) greatest odd summand k by the summands 1 and $k-1$. This correspondence is $1-1$. 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.

Now let $r \geq 2$ and $m \geq 5$. In this case we can write $k(G) \leq p(m)^r \cdot 2^{r-1}$ by part (ii) of Lemma 2.1 and by Theorem 2 of [10]. It is enough to prove $p(m)^r 2^{r-1} < p(m^r)$. Let $r = 2$. It is sufficient to give $2p(m)^2 - p(m) + p(m+1) > 2p(m)^2$ different partitions of m^2. Let Π_1 be the set of all partitions of m^2 of the following form. Take any partition of m and multiply each summand by m. We get a partition of m^2. Now take a least summand im of the former partition and replace it by the summands $ij_1, \ldots, ij_s$ where $(j_1, \ldots, j_s)$ is an arbitrary partition of m. By this way we get $p(m)^2$ pairwise different partitions of m^2. Now let Π_2 be the set of all partitions of m^2 of the following form. Take any partition of m and multiply each summand by $m-1$. Uniting this partition with an arbitrary partition of m we get a partition of m^2. By this way we also get $p(m)^2$ pairwise different partitions of m^2. Since $m-1$ and m are relative prime numbers $|\Pi_1 \cap \Pi_2| = p(m)$. Finally, we define another set of partitions, Π_3 with the property that $\Pi_3 \cap (\Pi_1 \cap \Pi_2) = \emptyset$ by the following way. Take any partition of $m+1$ and add the additional summand $m^2 - m - 1$ to it. We get a partition of m^2. The number of such partitions is clearly $p(m+1)$. So we get $|\Pi_1 \cup \Pi_2 \cup \Pi_3| = 2 \cdot p(m)^2 - p(m) + p(m+1) > 2 \cdot p(m)^2$. Now let $r \geq 3$. It is sufficient to give $2 \cdot (p(m)-1)^r m^{r-2}$ different partitions of m^r. To do this first define the following process for arbitrary numbers $2 \leq i \leq r$ and a.

(1) Take any partition of the number $m^i a$ with at least two summands and with

each summand divisible by $m^{i-1}a$. (The number of such partitions is $p(m)-1$.)

(2) If $i \geq 3$, then take any integer $0 \leq s \leq m-1$. (There are m different possibilities.) Else if $i = 2$ or 1, then take any integer $0 \leq s \leq i-1$. (There are i different possibilities.)

(3) Take a maximal summand say $jm^{i-1}a$, and replace it by the two summands $jm^{i-1}a - s$ and s.

(4) Take a minimal summand which is divisible by $m^{i-1}a$ and different from the one chosen in (3), say $m^{i-1}b$. Put $i := i-1$ and $a := b$.

For $m^r \cdot 1$ repeat steps (1)-(4) $r-1$-times. Finally, for all possible outputs do step (1). By this way we get $2 \cdot (p(m)-1)^r m^{r-2}$ pairwise different partitions of m^r.

$\square$

Suppose that $N \neq \{1\}$ is a normal subgroup of a primitive group G of degree n with socle $S = L^r$ where L is a non-abelian alternating group different from A_6. By the proof of Lemma 2.2, there exists a normal subgroup K (or K') of N with the property that K (or K') embeds into $Aut(L)^r$ (or $Aut(L)^l$ where $r = 2l$) in such a way that $k(K)$ (or $k(K')$) is at most $p(m)^r$ where $L = A_m$ and that N/K (or N/K') has an embedding into S_r. Now, by part (ii) of Lemma 2.1 and by Theorem 2 of [10], we see that $k(N) \leq p(m)^r 2^{r-1}$. By the proof of Lemma 2.3 we have that $p(m)^r 2^{r-1} < p(m^r)$ for $r \geq 2$. In case $r = 1$, apply the statement of Lemma 2.3. Finally, $m^r \leq n$ follows from Lemma 2.13 of [10].

If L is isomorphic to A_6 or is abelian or a non-alternating simple group, then by part (2) of Theorem 1.3 (and its proof) and by Theorem 4.2 of [11] we have $k(N) \leq n^6 < e^{2.5\sqrt{n}}/13n < p(n)$ for $n \geq 284$. Moreover by [6] 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 part (1) of Theorem 1.3 we may suppose that $n < 252$. Now the computer package [6] 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 $N = S_n$ (when $n \leq 4$ or $n = 6$), or if $N = A_3$ when $n = 3$.

This completes the proof of part (1) of Theorem 1.3.

3 The general bound.

In this section we prove Theorem 1.1. We will start with a few lemmas.

Lemma 3.1. *If G is a subgroup of S_n with $n \leq 12$, then $k(G) \leq 5^{\frac{n}{4}}$.*

Proof. Use induction on n. If G is intransitive and has an orbit Δ of length $k < n$, then by induction $k(G) \leq k(G/K) \cdot k(K) \leq 5^{k/4} \cdot 5^{(n-k)/4} = 5^{n/4}$ 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 [6].

$\square$

We also need to give an upper estimate for the number of partitions of the integer n.

Lemma 3.2. *For $n > 12$ we have $p(n) < c \cdot (3/2)^n$ where $c = (2 \cdot \sqrt{3})^{-\frac{1}{2}}$.*

Proof. For $n \geq 50$ we have $p(n) \leq e^{\pi\sqrt{2n/3}}$ by [4], and the right hand side is smaller than $c \cdot (3/2)^n$. For $12 < n < 50$ the statement is checked easily. □

We state another technical lemma.

Lemma 3.3. *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 $k(N) \leq 2^{(n-1)/2}$.*

Proof. This is checked easily by [6]. □

Finally, the following is taken from page 447 of [8].

Lemma 3.4. *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 will now begin the proof of Theorem 1.2. 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 [3] we have four possibilities to consider for subgroups of G containing H. These were also given in [8], so from now on we use the notations of that paper for simplicity.

(i) H max G.

(ii) H max K max G with $(G : K) = 2$.

(iii) H max K max G with $(K : H) = 2$.

(iv) H max K max L max G with $(K : H) = (G : L) = 2$.

By Lemma 3.1, we may suppose that $n \geq 13$.

Case (i). By part (1) of Theorem 1.3 and Lemma 3.2, 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 $G \setminus K$ 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 part (1) of Theorem 1.3, 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 3.2, 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 3.2 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 3.1 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 3.3 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 3.1, every subgroup of G/C has at most $5^{a/4}$ conjugacy classes, so by Lemma 3.4 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 part (1) of Theorem 1.3, $k(L/D) \leq p(a)$, so that $k(L/C) \leq 2^a p(a)$. Now set $M = CC^x$. Then $k(MD^x/D^x) \leq p(a)$ by part (1) of Theorem 1.3, 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 $k(G) \leq 2 \cdot 4^a p(a)^2$. Suppose first that $a > 12$. By Lemma 3.2 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 3.1 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 3.3. 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 3.4. 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 $p(a) \leq 2^{(a+1)/2}$ sufficies 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 3.4 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 3.4, we get $k(L/C) \leq ((2^5 - 2)/5 + 2) \cdot 7 = 56$. Similarly $k(M/C^x) \leq 56$. This m eans 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 3.4, 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 Groups with no composition factor isomorphic to C_2.

We start with the following

Lemma 4.1. *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 $k(G) \leq k(A_n)$.

Proof. This is easily checked by [6].

□

We now turn to the proof of Theorem 1.4. It is sufficient to prove 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 $|\Delta|$ can not 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 [3] 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 with $(G : K) = 3$.

(iii) H max K max G with $(K : H) = 3$.

(iv) H max K max L max G with $(K : H) = (G : L) = 3$.

By Lemma 4.1, we may suppose that $n \geq 13$.

Case (i). By part (1) of Theorem 1.3 and by Lemma 3.2, 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 part (1) of Theorem 1.3, 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 3.2 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 [6] 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). Observe that K is normal in G. Let $(G : K) = a$, and let $C = core_G(K)$. Since C has no composition factors 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 part (1) of Theorem 1.3. This yields $k(G) \leq k(C) \cdot k(G/C) \leq 3^{n/3} \cdot p(n/3)$. By Lemma 3.2, 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 [6] 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 4.1 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 $(G : K) = a$. 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 part (1) of Theorem 1.3 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 part (1) of Theorem 1.3 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 $k(G) \leq 3 \cdot k(L) \leq 3 \cdot k(L/C) \cdot k(C) \leq 3^{a+1}p(a) \cdot k(C) \leq 3^{a+1}p(a) \cdot k(C/C^x \cap C) \cdot k(C^x \cap C) \leq 3^{3a+1}p(a)^3 = 3 \cdot 3^{n/3}p(n/9)^3$. By Lemma 3.2 we have $k(G) \leq 3 \cdot 3^{n/3}p(n/9)^3 < 3 \cdot 3^{n/3} \cdot c^3 \cdot (3/2)^{n/3} < (5/3)^{n-1}$ for $n > 108$. For $n = 90$, 99 and 108 it is checked by [6] that $k(G) \leq 3 \cdot 3^{n/3}p(n/9)^3 < (5/3)^{n-1}$. For $n = 45$, 54, 63, 72 and 81 notice that by Lemma 4.1, 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 $n \neq 18$ nor 36, because $a \neq 2$ nor 4, since G does not have a composition fa ctor 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 4.1, 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.

5 Nilpotent groups.

In this section we prove Theorem 1.5. 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 [15]. 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 5.1. *If G is a p-subgroup of S_n with $n > 3$ and $p > 2$, then $k(G) \leq 5^{(n-1)/4}$.*

Proof. Let G be a counterexample with n minimal. By the argument at the beginning of this section we may suppose that G is transitive. We may also assume that $n = 3^t$, for if $p > 3$, then $k(G) \leq |G| \leq 5^{(n-1)/4}$. If $t = 2$, then by [6] we see that $k(G) \leq 17 < 5^{(n-1)/4}$. Let $t = 3$. We may suppose that $|G| > 3^9$. For otherwise, we would have $k(G) \leq |G| \leq 3^9 < 5^{(n-1)/4}$. A 3-Sylow subgroup of S_{27} has order 3^{13} and has 1683 conjugacy classes by [12]. So if G has order different from 3^{10}, then by part (i) of Lemma 2.1, we get $k(G) \leq 9 \cdot 1683 < 3^9$. Else if $|G| = 3^{10}$, then $k(G) \leq 3^3 + ((3^{10} - 3^3)/3) < 5^{13/2}$. Finally, if $t > 3$, then let Δ be a block of imprimitivity of G of size 9. Let the base group of the system of imprimitivity associated to the block Δ be B. Then by assumption we have $k(G) \leq k(B) \cdot k(G/B) \leq 5^{(n-3^{t-2})/4} \cdot 5^{(3^{t-2}-1)/4} = 5^{(n-1)/4}$. This is a contradiction.

□

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 [6] 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 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 [10] and the asymptotic estimate for the number of conjugacy classes of the symmetric 2-group of [12] 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. So we ask the following.

Question 5.1. *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 $k(G) > p(n)$.

Interestingly, one meets similar problems when trying to improve existing *lower* bounds for $k(G)$ (in terms of $|G|$) as it is suggested in [13].

Acknowledgements

Thanks are due to both L. Pyber and G. R. Robinson for their kind help and encouragement. The author also thanks A. Hulpke for providing information about transitive 2-groups of degree 32, and is grateful to S. Hendren and the referee for some helpful comments.

References

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

[2] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A. Atlas of finite groups. *Oxford University Press*, Eynsham, (1985).

[3] Dixon, J. D.; Mortimer, B. Permutation groups. *Springer*, Graduate Texts in Mathematics, **163** (1996).

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

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

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

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

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

[9] 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.

[10] 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.

[11] 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).

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

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

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

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