BOUNDING THE NUMBER OF CLASSES OF A FINITE GROUP IN TERMS OF A PRIME

ATTILA MARÓTI AND IULIAN I. SIMION

Abstract. Héthelyi and Külshammer showed that the number of conjugacy classes $k(G)$ of any solvable finite group G whose order is divisible by the square of a prime p is at least $(49p+1)/60$. Here an asymptotic generalization of this result is established. It is proved that there exists a constant $c > 0$ such that for any finite group G whose order is divisible by the square of a prime p we have $k(G) \geq cp$.

1. Introduction

Let $k(G)$ denote the number of conjugacy classes of a finite group G. This is also the number of complex irreducible characters of G. Bounding $k(G)$ is a fundamental problem in group and representation theory.

Let G be a finite group and p a prime divisor of the order $|G|$ of G. In this paper we discuss lower bounds for $k(G)$ only in terms of p.

Pyber observed that results of Brauer [1] imply that G contains at least $2\sqrt{p-1}$ conjugacy classes provided that p^2 does not divide $|G|$. Building on works of Héthelyi and Külshammer [8], Malle [17], Keller [12], Héthelyi, Horváth, Keller and Maróti [7], it was shown in [19] that $k(G) \geq 2\sqrt{p-1}$ for any finite group G and any prime p dividing $|G|$, with equality if and only if $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $C_G(C_p) = C_p$.

The objective of the current paper is to provide a stronger lower bound for $k(G)$ in case p^2 divides $|G|$. Héthelyi and Külshammer [9] showed that for any finite solvable group G and any prime p such that p^2 divides $|G|$, the number of conjugacy classes of G is at least $(49p + 1)/60$. This bound is sharp [9] for infinitely many primes p, however it does not generalize [8] to arbitrary finite groups since there are infinitely many non-solvable groups G and primes p with $k(G) = 0.55p - 0.05$.

The main result of this paper is the following.

Theorem 1.1. *There exists a constant $c > 0$ such that for any finite group G whose order is divisible by the square of a prime p we have $k(G) \geq cp$.*

Questions of Pyber and the papers [8] and [9] of Héthelyi and Külshammer motivated our result.

Date: March 11, 2020.

2010 *Mathematics Subject Classification.* 20B05, 20C99, 20C33 (20C34, 20H30).

Key words and phrases. finite linear group, finite simple group.

The work of the first author leading to this application has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 741420). The first author was supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K132951 and No. K115799 and by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

Let B be a p-block of a finite group G and let D be a defect group of B. The number $k(B)$ of complex irreducible characters of G associated to the block B is a lower bound for $k(G)$. A recent result of Otokita [20, Corollary 4] states that $k(B) \geq (p^m + p - 2)/(p-1)$ where p^m denotes the exponent of the center of D.

Finally, note that Kovács and Leedham-Green [14] have constructed, for every odd prime p, a finite p-group G of order p^p with $k(G) = \frac{1}{2}(p^3 - p^2 + p + 1)$ (see also [21]).

2. Affine groups

The purpose of this section is to prove Proposition 2.2. For this we need the following lemma. The base of the logarithms in this paper is always 2.

Lemma 2.1. *Let H be a finite group and V be a finite, faithful, completely reducible H-module over a finite field of characteristic p. Assume that H has no composition factor isomorphic to an alternating group of degree larger than $(\log p)^3$ and has no composition factor isomorphic to a simple group of Lie type defined over a field of characteristic p. Put $p^n = |V|$. Then H has an abelian subgroup of index at most $(c_1 \log p)^{7(n-1)}$ for some universal constant $c_1 > 1$.*

Note that once Lemma 2.1 is proved it may be extended by a theorem of Chermak and Delgado [11, Theorem 1.41] as follows. Under the conditions of Lemma 2.1, the group H contains a characteristic abelian subgroup of index at most $(c_1 \log p)^{14(n-1)}$ for some universal constant $c_1 > 1$.

Proof of Lemma 2.1. Assume first that V is a primitive and irreducible H-module. We use the following structure result which is implicit in the proofs of [6] (see for example the proof of [6, Theorem 9.1]). Let F be the largest field such that H embeds in $\Gamma L_F(V)$. Let C be the subgroup of non-zero elements in F. We claim that $|H/(H \cap C)| \leq (c_1 \log p)^{7(n-1)}$ for some universal constant $c_1 > 1$. For this we may assume that $C \leq H$.

Let H_0 be the centralizer of C in H and let R be a normal subgroup of H contained in H_0 minimal with respect to not being contained in C (if such exists). There are two possibilities for R. It is of symplectic type and $|R/Z(R)| = r^{2a}$ for some prime r and integer a such that r divides $|F| - 1$ or R is a central product of t isomorphic quasisimple groups.

Choose a maximal collection $J_1, \ldots, J_m$ of such non-cyclic normal subgroups in H_0 which pairwise commute (if such exist). Let J be the central product of the subgroups $J_1, \ldots, J_m$. Then $H_0/(C \cdot \mathrm{Sol}(J))$ embeds in the direct product of the automorphism groups of $J_i/Z(J_i)$ where $\mathrm{Sol}(J)$ denotes the solvable radical of J. (Note that in the proof of [6, Theorem 9.1] it was falsely asserted that H_0/C embeds in the direct product of the automorphism groups, however this did not affect the proof of [6, Theorem 9.1] nor [6, Theorem 10.1].)

Let W be an irreducible constituent of V for the normal subgroup J of H (provided that J is non-trivial). Since H is primitive on V, it follows that J acts homogeneously on V by Clifford's theorem. Let $E = \mathrm{End}_{FJ}(W)$. Now $W \cong U_1 \otimes \cdots \otimes U_m$ where U_i is an absolutely irreducible EJ_i-module by [13, Lemma 5.5.5]. Notice that E may be viewed as a subfield of $\mathrm{End}_{FJ}(V)$ and since J is normal in H, the multiplicative group of E is normalized by H. Our choice of F implies that $E = F$. If J_i is of symplectic type with $J_i/Z(J_i)$ of order $r_i^{2a_i}$, then $\dim U_i = r_i^{a_i}$. If J_i

is a central product of t isomorphic quasisimple groups $Q_{i,j}$ with $1 \leq j \leq t$, then $U_i \cong U_{i,1} \otimes \cdots \otimes U_{i,t}$ where $U_{i,j}$ is an absolutely irreducible (faithful) $FQ_{i,j}$-module for every j with $1 \leq j \leq t$, by [13, Lemma 5.5.5 and Lemma 2.10.1].

Let $|F| = p^f$ and let $d = \dim_F V$. The product of the orders of all abelian composition factors in any composition series of the factor group H/C is less than $f \cdot d^{2\log d+3} \leq n^{2\log n+4}$ by [6, Theorem 10.1] and its proof. This is at most $(c_2 \log p)^{n-1}$ for some constant $c_2 > 2$. We may now assume that $J \neq 1$ and $n > 1$.

Let $b(X)$ denote the product of the orders of all non-abelian composition factors in any composition series of a finite group X. Since $|H/C| \leq (c_2 \log p)^{n-1} b(H)$, we proceed to bound $b(H)$.

Without loss of generality, assume that $J_1, \ldots, J_k$ are groups of symplectic type with $k \geq 0$ and $|J_i/Z(J_i)| = r_i^{2a_i}$ for some primes r_i and integers a_i, and assume that $J_{k+1}, \ldots, J_m$ are groups not of symplectic type. For each ℓ with $k+1 \leq \ell \leq m$, let J_ℓ be a central product of t_ℓ copies, say $Q_{\ell,1}, \ldots, Q_{\ell,t_\ell}$, of a quasisimple group Q_ℓ. In this case $U_\ell \cong U_{\ell,1} \otimes \cdots \otimes U_{\ell,t_\ell}$ where $U_{\ell,j}$ is an irreducible (faithful) $Q_{\ell,j}$-module for every j with $1 \leq j \leq t_\ell$. Using this notation we may write the following.

$$\begin{aligned} n \geq d = \dim V \geq \dim W &= \Big(\prod_{i=1}^{k} \dim U_i\Big) \cdot \Big(\prod_{\ell=k+1}^{m} \dim U_\ell\Big) = \\ &= \Big(\prod_{i=1}^{k} {r_i}^{a_i}\Big) \cdot \Big(\prod_{\ell=k+1}^{m} (\dim U_{\ell,1})^{t_\ell}\Big) \geq \Big(\prod_{i=1}^{k} {r_i}^{a_i}\Big) \cdot 2^{\sum_{\ell=k+1}^{m} t_\ell}. \end{aligned} \tag{1}$$

Since H/H_0 and $C \cdot \mathrm{Sol}(J)$ are solvable, $b(H) = b(H_0/(C \cdot \mathrm{Sol}(J)))$. Recall from the third paragraph of this proof that the group $H_0/(C \cdot \mathrm{Sol}(J))$ embeds in the direct product of the automorphism groups of the $J_i/Z(J_i)$. There exists a chain of subnormal subgroups

$$H_0/(C \cdot \mathrm{Sol}(J)) = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_m = \{C \cdot \mathrm{Sol}(J)\}$$

such that $N_{i-1}/N_i \leq \mathrm{Aut}(J_i/Z(J_i))$ for every i with $1 \leq i \leq m$. These give

$$b(H) \leq \Big(\prod_{i=1}^{k} |N_{i-1}/N_i|\Big) \cdot \Big(\prod_{\ell=k+1}^{m} b(N_{\ell-1}/N_\ell)\Big). \tag{2}$$

Since $\prod_{i=1}^{k} r_i^{a_i} \leq n$ by (1), we have

$$\prod_{i=1}^{k} |N_{i-1}/N_i| < \prod_{i=1}^{k} r_i^{4a_i^2} \leq \prod_{i=1}^{k} n^{4\log(r_i^{a_i})} \leq n^{4\sum_{i=1}^{k} \log(r_i^{a_i})} \leq n^{4\log n}. \tag{3}$$

We see by Schreier's conjecture that for every ℓ with $k+1 \leq \ell \leq m$, we have $b(N_{\ell-1}/N_\ell) \leq |T_\ell| \cdot b(Q_\ell)^{t_\ell}$ where T_ℓ is some permutation group of degree t_ℓ having no composition factor isomorphic to an alternating group of degree larger than $(\log p)^3$. Now $|T_\ell| \leq (2\log p)^{3(t_\ell-1)}$ by [18, Corollary 1.5]. Using the fact that $\sum_{\ell=k+1}^{m} t_\ell \leq \log n$ (see (1)), we have

$$\prod_{\ell=k+1}^{m} b(N_{\ell-1}/N_\ell) \leq (2\log p)^{3(\log n-1)} \cdot \Big(\prod_{\ell=k+1}^{m} b(Q_\ell)^{t_\ell}\Big). \tag{4}$$

It follows by (2), (3) and (4) that

$$b(H) < (c_3 \log p)^{3(n-1)} \cdot \Big(\prod_{\ell=k+1}^{m} b(Q_\ell)^{t_\ell} \Big) \tag{5}$$

for some constant $c_3 > 1$.

Let T be a quasisimple group with $T/Z(T)$ not isomorphic to an alternating group of degree larger than $(\log p)^3$ and not isomorphic to a simple group of Lie type defined over a field of characteristic p. Let U be any finite, faithful FT-module over the finite field F of order p^f. Put $|F|^s = |U|$. We claim that

$$b(T) = |T/Z(T)| < (c_4 \log p)^{3(s-1)} \tag{6}$$

for some universal constant $c_4 > 1$. We use [15]. A consequence of [13, (5.3.2), Corollary 5.3.3 and Theorem 5.3.9] is that if $T/Z(T)$ is a simple group of Lie type in characteristic different from p, then $|T/Z(T)| < (c_4 \log p)^{3(s-1)}$ for some constant $c_4 > 1$. By choosing c_4 to be at least the maximum of the size of the Monster and the largest value of $r!$ for which $r! \geq r^{r-5}$ where r is a positive integer, our bound on $|T/Z(T)|$ extends to the case when $T/Z(T)$ is a sporadic simple group or $T/Z(T)$ is an alternating group of degree r with $r! \geq r^{r-5}$. If $T/Z(T)$ is an alternating group of degree $r \leq (\log p)^3$ such that $r! < r^{r-5}$, then

$$|T/Z(T)| < r! < r^{r-5} \leq (\log p)^{3(r-5)} \leq (\log p)^{3(s-1)}$$

where the last inequality follows from [13, (5.3.2), Corollary 5.3.3 and Proposition 5.3.7]. This proves our claim.

For every ℓ with $k+1 \leq \ell \leq m$, define $s_\ell \geq 2$ by $|U_{\ell,1}| = |F|^{s_\ell}$, that is, $s_\ell = \dim U_{\ell,1}$. Using (6) and (1) we find that

$$\begin{aligned}\prod_{\ell=k+1}^{m} b(Q_\ell)^{t_\ell} < \prod_{\ell=k+1}^{m} (c_4 \log p)^{3(s_\ell - 1)t_\ell} \leq \prod_{\ell=k+1}^{m} (c_4 \log p)^{3(s_\ell^{t_\ell} - 1)} \leq \\ \leq (c_4 \log p)^{3((\sum_{\ell=k+1}^{m} s_\ell^{t_\ell})-1)} \leq (c_4 \log p)^{3((\prod_{\ell=k+1}^{m} s_\ell^{t_\ell})-1)} \leq (c_4 \log p)^{3(n-1)}.\end{aligned} \tag{7}$$

We have $b(H) < (c_3 c_4 \log p)^{6(n-1)}$ by (5) and (7). Thus

$$|H/C| \leq (c_2 \log p)^{n-1} b(H) < (c_2 c_3 c_4 \log p)^{7(n-1)}.$$

Finally, set $c_1 = c_2 c_3 c_4 > 2$.

This finishes the proof of the lemma in case V is a primitive and irreducible H-module.

Let H be a counterexample to the statement of the lemma with $\dim V$ minimal and with c_1 as before. Put $f(p) = (c_1 \log p)^7$.

We claim that V must be an irreducible H-module. For assume that $V = V_1 \oplus V_2$ where V_1 and V_2 are non-trivial (completely reducible) H-modules. Let H_1 be the action of H on V_1 and H_2 be the action of H on V_2. The groups H_1 and H_2 are factor groups of H and thus have no non-abelian composition factor which is not a composition factor of H. The group H may be viewed as a subgroup of $H_1 \times H_2$. Since H is a counterexample with $\dim V$ minimal, there exist an abelian subgroup A_1 in H_1 of index at most $f(p)^{m-1}$ and an abelian subgroup A_2 in H_2 of index at most $f(p)^{n-m-1}$ where $p^m = |V_1|$. The group $A = (A_1 \times A_2) \cap H$ is an abelian subgroup of H. Moreover,

$$|H : A| = |H(A_1 \times A_2)|/|A_1 \times A_2| \leq |H_1 \times H_2|/|A_1 \times A_2| \leq f(p)^{n-2} < f(p)^{n-1}.$$

This is a contradiction. Thus V is an irreducible H-module.

We claim that V cannot be an imprimitive H-module. For let $V = V_1 + \cdots + V_t$ with $t > 1$ be an imprimitivity decomposition for V with each V_i a subspace in V and let N be the normal subgroup of H consisting of all elements leaving every V_i invariant. The group N acts completely reducibly on V and thus also on each V_i by Clifford's theorem. For every i with $1 \leq i \leq t$, let H_i be the action of N on V_i. The group H/N may be viewed as a permutation group of degree t. In particular, H may be viewed as a subgroup of a full wreath product of the form $W = (H_1 \times \cdots \times H_t) : \mathrm{Sym}(t)$. Since H is a counterexample with $\dim V$ minimal, there exists an abelian subgroup A_i in H_i, for every i with $1 \leq i \leq t$, such that $|H_i : A_i| \leq {f(p)}^{(n/t)-1}$. The group $A_1 \times \cdots \times A_t$ is contained in W. Thus $A = (A_1 \times \cdots \times A_t) \cap N$ is an abelian subgroup in H. As before,

$$|N : A| = |N(A_1 \times \cdots \times A_t)|/|A_1 \times \cdots \times A_t| \leq |\prod_{i=1}^{t} H_i|/|\prod_{i=1}^{t} A_i| \leq \leq \prod_{i=1}^{t} |H_i : A_i| \leq \prod_{i=1}^{t} {f(p)}^{(n/t)-1} = {f(p)}^{n-t}. \tag{8}$$

The permutation group H/N of degree t has no composition factor isomorphic to an alternating group of degree larger than ${(\log p)}^3$. It follows that

$$|H/N| \leq {(2 \log p)}^{3(t-1)} < {f(p)}^{t-1} \tag{9}$$

by [18, Corollary 1.5]. We thus have $|H : A| < {f(p)}^{n-t} {f(p)}^{t-1} = {f(p)}^{n-1}$ by (8) and (9). A contradiction.

This finishes the proof of the lemma. □

Let X be a finite group. Denote the number of orbits of $\mathrm{Aut}(X)$ on X by $k^*(X)$. If X acts on a set Y, then denote the number of orbits of X on Y by $n(X, Y)$.

Proposition 2.2. *There exists a universal constant $c_5 > 0$ such that if G is a finite group having an elementary abelian minimal normal subgroup V of p-rank at least 2 and $|G/V|$ is not divisible by p^2, then $k(G) \geq c_5 p$.*

Proof. Since $k(G) \geq k(G/V) + n(G, V) - 1$ by Clifford's theorem, it is sufficient to show that $k(G/V) + n(G, V) \geq c_6 p$ for some universal constant $c_6 > 0$. For this latter claim we may assume that G/V acts faithfully on V, that is, V is a faithful and irreducible $H := G/V$-module. This is because $k(G/V) \geq k(G/C_G(V))$ and $n(G, V) = n(G/C_G(V), V)$.

We may assume that p is sufficiently large.

Every non-abelian (simple) composition factor of H (provided that it exists) has order coprime to p, except possibly one which has order divisible by p (but not by p^2). There are the following possibilities for a non-abelian composition factor S of H: (i) S is an alternating group; (ii) S is a simple group of Lie type in characteristic different from p; (iii) $S \cong \mathrm{PSL}(2, p)$; (iv) S is a sporadic simple group.

Suppose that such a composition factor S exists. We have $k(H) \geq k^*(S)$ by [21, Lemma 2.5]. Since $k^*(\mathrm{PSL}(2, p)) \geq (p-1)/4$, by considering diagonal matrices in $\mathrm{SL}(2, p)$, we may exclude case (iii) by choosing $c_5 < \frac{1}{5}$ (since we are assuming that p is sufficiently large). Let S be an alternating group of degree $r \geq 5$. Since $|\mathrm{Out}(S)| \leq 4$, we have $k^*(S) \geq k(S)/4$. Since S is a normal subgroup of index 2 in the symmetric group of degree r, we have $k(S) \geq \pi(r)/2$ where $\pi(r)$ denotes the number of partitions of r. We thus find that $k^*(S) \geq c_7^{\sqrt{r}}$ for some constant $c_7 > 1$. If $r > (\log p)^3$, then $k^*(S) > p$ for sufficiently large p. Thus we assume that every alternating composition factor of H has degree at most $(\log p)^3$.

The group H contains an abelian subgroup A with $|H : A| < |V|^{o(1)}$ as $p \to \infty$, by Lemma 2.1. Furthermore, $k(H) \geq k(A)/|H : A| = |A|/|H : A|$ by [4, p. 502] and $n(G, V) \geq |V|/|H|$. These give

$$k(H) + n(G, V) \geq \frac{|A|}{|H : A|} + \frac{|V|}{|H|} = \frac{|A|}{|H : A|} + \frac{|V|/|A|}{|H : A|} > \frac{|A| + (|V|/|A|)}{|V|^{o(1)}},$$

as $p \to \infty$. Since the real function $g(x) = x + (|V|/x)$ takes its minimum in the interval $[1, |V|]$ when $x = \sqrt{|V|}$, we find that $k(H) + n(G, V) > 2 \cdot |V|^{(1/2) - o(1)} > p$ for sufficiently large p, unless $|V| = p^2$.

Let $|V| = p^2$. Note that in [9, p. 661 and 662] it is shown that if G is solvable, we have

$$k(G/V) + n(G, V) - 1 \geq \frac{49p + 1}{60}.$$

Thus we may assume that G is non-solvable. In this case $H/Z(H)$ is either Alt(5) or Sym(5) (given that case (iii) above cannot occur) by [2, Section XII.260] or [10, Hauptsatz II.8.27]. Also $|Z(H)| < p$ since H is non-solvable by assumption. Thus there exists a constant $c_8 > 0$ such that $k(G) \geq n(G, V) \geq |V|/|H| > c_8 p$.

This finishes the proof of the proposition. □

3. Finite simple groups

In this section we prove Propositions 3.7 and 3.8. We first prove a few preliminary lemmas.

Lemma 3.1. *Let $p, q \in \mathbb{N}^+ \setminus \{1\}$ such that $p \mid q^i + (-1)^a$ and $p \mid q^j + (-1)^b$ for some $i, j \in \mathbb{N}^+$ and some $a, b \in \{0, 1\}$. If $(i, a) \neq (j, b)$ then $p \leq q^{\min\{i,j,|i-j|\}} + 1$.*

Proof. Without loss of generality we may assume that $j \leq i$. By our assumptions, since $p \leq q^j + 1$, it is sufficient to show that $p \leq q^{i-j} + 1$. We have

$$p \mid \left(q^i + (-1)^a\right) - \left(q^j + (-1)^b\right) = q^i - q^j + (-1)^a - (-1)^b.$$

Assume first that $i \neq j$ and $a = b$. Then $p \mid q^i - q^j = q^j(q^{i-j} - 1)$ and so $p \leq q^{i-j} - 1$. If $a \neq b$, then $p \mid \left(q^i + (-1)^a\right) + \left(q^j + (-1)^b\right) = q^i + q^j = q^j(q^{i-j} + 1)$ and so $p \leq q^{i-j} + 1$. □

Lemma 3.2. *Let $P(x)$ be a polynomial admitting a factorisation of the form $P^+(x)P^-(x)$ where*

$$P^+(x) = \prod_{i \in S^+} (x^i + 1)^{k_i^+} \quad \text{and} \quad P^-(x) = \prod_{i \in S^-} (x^i - 1)^{k_i^-}$$

for some sets of integers S^+ and S^- and positive integers k_i^+ and k_i^-. Set $m = \max\{S^+ \cup S^-\}$. Assume that $k_i^+ = k_i^- = 1$ for every index i strictly larger than $m/2$. If p is an odd prime such that $p^2 | P(q)$ for some integer $q \geq 2$, then $p \leq q^{m/2} + 1$.

Proof. Let p be an odd prime such that $p^2 \mid P(q)$ for some positive integer $q \geq 2$. Let $i \in S^+ \cup S^-$ be such that $p \mid q^i + 1$ or $p \mid q^i - 1$. If $i \leq m/2$, the assertion is clear, so assume that $i > m/2$. If $p^2 \mid q^i + 1$ or $p^2 \mid q^i - 1$, then

$$p \leq \sqrt{q^i \pm 1} < q^{i/2} + 1 \leq q^{m/2} + 1.$$

Otherwise there exists $j \in S^+ \cup S^-$ distinct from i such that $p \mid q^j+1$ or $p \mid q^j-1$. By Lemma 3.1, $p \le q^{\min\{i,j,|i-j|\}}+1$. Observe that $\min\{i,j,|i-j|\} \le m/2$. For a proof of this observation we may assume that $i \le j \le m$ and so i or $j-i$ is at most $m/2$. □

S, r	$P^-(q)$	$P^+(q)$
$A_n(q), n$	$\prod_{i=2}^{n+1}(q^i-1)$	1
$B_n(q), C_n(q), n$	$\prod_{i=2}^{n}(q^i-1)$	$\prod_{i=2}^{n}(q^i+1)$
$D_n(q), n$	$\prod_{i=1}^{n}(q^i-1)$	$\prod_{i=1}^{n-1}(q^i+1)$
${}^2D_n(q), n-1$	$\prod_{i=1}^{n-1}(q^i-1)$	$\prod_{i=1}^{n}(q^i+1)$
$G_2(q), 2$	$(q-1)(q^3-1)$	$(q+1)(q^3+1)$
$F_4(q), 4$	$(q-1)(q^3-1)^2(q^4-1)$	$(q+1)(q^3+1)^2(q^4+1)$ $\cdot(q^6+1)$
$E_6(q), 6$	$(q-1)^2(q^3-1)^3(q^5-1)$	$(q+1)^2(q^2+1)(q^3+1)^3$ $\cdot(q^4+1)(q^6+1)$
$E_7(q), 7$	$(q-1)^2(q^3-1)^2(q^5-1)$ $(q^7-1)(q^9-1)$	$(q+1)^2(q^2+1)(q^3+1)^2$ $\cdot(q^4+1)(q^5+1)(q^6+1)$ $\cdot(q^7+1)(q^9+1)$
$E_8(q), 8$	$(q-1)^2(q^3-1)^2(q^5-1)$ $\cdot(q^7-1)(q^9-1)(q^{15}-1)$	$(q+1)^2(q^2+1)(q^3+1)^2$ $\cdot(q^4+1)(q^5+1)(q^6+1)^2$ $\cdot(q^7+1)(q^9+1)(q^{10}+1)$ $\cdot(q^{12}+1)(q^{15}+1)$

TABLE 1.

Lemma 3.3. *Let S be a finite simple group of Lie type of Lie rank r defined over a field of size q as in Table 1. If p is an odd prime such that $p \nmid q$ and $p^2 \mid |S|$, then $p \le q^{(r+1)/2}+1$ if $r > 8$ and $p \le q^{r-\frac{1}{2}}+1$ if $r \le 8$.*

Proof. Observe that $|S|$ divides $P^-(q)P^+(q)$ times a suitable power of q, so $p^2 \mid P^-(q)P^+(q)$. If m is as in the statement of Lemma 3.2, then $p \le q^{m/2}+1$. According to Table 1, $m \le r+1$ if $r > 8$ and $m \le 2r-1$ if $r \le 8$. The result follows. □

S, r	$P(q)$
${}^2B_2(q), 1$	$(q-1)(q-\sqrt{2q}+1)(q+\sqrt{2q}+1)$
${}^2G_2(q), 1$	$(q-1)(q+1)(q-\sqrt{3q}+1)(q+\sqrt{3q}+1)$
${}^2F_4(q), 2$	$(q-1)^2(q+1)(q-\sqrt{2q}+1)(q+\sqrt{2q}+1)$ $\cdot(q^3+1)(q^3-\sqrt{2q^3}+1)(q^3+\sqrt{2q^3}+1)$

TABLE 2.

Lemma 3.4. *Let S be a finite simple group of Lie type of Lie rank r defined over a field of size q as in Table 2. There exists a constant c_{10} such that if p is an odd prime with $p \nmid q$ and $p^2 \mid |S|$, then $p \leq c_{10} \cdot q^{r-\frac{1}{2}}$.*

Proof. Let $P(q)$ be as in Table 2. Notice that $p^2 | P(q)$. If p^2 divides any of the three, four and eight factors in the factorisations of $P(q)$ in Table 2, in the respective three cases, then the statement holds. The statement also holds in case $S = {}^2F_4(q)$ when $p^2 \mid (q-1)^2$. We may assume that there are two distinct factors $P_1(q)$ and $P_2(q)$ in the factorisation of $P(q)$ given in Table 2 which are divisible by p. Hence $p \mid P_1(q) - P_2(q)$.

Let S be ${}^2B_2(q)$ where $q = 2^{2t+1}$. In this case $|P_1(q) - P_2(q)| \leq 2\sqrt{2q}$. Similarly, if S is ${}^2G_2(q)$, then $p \leq 2\sqrt{3q}$.

Let S be ${}^2F_4(q)$ where $q = 2^{2t+1}$. Assume first that $P_1(q)$ and $P_2(q)$ have the same degree. In this case $|P_1(q) - P_2(q)| \leq 2\sqrt{2q^3}$. Otherwise p divides a factor of degree 1, and so $p \leq q + \sqrt{2q} + 1$. In any case the result follows. □

S, r	$P(q)$
${}^3D_4(q), 2$	$(q-1)^2(q+1)(q^2+q+1)(q^3+1)(q^8+q^4+1)$
${}^2E_6(q), 4$	$(q^2-1)(q^3-1)^2(q^3+1)^2(q^4-1)(q^4+1)(q^5+1)(q^6+1)(q^9+1)$
${}^2A_{n-1}(q), [n/2]$	$\prod_{\substack{i=2 \\ i \text{ even}}}^{n} (q^i - 1) \prod_{\substack{i=3 \\ i \text{ odd}}}^{n} (q^i + 1)$

TABLE 3.

Lemma 3.5. *Let S and r be as in Table 3. Then both $k({}^3D_4(q))$ and $k({}^2E_6(q))$ are at least $c_{11} \cdot q^{r+2}$ for some constant $c_{11} > 0$. We also have*

$$k({}^2A_{n-1}(q)) \geq q^{2r-1} / \min\{2r+1, q+1\}.$$

Proof. See [16] and [5, Corollary 3.11]. □

Lemma 3.6. *Let S be a finite simple group of Lie type of Lie rank r defined over a field of size q as in Table 3. There exists a constant c_{12} such that if p is an odd prime with $p \nmid q$ and $p^2 \mid |S|$, then $p \leq c_{12} \cdot q^{r+1}$.*

Proof. First let S be ${}^3D_4(q)$. If p divides a factor of $P(q)$ as in Table 3 of degree at most 3, then the claim is clear. Otherwise,

$$p^2 \mid q^8 + q^4 + 1 = \frac{q^{12}-1}{q^4-1} = \frac{(q^6-1)(q^6+1)}{q^4-1}.$$

Since p is an odd prime and $p^2 \mid (q^6-1)(q^6+1)$, we have $p^2 \leq q^6+1$. Next, let S be ${}^2E_6(q)$. If p divides a factor of $P(q)$ in Table 3 of degree at most 5, then the claim follows. Thus we may assume that $p^2 | (q^6+1)(q^9+1)$. By Lemma 3.2, $p \leq q^{4.5}+1$.

Finally, let S be ${}^2A_{n-1}(q)$. In this case $p \leq q^{r+\frac{1}{2}} + 1$, by Lemma 3.2. □

Let $\mathrm{M}(S)$ denote the Schur multiplier of a non-abelian finite simple group S.

Proposition 3.7. *There exists a constant $c_9 > 0$ such that $k^*(S) \geq c_9 p$ for any non-abelian finite simple group S and any prime p such that $p^2 \mid |S|$ or $p \mid |\mathrm{Out}(S)|$ or $p \mid |\mathrm{M}(S)|$.*

Proof. We may assume that S and p are sufficiently large. In particular, we may ignore sporadic simple groups and small alternating groups, and we may assume that p is odd.

Let S be an alternating group $\mathrm{Alt}(r)$. Since p is odd, p^2 must divide $|S|$, and so $p \leq r$. Since there are $[r/3]$ conjugacy classes of elements of order 3 in $\mathrm{Sym}(r)$, we have $[r/3] \leq k^*(\mathrm{Alt}(r))$, for $r \geq 7$. The constant c_9 can be chosen such that $[r/3] \geq c_9 r$.

Let S be a finite simple group of Lie type of Lie rank r defined over the field of size $q = \ell^f$ for some prime ℓ and positive integer f. We have

$$k^*(S) \geq \frac{q^r}{|\mathrm{M}(S)| \cdot |\mathrm{Out}(S)|}$$

by [17, p. 657]. Since both $|\mathrm{Out}(S)|$ and $|\mathrm{M}(S)|$ are at most $c_{13} \cdot \min\{r, q\} \cdot f$ for some constant c_{13}, we find that

$$k^*(S) \geq \frac{q^r}{(c_{13} \cdot \min\{r, q\} \cdot f)^2}. \tag{10}$$

From this it follows that if $p \mid q$, then $k^*(S) \geq c_{14} \cdot p$ for some constant $c_{14} > 0$. Thus assume that p does not divide q. Notice that $f \leq \log q$.

Assume first that p^2 does not divide $|S|$. Then $p \leq c_{13} \cdot \min\{r, q\} \cdot \log q$. In order to establish the claim in this case it is sufficient to find a constant $c_{15} > 0$ such that $q^r \geq c_{15} \cdot (c_{13} \cdot \min\{r, q\} \cdot \log q)^3$. For any fixed constant c_{15} this is certainly true for sufficiently large q or sufficiently large r. Thus we may assume that $p^2 \mid |S|$.

Assume first that r is bounded. Let S be as in Tables 1 or 2. By Lemmas 3.3 and 3.4, p is at most $c_{16} \cdot q^{r-\frac{1}{2}}$ for some constant c_{16}. In this case, by (10), it is sufficient to find a constant $c_{17} > 0$ such that

$$q^r \geq c_{17} \cdot (c_{13} \cdot \min\{r, q\} \cdot \log q)^2 \cdot c_{16} \cdot q^{r-\frac{1}{2}}.$$

For any fixed c_{17} this inequality holds apart from at most finitely many pairs (r, q). Next let S be one of the first two groups in Table 3. In this case

$$k^*(S) \geq \frac{c_{18} \cdot q^{r+2}}{(c_{13} \cdot \min\{r, q\} \cdot f)^2}$$

for some constant $c_{18} > 0$, by Lemma 3.5. Also, $p \leq c_{12} \cdot q^{r+1}$ by Lemma 3.6. Again, it is sufficient to find a constant $c_{19} > 0$ such that

$$c_{18} \cdot q^{r+2} \geq c_{19} \cdot (c_{13} \cdot \min\{r, q\} \cdot \log q)^2 \cdot c_{12} \cdot q^{r+1}.$$

But this is possible since r is bounded.

Finally, assume that r is unbounded. Let S be as in Table 1. By Lemma 3.3, p is at most $q^{(r+1)/2} + 1$. Since there exists a constant $c_{20} > 0$ such that

$$q^r \geq c_{20} \cdot (c_{13} \cdot \min\{r, q\} \cdot \log q)^2 \cdot (q^{(r+1)/2} + 1),$$

the lemma follows by (10). The only remaining case is $S = {}^2A_{n-1}(q)$. Here

$$k^*(S) \geq \frac{q^{2r-1}}{\min\{2r+1, q+1\} \cdot (c_{13} \cdot \min\{r, q\} \cdot f)^2}$$

by Lemma 3.5. Also, $p \leq c_{12} \cdot q^{r+1}$ by Lemma 3.6. Again, there exists a constant $c_{21} > 0$ such that

$$q^{2r-1} \geq c_{21} \cdot \min\{2r+1, q+1\} \cdot (c_{13} \cdot \min\{r, q\} \cdot \log q)^2 \cdot c_{12} \cdot q^{r+1}.$$

The proof is complete with c_9 the minimum of c_{14}, c_{15}, c_{17}, c_{19}, c_{20} and c_{21}. □

Proposition 3.8. *There exists a universal positive constant c_{22} such that for every non-abelian finite simple group S and every prime p dividing $|S|$ the inequalities $k(S) \geq c_{22} \cdot |\mathrm{Out}(S)| \cdot \sqrt{p}$ and $k^*(S) \geq k(S)/|\mathrm{Out}(S)|$ hold.*

Proof. The second inequality follows from [21, Lemma 2.6].

Since c_{22} is allowed to be chosen small enough, it may be assumed that S is different from a sporadic group, different from $\mathrm{Alt}(5)$, $\mathrm{Alt}(6)$, and different from $\mathrm{PSL}(2,16)$, $\mathrm{PSL}(2,32)$ and ${}^2B_2(32)$.

Let S be an alternating group $\mathrm{Alt}(r)$ with $r \geq 7$. We have

$$k(S) \geq k^*(\mathrm{Alt}(r)) \geq c_9 r \geq c_9 p$$

from the proof of Proposition 3.7. The claimed inequality holds if c_{22} is chosen to be at most $c_9/2$.

Let S be a finite simple group of Lie type of Lie rank r defined over a field of size q. Malle in [17, p. 657] showed that $k(S) \geq q^r/|\mathrm{M}(S)|$ and

$$\frac{q^r}{|\mathrm{M}(S)|} \geq |\mathrm{Out}(S)| \cdot 2 \cdot \sqrt{p-1} \geq |\mathrm{Out}(S)| \cdot \sqrt{p}$$

for all S except for $\mathrm{PSL}(2,16)$, $\mathrm{PSL}(2,32)$ and ${}^2B_2(32)$. □

4. Proof of Theorem 1.1

Let G be a counterexample to Theorem 1.1 with $c = \min\{c_5, c_9, c_{22}, c_{22}^2/2, 1/2\}$ and $|G|$ minimal.

Lemma 4.1. *Let N be a non-trivial normal subgroup of G. Then p divides $|N|$ and p^2 does not divide $|G/N|$.*

Proof. The number $k(G)$ of complex irreducible characters of G is at least $k(G/N)$, the number of complex irreducible characters of G with N in their kernel. If $|N|$ is not divisible by p, then $|G/N|$ is divisible by p^2, and so $k(G/N) \geq cp$, since $|G/N| < |G|$. □

Let $M = \mathrm{soc}(G)$ be the socle of G which is defined to be the product of all minimal normal subgroups of G. This group M is a direct product of some of the minimal normal subgroups of G by [3, Theorem 4.3A (ii)]. By Lemma 4.1, we may write M in the form $M_1 \times M_2$ where M_1 is a (possibly trivial) elementary abelian p-group and M_2 is a (possibly trivial) direct product of non-abelian finite simple groups.

Lemma 4.2. *The group M_1 is trivial or is cyclic of order p.*

Proof. Assume that p^2 divides $|M_1|$. By Lemma 4.1 and Proposition 2.2, we may assume that every abelian minimal normal subgroup of G is cyclic of order p. Furthermore, by the minimality of G, we may assume that $M = M_1 = C_p \times C_p$. Indeed, since $M = C_p \times \cdots \times C_p \times M_2$, a factor group of G will have order divisible by p^2 unless $M = C_p \times C_p$.

We claim that $k(G) \geq k(G/M) + n(G,M) - 1 \geq p - 1 \geq cp$. For this let $C = C_G(M)$ and $H = G/C$. Since H acts faithfully on M, it is an abelian group of exponent dividing $p-1$. Let H_1 be the kernel of the action of H on the first direct factor C_p of M. Then, since H is abelian, $k(G/M) \geq k(H) = |H|$, and we get

$$k(G/M) + n(G,M) - 1 \geq |H| + n(H/H_1, C_p) \cdot n(H_1, C_p) - 1.$$

Observe that $n(H/H_1, C_p) = 1 + \frac{p-1}{|H/H_1|}$ and $n(H_1, C_p) = 1 + \frac{p-1}{|H_1|}$. Thus

$$|H| + n(H/H_1, C_p) \cdot n(H_1, C_p) - 1 > |H| + \frac{(p-1)^2}{|H|} \geq p - 1.$$

□

Lemma 4.3. *The group G cannot contain a normal subgroup which is a direct product of $t \geq 2$ copies of a non-abelian finite simple group.*

Proof. Let N be a normal subgroup of G which is a direct product of $t \geq 2$ copies of a non-abelian finite simple group S. The prime p divides $|N|$ and therefore $|S|$ by Lemma 4.1. Since $t \geq 2$ we have $p^2 \mid |N|$. On the other hand, by $C_G(N) \cap N = 1$ and by the minimality of G we may assume that $C_G(N) = 1$. We then have

$$N \leq G \leq \mathrm{Aut}(S) \wr \mathrm{Sym}(t).$$

Let $s = k^*(S)$. Choose a representative conjugacy class of S from every $\mathrm{Aut}(S)$-orbit on S. Let these be $C_1, \ldots, C_s$. Put $C = C_{i_1} \cdots C_{i_t}$ where for each j between 1 and t the integer i_j is between 1 and s. Note that C is a conjugacy class of N which can be uniquely labelled by a non-negative integer vector $(r_1, \ldots, r_s)$ where r_i $(1 \leq i \leq s)$ is the number of j such that $i_j = i$ and hence it is contained in a unique conjugacy class of G. Note that the conjugation action of $\mathrm{Aut}(S) \wr \mathrm{Sym}(t)$ on N can only fuse N-classes which carry the same $(r_1, \ldots, r_s)$ label. Hence we have a family of conjugacy classes of G which are uniquely labelled by these vectors. The set of all such vectors is the set of all non-negative integer solutions to the equation $x_1 + \cdots + x_s = t$. Therefore $k(G) \geq \binom{t+s-1}{t} \geq \binom{s+1}{2} = s(s+1)/2$. Since $s \geq c_{22} \cdot \sqrt{p}$ by Proposition 3.8, we have $k(G) > (c_{22}^2/2) \cdot p$. □

The group M_1 is C_p or is trivial and M_2 is trivial or is a direct product of pairwise non-isomorphic non-abelian finite simple groups, by Lemmas 4.2 and 4.3.

Lemma 4.4. *If $M_2 \neq 1$, then M_2 is simple.*

Proof. Assume that the group M_2 is non-trivial and not simple. The minimality of G and Lemma 4.1 imply that $M_2 = S \times F$ where S and F are non-isomorphic non-abelian finite simple groups both of order divisible by p. There are at least $k^*(S) \cdot k^*(F) \geq (c_{22} \cdot \sqrt{p})^2 = c_{22}^2 \cdot p$ conjugacy classes of G contained in M_2 by Proposition 3.8. This is a contradiction. □

Lemma 4.5. *The group G cannot be almost simple.*

Proof. This follows from Proposition 3.7. □

Lemma 4.6. *We must have $M_2 = 1$.*

Proof. Assume for a contradiction that $M_2 \neq 1$. Then M_2 is a non-abelian finite simple group S by Lemma 4.4. Consider the normal subgroup $R = C_G(S) \times S$ of G. The group G/R can be considered as a subgroup of $\mathrm{Out}(S)$. Since $C_G(S)$ is normal in G, it is either trivial or p divides $|C_G(S)|$ by Lemma 4.1. The first possibility cannot occur by Lemma 4.5. Thus p must divide $|C_G(S)|$. On the other hand, p^2 cannot divide $|C_G(S)|$ by the minimality of G. By a result of Brauer [1], $k(C_G(S)) \geq 2\sqrt{p-1}$. By Proposition 3.8, it then follows that

$$k(G) \geq \frac{k(R)}{|\mathrm{Out}(S)|} = \frac{k(C_G(S)) \cdot k(S)}{|\mathrm{Out}(S)|} \geq 2\sqrt{p-1} \cdot c_{22} \cdot \sqrt{p} > c_{22} \cdot p.$$

□

Observe that $M = M_1 = C_p$ by Lemmas 4.2 and 4.6. Put $C = C_G(M)$. Then $|G/C|$ divides $p-1$. Consider a maximal chain of normal subgroups of G from C to 1 containing M. Let K_1 be the smallest group in this chain with the property that p^2 divides $|K_1|$. Let K_2 be the next smaller neighbour of K_1 in this chain. The group M is contained in the center of K_2 but $|K_2/M|$ is not divisible by p. By the Schur-Zassenhaus theorem, $K_2 = M \times K$ for a p'-subgroup K of K_2. Since K is characteristic in K_2 and K_2 is normal in G, the group K is normal in G. This occurs only if $K = 1$ by Lemma 4.1. By the maximality of the chain of normal subgroups of G, the group K_1/M is a direct product of isomorphic simple groups T. Since p^2 divides $|K_1|$, the prime p must divide $|T|$. By the minimality of G, the factor group K_1/M is isomorphic to T.

Lemma 4.7. *The group T cannot be C_p.*

Proof. Assume that T is cyclic of order p. Then $|K_1| = p^2$. Since $k(G) \geq k(G/M)$ and G is a minimal counterexample, we see that $|G/M|$ is not divisible by p^2 but divisible by p. Thus G/K_1 is a p'-group. By the Schur-Zassenhaus theorem, there is a p'-subgroup H of G such that $G = HK_1$. The group $C_H(K_1)$ is centralized by K_1 and it is the kernel of the action of H on the normal subgroup K_1 of G. Thus $C_H(K_1)$ is normalized by $HK_1 = G$. Since H is a p'-group, $C_H(K_1)$ must be trivial by Lemma 4.1. We conclude that H may be considered as an automorphism group of K_1. Since $|K_1| = p^2$, the group H and so G must be solvable. The claim follows by [8]. □

The group T must be a non-abelian simple group by Lemma 4.7 and the fact that p divides $|T|$, see the paragraph before Lemma 4.7. By Lemma 4.6, K_1 is thus perfect and therefore a quasisimple group.

Notice that $k(G)$ is at least $k^*(K_1)$. We claim that $k^*(K_1) \geq k^*(T)$. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be two distinct $\mathrm{Aut}(T)$-orbits in T. Consider $\phi^{-1}(\mathcal{T}_1)$ and $\phi^{-1}(\mathcal{T}_2)$ where ϕ is the natural projection from K_1 to T. Notice that these two sets are disjoint and $\mathrm{Aut}(K_1)$-invariant. This proves the claim.

The following lemma completes the proof of Theorem 1.1.

Lemma 4.8. *Let T be a non-abelian finite simple group. Let p be a prime divisor of $|T|$ such that p divides the size of the Schur multiplier of T. Then $k^*(T) \geq c_9 p$.*

Proof. This follows from Proposition 3.7. □

Acknowledgement

The authors thank Hung Ngoc Nguyen for a remark on Section 4 and the anonymous referee for a careful reading of the draft.

References

[1] Brauer, R. On groups whose order contains a prime number to the first power. *I. Amer. J. Math.* **64**, (1942), 401–420.
[2] Dickson, L. E. Linear groups: With an exposition of the Galois field theory. With an introduction by W. Magnus Dover Publications, Inc., New York 1958.
[3] Dixon, J.D.; Mortimer, B. Permutation groups. Graduate Texts in Mathematics, 163. Springer-Verlag, New York, 1996.

[4] Ernest, J. A. Central intertwining numbers for representations of finite groups. *Trans. Amer. Math. Soc.* **99** (1961), 499–508.
[5] Fulman, J.; Guralnick, R.M. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.* **364** (2012), no. 6, 3023–3070.
[6] Guralnick, R.M., Maróti, A., Pyber, L. Normalizers of primitive permutation groups. *Adv. Math.* **310** (2017), 1017–1063.
[7] Héthelyi, L.; Horváth, E.; Keller, T. M.; Maróti, A. Groups with few conjugacy classes. *Proc. Edinb. Math. Soc.* (2) **54** (2011), no. 2, 423–430.
[8] Héthelyi, L.; Külshammer, B. On the number of conjugacy classes of a finite solvable group. *Bull. London Math. Soc.* **32** (2000), no. 6, 668–672.
[9] Héthelyi, L.; Külshammer, B. On the number of conjugacy classes of a finite solvable group. II. *J. Algebra* **270** (2003), no. 2, 660–669.
[10] Huppert, B. Endliche Gruppen I, Springer-Verlag, Berlin, 1967.
[11] Isaacs, I. M. Finite group theory. Graduate Studies in Mathematics, 92. American Mathematical Society, Providence, RI, 2008.
[12] Keller, T.M. Lower bounds for the number of conjugacy classes of finite groups. *Math. Proc. Cambridge Philos. Soc.* **147** (2009), no. 3, 567–577.
[13] Kleidman, P.; Liebeck, M.W. The subgroup structure of the finite classical groups. (1991)
[14] Kovács, L.G.; Leedham-Green, C.R. Some normally monomial p-groups of maximal class and large derived length. *Quart. J. Math. Oxford Ser.* (2) **37** (1986), no. 145, 49-54.
[15] Landazuri, V.; Seitz, G.M. On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32** (1974), 418–443.
[16] Lübeck, F. `http://www.math.rwth-aachen.de/~Frank.Luebeck`
[17] Malle, G. Fast-einfache Gruppen mit langen Bahnen in absolut irreduzibler Operation. *J. Algebra* **300** (2006), no. 2, 655–672.
[18] Maróti, A. On the orders of primitive groups. *J. Algebra* **258** (2002), no. 2, 631–640.
[19] Maróti, A. A lower bound for the number of conjugacy classes of a finite group. *Adv. Math.* Vol. **290** (2016), 1062–1078.
[20] Otokita, Y. Notes on Loewy series of centers of p-blocks. ArXiv:1806.08029.
[21] Pyber, L. Finite groups have many conjugacy classes. *J. London Math. Soc.* (2) 46 (1992), no. 2, 239–249.

(Attila Maróti) Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Reáltanoda utca 13-15, H-1053, Budapest, Hungary
Email address: `maroti.attila@renyi.mta.hu`

(Iulian I. Simion) Department of Mathematics, 'Babeş-Bolyai' University, str. Ploieşti nr.23-25, 400157 Cluj-Napoca, Romania
Email address: `simion@math.ubbcluj.ro`