SYLOW SUBGROUPS AND THE NUMBER OF CONJUGACY CLASSES OF p-ELEMENTS

ALEXANDER MORETÓ, JOSU SANGRÓNIZ, AND ALEXANDRE TURULL

1. Introduction

Let G be a finite group, p a prime, and P a Sylow p-subgroup of G. Let $k_p(G)$ denote the number of conjugacy classes of non-trivial p-elements of G. Furthermore, we write $\tilde{k}_p(G)$ to denote the number of orbits of non-trivial p-elements of G under the action of $\mathrm{Aut}(G)$. Clearly, $\tilde{k}_p(G) \leq k_p(G)$ for all finite groups G and all primes p. Our goal is to bound the derived length of P in terms of $k_p(G)$ or $\tilde{k}_p(G)$. For p-solvable groups there is a straight forward bound.

Theorem A. Let G be a finite p-solvable group and $P \in \mathrm{Syl}_p(G)$. Then the derived length of P cannot exceed $\tilde{k}_p(G)$ (and hence, can not exceed $k_p(G)$ either).

As it stands, this bound is not valid for all finite groups. Indeed, checking in the Atlas [2] yields the following facts. There are groups with extraspecial Sylow 3-subgroups of order 27 but only one conjugacy class of non-trivial 3-elements, such as the Tits Group ${}^2F_4(2)'$, the Fourth Janko Group J_4 and the Rudvalis Group Ru. Furthermore, if $G = M$ is the Monster and $p = 7$, then $k_p(G) = \tilde{k}_p(G) = 2$, while the derived length of a Sylow p-subgroup is 3. However, using the Classification of Finite Simple Groups, we also prove the following.

Theorem B. Let G be a finite group and $P \in \mathrm{Syl}_p(G)$. Then the derived length of P cannot exceed $\tilde{k}_p(G)+7$ (and hence, cannot exceed $k_p(G) + 7$ either).

The first and second author's research is partially supported by the Spanish Ministerio de Ciencia y Tecnología, grant BFM2001-0180 and the FEDER. The first author is also supported by the Basque Government. The second author is also partially supported by the University of the Basque Country, grant 1/UPV00127.310-E-13817/2001. The third author is partially supported by a grant from the NSA.

We have not tried to use the smallest possible additive constant. Instead, we use 7 to provide smooth proofs. We propose this result as qualitative only, and suggest that there could, in fact, be a logarithmic bound. Indeed, such logarithmic bound does exist for solvable and simple groups. It could even be true that the best possible bound is a double logarithmic one. Notice that a logarithmic bound for the derived length would follow from a linear bound for the nilpotency class, however, it is not clear to us if the nilpotency class can be bounded at all by any function of $k_p(G)$. On the other hand, although our results refer to the derived length, the proofs work as well for the length of the Frattini series (defined by $P_0 = P$, $P_i = \Phi(P_{i-1})$ for $i > 0$). As the semilinear groups show, it is not possible to bound the exponent of p in the order of a Sylow p-subgroup by any function of the number of conjugacy classes of p-elements.

2. Proofs

We begin by proving a convenient property of the invariant $\tilde{k}_p(G)$.

Lemma 2.1. *Let G be a finite group and let p be a prime. Let N be a characteristic subgroup of G. Then*

$$\tilde{k}_p(G/N) + \tilde{k}_p(N) \leq \tilde{k}_p(G).$$

Proof. Clearly the representatives of the orbits of non-trivial p-elements of N under the action of $\mathrm{Aut}(N)$ are also representatives of distinct orbits of non-trivial p-elements of N under the action of $\mathrm{Aut}(G)$. Now, for each representative gN of an orbit of the action of $\mathrm{Aut}(G/N)$ on the non-trivial p-elements of G/N, we take the p-part g_p of g. Notice that $g_p \notin N$. All these elements g_p determine different orbits of non-trivial p-elements under the action of $\mathrm{Aut}(G)$, so the inequality follows immediately. □

We can now deduce Theorem A.

Proof of Theorem A. Suppose false, and let G be a counterexample with minimum order. Suppose that G is not characteristically simple. Then let N be a characteristic subgroup of G, with $1 \neq N \neq G$. Let $P \in \mathrm{Syl}_p(G)$. By the minimality of our counterexample, we have

$$\mathrm{dl}(P) \leq \mathrm{dl}(PN/N) + \mathrm{dl}(P \cap N) \leq \tilde{k}_p(G/N) + \tilde{k}_p(N).$$

Therefore, the result follows immediately from Lemma 2.1 in this case. Hence, G is characteristically simple. Since G is p-solvable, it follows

that G is an abelian p-group or a p'-group. Hence the result holds for G. This contradiction completes the proof of the theorem. □

We could have given an easier proof of this theorem: it suffices to observe that if G is p-solvable and we take a series of characteristic subgroups with characteristically simple factors, then the derived length of a Sylow p-subgroup of G is at most the number of factors which are p-groups. On the other hand, if we take a non-trivial element in each of these factors, then the p-part of their pull-backs in G produce representatives of different orbits under the action of $\mathrm{Aut}(G)$, so the result is clear. However, we have preferred to include the present argument since it will be used twice later on in the proof of Theorem B.

For solvable groups the following stronger result holds relating the derived length and the number of conjugacy classes of p-elements.

Theorem 2.2. *There exist constants A and B such that if G is solvable and p divides $|G|$, then*

$$\mathrm{dl}(G/O_{p'}(G)) \leq A \log\left(k_p(G/O_{p'}(G))\right) + B.$$

Proof. It is clear that we can assume that $O_{p'}(G) = 1$. It is proved in Theorem 2.4 of [4] that if V is a faithful irreducible module for a solvable group G, then the derived length of G is bounded by a doubly logarithmic function of the number of orbits. It is easy to see that this result can be extended to completely reducibly actions, so in our case we can apply it to the action of $G/F(G)$ on $F(G)/\Phi(G)$, by Gaschutz's theorem (see Satz III.4.2 and III.4.5 of [3]). This yields that the derived length of $G/F(G)$ is bounded by a doubly logarithmic function of the number of G-conjugacy classes of $F(G)$ and, since this is a p-subgroup, by the number of classes of p-elements of G.

Now, it suffices to find a logarithmic bound for the derived length of $F(G)$ in terms of $k_p(G)$. But it is well-known that the derived length of a p-group is bounded logarithmically by the nilpotency class (see Satz III.2.12 of [3]) and this is obviously smaller than the number of G-classes contained in $F(G)$. □

We begin work toward a proof of Theorem B. Our first lemma is probably well-known, but we include its easy proof for the sake of completeness.

Lemma 2.3. *Let F be any field and let P be a finite p-subgroup of $\mathrm{GL}(n, F)$. Then the derived length of P does not exceed $\lfloor \log_2(n) \rfloor + 1$.*

Proof. Assume first that the characteristic of F is p. Then P is conjugate to a subgroup of the group of upper unitriangular matrices and the result follows since the derived length of this group is $\log_2(n)$ or $\lfloor \log_2(n) \rfloor + 1$, depending on whether n is a power of 2 or not (see Satz III.16.3 of [3] for a proof).

Thus, we may assume that the characteristic of F is coprime to $|P|$. Let $\overline{F}$ be an algebraic closure of F. The group P embeds into $\mathrm{GL}(n, \overline{F})$. Since P acts completely reducibly on its natural module, we may assume that it is an irreducible subgroup of $\mathrm{GL}(n, \overline{F})$, that is, P has a faithful irreducible character χ of degree n. In particular, $n = p^a$ for some a. Since P is a monomial group, there exists a subgroup H of index n in P and $\lambda \in \mathrm{Irr}(H)$ such that $\chi = \lambda^P$. Since $P^{(a)} \leq H$, we have that $P^{(a+1)} \leq H'$ is a normal subgroup contained in $\mathrm{Ker}\, \chi = 1$. Therefore $\mathrm{dl}(P) \leq \log_p(n) + 1 \leq \log_2(n) + 1$ and the proof is complete. □

In the next result, we prove a strong form of Theorem B for certain groups.

Lemma 2.4. *Let G be a finite group all of whose composition factors are either abelian or subgroups of S_7. If $P \in \mathrm{Syl}_p(G)$, then $\mathrm{dl}(P) \leq \tilde{k}_p(G)$.*

Proof. Let G be a counterexample with minimum order. By the proof of Theorem A, G is characteristically simple. Clearly, G is not abelian. Hence, G is a direct sum of isomorphic non-abelian simple groups. Assume that G is not simple and let S be a simple normal subgroup of G. By the minimality of G, we have that

$$\mathrm{dl}(P) = \mathrm{dl}(P \cap S) \leq \tilde{k}_p(S) \leq \tilde{k}_p(G).$$

Hence, G is simple. Then $|G|$ divides $|S_7| = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. The Sylow p-subgroups of G are abelian for $p > 2$ and the result follows in this case. If $p = 2$, then the derived length of P cannot exceed 2 and it suffices to observe that groups of exponent 2 are abelian to deduce the result. □

Now, we prove Theorem B for each family of simple groups

Lemma 2.5. *Theorem B holds for the alternating groups.*

Proof. It is well-known that the derived length of the Sylow p-subgroups of S_n is $\lfloor \log_p(n) \rfloor$ (see Satz III.15.3 of [3]), so all we need to prove is

that $\lfloor \log_p(n) \rfloor \leq 7 + \tilde{k}_p(A_n)$. We can suppose that $n > 6$, so that the automorphisms of A_n consist of conjugation by elements of S_n. If p is odd, by considering products of disjoint p-cycles, we get that $\tilde{k}_p(A_n) \geq \lfloor n/p \rfloor$. For $p = 2$ we consider products of an even number of transpositions so that $\tilde{k}_2(A_n) \geq \lfloor n/4 \rfloor$. The result is clear in both cases. □

Lemma 2.6. *Suppose G has a faithful projective representation of dimension at most 255 over some field. Then, Theorem B holds for G.*

Proof. Since Theorem B holds when p does not divide the order of G, it suffices to show that $\mathrm{dl}(P) \leq 8$. By Lemma 2.3, we have that $\mathrm{dl}(P) \leq \lfloor \log_2(255) \rfloor + 1 = 8$. The result follows. □

Lemma 2.7. *Theorem B holds for all the sporadic simple groups, all exceptional or exceptional twisted simple groups, and all classical simple groups whose defining module has dimension smaller than 256.*

Proof. ¿From the order formulas of the sporadic groups, we notice that $\mathrm{dl}(P) \leq 7$ for every sporadic group G and prime p. Hence, Theorem B holds for the sporadic groups. By p. 43 of [1], any exceptional or exceptional twisted group of Lie type embeds into the automorphism group of a vector space whose dimension does not exceed 248. Hence, Lemma 2.6 completes the proof of the lemma. □

The following estimation for the derived length of a p-subgroup of $\mathrm{GL}(n, q)$ is a refinement of Lemma 2.3.

Lemma 2.8. *Let P be a p-subgroup of $\mathrm{GL}(n, q)$. Then the derived length of P does not exceed $\lfloor \log_2(n/e) \rfloor + 1$, where e is 1 if q is a power of p, and otherwise, e is the order of q modulo p.*

Proof. We can suppose that q is not a power of p (for $e = 1$ the result reduces to Lemma 2.3). Set $m = \lfloor n/e \rfloor$. The group $\mathrm{GL}(m, q^e)$ can be embedded into $\mathrm{GL}(me, q)$ which in turn can be mapped into $\mathrm{GL}(n, q)$. On the other hand, the order of the Sylow p-subgroups of $\mathrm{GL}(m, q^e)$ and $\mathrm{GL}(n, q)$ is the same (the key is that p does not divide $q^i - 1$ unless i is a multiple of e). We conclude that the Sylow p-subgroups of $\mathrm{GL}(m, q^e)$ and $\mathrm{GL}(n, q)$ are isomorphic and so P can be embedded into $\mathrm{GL}(m, q^e)$. The result follows now from Lemma 2.3. □

Lemma 2.9. *Theorem B holds for all classical simple groups of Lie type.*

Proof. Let S be a classical simple group of Lie type. We can describe S as a factor group $X/X \cap Z$, where X is a suitable subgroup of $\mathrm{GL}(n,q)$ ($\mathrm{GL}(n,q^2)$ in the unitary case) and Z is the group of invertible scalar matrices. By Lemma 2.6, we assume without loss that $n \geq 256$. It follows that all automorphisms of S can be viewed as compositions of conjugation by elements of $\mathrm{GL}(n,q^2)$, field automorphisms, and the inverse-transpose automorphism. As in Lemma 2.8, we define e to be 1 if q is a power of p, and otherwise, we define e to be the order of q modulo p. Considering a particular set of matrices of X, we shall prove that $\tilde{k}_p(S) \geq cn/e$ for some (not too small) explicit constant c. It will be obvious in all the cases that this linear bound is much bigger that the logarithmic bound in Lemma 2.8 and so Theorem B will be proved for these groups too.

The matrices in X that will represent the desired different orbits of p-elements in S under the action of $\mathrm{Aut}(S)$ will have a simple diagonal block structure. We start by taking a suitable small $r \times r$ matrix C of order p and then, for each i with $ri < n$, we construct the matrix T_i with i diagonal blocks equal to C and the identity block of size $n - ri$. Any automorphism of S lifts to X and moreover preserves the multiplicity of the eigenvalue 1, so if one of the matrices T_i is transformed into a scalar multiple of T_j, say λT_j, then either $\lambda = 1$ or λ^{-1} is an eigenvalue of C. In any case, by comparing the multiplicity of 1 as an eigenvalue of T_i and λT_j, we notice that j is uniquely determined by λ and i. Since the number of possibilities for λ cannot exceed $r+1$, it is clear that the matrices T_i define at least $\frac{1}{r+1}\lfloor \frac{n-1}{r} \rfloor$ orbits for the action of $\mathrm{Aut}(S)$ on S. Actually, if p does not divide $q-1$, C cannot have eigenvalues different from 1, and so the matrices T_i define at least $\lfloor \frac{n-1}{r} \rfloor$ different orbits. If q is a power of p, the only eigenvalue of C is 1 and all the matrices T_i with $ri \leq n$ have different Jordan forms, so we obtain in this case at least $\lfloor \frac{n}{r} \rfloor$ different orbits.

We start by the linear groups $S = \mathrm{PSL}(n,q)$. We distinguish three cases. If p does not divide $q-1$ and q is not a power of p, then p divides the order of $\mathrm{SL}(e,q)$ and we can choose a matrix C of order p in this group. By the preceding discussion, the matrices T_i define at least $\lfloor \frac{n-1}{e} \rfloor$ orbits and so $\tilde{k}_p(S) \geq \lfloor \frac{n-1}{e} \rfloor$. If p divides $q-1$, then $\mathrm{SL}(2,q)$ has elements of order p and we obtain the bound $\tilde{k}_p(S) \geq \frac{1}{3}\lfloor \frac{n-1}{2} \rfloor$. Finally, if q is a power of p, then again there are matrices of order p is $\mathrm{SL}(2,q)$ and $\tilde{k}_p(S) \geq \lfloor \frac{n}{2} \rfloor$.

The symplectic and unitary cases can be dealt with similarly, so we consider next the orthogonal case $S = \Omega(2n+1,q)$ in odd characteristic.

If q is not a power of p, then p divides the order of $\Omega(2e+1,q)$ and we can take a matrix C of order p in this group. The matrices T_i yield then the bound $\tilde{k}_p(S) \geq \lfloor \frac{2n}{2e+1} \rfloor$. If q is a power of p we can take C in $\Omega(3,q)$ and we obtain $\tilde{k}_p(S) \geq \lfloor \frac{2n+1}{3} \rfloor$.

We consider now the orthogonal groups in odd characteristic and even dimension. There are two families of such groups, $S = P\Omega^{\pm}(2n,q)$. In any of the two cases there is a natural embedding $\Omega(2n-1,q) \subseteq \Omega^{\pm}(2n,q)$. Suppose that q is not a power of p and take a matrix C of order p in $\Omega(2e+1,q)$. Then the matrices T_i with $(2e+1)i < 2n$ give the bound $\tilde{k}_p(S) \geq \frac{1}{2}\lfloor \frac{2n-1}{2e+1} \rfloor$ (we divide by 2 because there are two scalar matrices in $\Omega^{\pm}(2n,q)$). If q is a power of p, then we can take C in $\Omega(3,q)$ and $\tilde{k}_p(S) \geq \lfloor \frac{2n-1}{3} \rfloor$.

Finally suppose that $S = \Omega^{\pm}(2n,q)$, where q is a power of 2. We can describe the elements in the orthogonal group $\mathrm{O}^{\pm}(2n,q)$ as the matrices M such that $M^t(B+B^t)M = B+B^t$ and all the elements in the diagonal of M^tBM are zero. Here the superscript t indicates transposition and B is the diagonal block matrix in which $n-1$ blocks are equal to $J = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and the last block is either J (in the $+$ case) or $\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$ (in the $-$ case), α being an element in the field such that the polynomial $\alpha x^2 + x + \alpha$ is irreducible. The group S is the commutator subgroup of $\mathrm{SO}^{\pm}(2n,q)$. If $p \neq 2$, we take a matrix C of order p in $\Omega^{+}(2(e+1),q)$. All the matrices T_i with $2(e+1)i \leq 2n-2$ belong to $\Omega^{\pm}(2n,q)$ and so $\tilde{k}_p(S) \geq \lfloor \frac{2n-2}{2(e+1)} \rfloor$. If $p = 2$, we can take C in $\Omega^{+}(4,q)$ and then $\tilde{k}_p(S) \geq \lfloor \frac{2n-2}{4} \rfloor$. □

Now, we are ready to conclude the proof of Theorem B

Proof of Theorem B. Assume false. Let G be a counterexample with minimum order. By Lemmas 2.6, 2.7, 2.5 and 2.9, G is not simple. Suppose $F(G) \neq 1$. Then, by Theorem A, we have $\mathrm{dl}(P \cap F(G)) \leq \tilde{k}_p(F(G))$, and by the minimality of our counterexample, we have $\mathrm{dl}(PF(G)/F(G)) \leq \tilde{k}_p(G/F(G)) + 7$. Arguing as in the proof of Theorem A, it follows that $\mathrm{dl}(P) \leq \tilde{k}_p(G) + 7$. As G is a counterexample to Theorem B, it follows that $F(G) = 1$. In a similar way, we also obtain that $O_{p'}(G) = 1$. Assume that N_1 and N_2 are two different

minimal characteristic subgroups of G. By the inductive hypothesis,

$$\begin{aligned}\mathrm{dl}(P) &= \max\{\mathrm{dl}(PN_1/N_1), \mathrm{dl}(PN_2/N_2)\}\\ &\leq \max\{\tilde{k}_p(G/N_1)+7, \tilde{k}_p(G/N_2)+7\}\\ &\leq \tilde{k}_p(G)+7.\end{aligned}$$

Thus $F^*(G)$ is the direct product of, say, t copies of a non-abelian simple group S and $G/F^*(G)$ embeds into $\mathrm{Out}(S) \wr S_t$. By Schreier's Conjecture, $\mathrm{Out}(S)$ is solvable. Since $O_{p'}(G) = 1$, we have that p divides $|S|$.

It follows that if $t \leq 7$, $G/F^*(G)$ satisfies the hypothesis of Lemma 2.4. Therefore, $\mathrm{dl}(PF^*(G)/F^*(G)) \leq \tilde{k}_p(G/F^*(G))$. Now, if S_1 is one of the direct factors of $F^*(G)$ isomorphic to S,

$$\begin{aligned}\mathrm{dl}(P) &\leq \mathrm{dl}(PF^*(G)/F^*(G)) + \mathrm{dl}(P \cap F^*(G))\\ &= \mathrm{dl}(PF^*(G)/F^*(G)) + \mathrm{dl}(P \cap S_1)\\ &\leq \tilde{k}_p(G/F^*(G)) + \tilde{k}_p(S_1) + 7\\ &\leq \tilde{k}_p(G/F^*(G)) + \tilde{k}_p(F^*(G)) + 7\\ &\leq \tilde{k}_p(G) + 7\end{aligned}$$

(the second inequality follows from Lemmas 2.6, 2.7, 2.5 and 2.9).

Hence, $t > 7$. We remark that, since $t > 7$ and p divides $|S|$, there are at least $t\tilde{k}_p(S) \geq \tilde{k}_p(S)+7$ orbits of non-trivial p-elements of $F^*(G)$ under the action of $\mathrm{Aut}(G)$. By the minimality, we have that

$$\mathrm{dl}(PF^*(G)/F^*(G)) \leq \tilde{k}_p(G/F^*(G)) + 7$$

and

$$\mathrm{dl}(P \cap F^*(G)) = \mathrm{dl}(P \cap S_1) \leq \tilde{k}_p(S_1) + 7 \leq \tilde{k}_p(F^*(G)).$$

Hence, it follows from Lemma 2.1 that $\mathrm{dl}(P) \leq \tilde{k}_p(G) + 7$, against the assumption that G is a counterexample. This contradiction completes the proof of Theorem B. □

References

[1] R. Carter, Simple groups of Lie type, John Wiley & Sons, London, 1989.
[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups, Clarendon Press, Oxford, 1985.
[3] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1967.
[4] T. M. Keller, Orbit sizes in finite group actions, preprint.

Departament d'Àlgebra, Universitat de València 46100 Burjassot. València. SPAIN

E-mail address: mtbmoqua@lg.ehu.es

Departamento de Matemáticas Facultad de Ciencias Universidad del País Vasco 48080 Bilbao. SPAIN

E-mail address: mtpsagoj@lg.ehu.es

Departament of Mathematics University of Florida Gainesville FL 32611 USA

E-mail address: turull@math.ufl.edu