Upper Bounds for the Number of Conjugacy Classes of a Finite Group

Martin W. Liebeck

Department of Mathematics, Imperial College, London, SW7 2BZ, United Kingdom

and

László Pyber*

Mathematical Institute of the Hungarian Academy of Sciences, P.O.B. 127, Budapest, H-1364, Hungary

Communicated by Peter M. Neumann

Received November 28, 1996

For a finite group $G$, let $k(G)$ denote the number of conjugacy classes of $G$. We prove that a simple group of Lie type of untwisted rank $l$ over the field of $q$ elements has at most $6q^l$ conjugacy classes. Using this estimate we show that for completely reducible subgroups $G$ of $GL(n, q)$ we have $k(G) \leq q^{ln}$, confirming a conjecture of Kovács and Robinson. For finite groups $G$ with $P^*(G)$ a $p$-group we prove that $k(G) \leq (cp)^n$ where $p^n$ is the order of a Sylow $p$-subgroup of $G$ and $c$ is a constant. For groups with $O_p(G) = 1$ we obtain that $k(G) \leq |G|^n$. This latter result confirms a conjecture of Iranzo, Navarro, and Monasor. We also improve various earlier results concerning conjugacy classes of permutation groups and linear groups. As a by-product we show that any finite group $G$ has a soluble subgroup $S$ and a nilpotent subgroup $N$ such that $k(G) \leq |S|$ and $k(G) \leq |N|^2$.

INTRODUCTION

The aim of this paper is to provide upper bounds of various types for $k(G)$, the number of conjugacy classes of a finite group $G$. Several such results were obtained by Kovács and Robinson in [KR], and we develop some of their themes, as well as proving some of their conjectures.

* The research of the second author was supported by the Hungarian National Foundation for Scientific Research Grant T016389.

0021-8693/97 $25.00
Copyright © 1997 by Academic Press
All rights of reproduction in any form reserved.
Throughout, we make use of the classification of finite simple groups. For this we require bounds for $k(G)$ when $G$ is simple, and our basic result is Theorem 1. In the statement we write $\text{rk}(G)$ for the “untwisted” Lie rank of the finite group $G$ of Lie type—that is, the rank of the corresponding simple algebraic group.

**Theorem 1.** Let $G$ be a finite simple group of Lie type over $\mathbb{F}_q$. If $l = \text{rk}(G)$ then

$$k(G) \leq (6q)^l.$$  

Note that if $\hat{G}$ is the simply connected cover of $G$ then $k(\hat{G})$ is at least $q^l$ unless $G$ is a Suzuki group or a Ree group where it is $q^{l/2}$ [Ca2, 3.7.6]. (This fact is used in [Py1] to obtain a roughly logarithmic lower bound on the number of conjugacy classes of a group of order $g$.)

There is not much that is new or difficult about Theorem 1, but it is a convenient and usable general result, and our proof is uniform and reasonably short. For many types of classical groups $G$, Wall and Macdonald [Wa, M ac] obtain precise values of $k(G)$ as coefficients of certain generating functions (although their groups $G$ are usually not simple), and the values of $k(G)$ for various exceptional simple groups $G$ can be found in the references [CR, Mi1, Shi1, Shi2, Sho, Su1, War].

Our first application of Theorem 1 is the completion of some work in [KR] on conjugacy classes of permutation groups. In [KR, Sect. 1], it is proved that any subgroup $G$ of $S_n$ satisfies $k(G) \leq 5^{n-1}$, 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. We use Theorem 1 to handle this case (see Proposition 1.9), thus completing the proof of

**Theorem 2.** If $G$ is any subgroup of $S_n$, then $k(G) \leq 2^{n-1}$.

Note that if $n$ is a power of 2 then $W = D_8 \wr C_{n/4}$ is a transitive 2-group in $S_n$ with $k(W) > 5^{n/4}/n$.

Using Theorem 1 we also prove the following two “reduction theorems.”

**Theorem 3.** Every finite group $G$ has a soluble subgroup $S$ such that $k(G) \leq |S|$.

By a result of Heineken [He] any finite soluble group $S$ has a nilpotent subgroup $N$ such that $|S| \leq |N|^c$ for some $c < 58/21$. Therefore we also have $k(G) \leq |N|^c$ for some nilpotent subgroup $N$ of $G$.

It would be of interest to decide whether the last assertion holds with $c = 1$. A particularly interesting special case is that of odd order groups. Note that for $G = \text{PSL}(2,q)$, $q$ even, the largest order of a nilpotent subgroup and $k(G)$ are both equal to $q + 1$. 
**Theorem 4.** Let $G$ be a finite group with $O_p(G) = 1$. Then $G$ has a soluble $p'$-subgroup $S$ such that $k(G) \leq |S|^3$.

If $G$ is a completely reducible subgroup of $GL(n, q)$, $q$ a power of $p$, then we have $O_p(G) = 1$. Moreover by [PP, Theorem 1], the order of any $p'$-subgroup of $GL(n, q)$ is less than $q^{3n}$. (Note that by a well-known result of Pálfy and Wolf [Pá, Wo] there is a slightly weaker bound for the order of soluble completely reducible subgroups of $GL(n, q)$.) Hence we obtain the following.

**Corollary 5.** If $G$ is a completely reducible subgroup of $GL(n, q)$ then $k(G) \leq q^{cn}$, where $c \leq 10$.

This confirms a conjecture of Kovacs and Robinson [KR, p. 459] in a somewhat stronger form.

One can use Corollary 5 to extend a result of Arregi and Vera-Lopez [AV] as follows. The proof is given at the end of Section 2.

**Corollary 6.** Fix a prime power $q$. If $G$ is any subgroup of $GL(n, q)$, then $k(G) \leq q^{(1/3 + o(1))n^2}$.

Note that $GL(n, q)$ contains abelian subgroups of order $q^{n^2/4}$.

We also use Corollary 5 to show that “most” primitive permutation groups have a surprisingly small number of conjugacy classes (see Corollary 2.15).

A longstanding problem of Brauer is to prove that whenever $B$ is a block with defect group $D$ of a finite group $G$, then $k(B)$, the number of ordinary irreducible characters in $B$ is at most $|D|$. If $F^*(G)$, the generalised Fitting subgroup of $G$, is a $p'$-group, then the only $p'$-block is the principal $p'$-block and $D$ is a Sylow $p'$-subgroup of $G$. Thus in this case the $k(B)$ problem amounts to showing $k(G) \leq |G|_p$. We prove the following.

**Theorem 7.** Let $G$ be a finite group such that $F^*(G)$ is a $p'$-group and $|G|_p = p^n$. Then $k(G) \leq (cp)^n$, where $c \leq 2^{11}$.

Note that in a recent paper Robinson and Thompson [RT] have provided an affirmative solution to Brauer's problem for $p'$-soluble groups when $p \geq 5^{30}$.

The proof of Theorem 7 relies on the following result, which may be of independent interest. In the statement, $\mathbb{F}_p$ denotes the algebraic closure of $\mathbb{F}_p$, and $\text{Lie}(p')$ denotes the collection of all finite simple groups of Lie type over fields of $p'$-characteristic.

**Theorem 8.** Let $H = S_1 \times \cdots \times S_r$ be a section of $GL_d(\mathbb{F}_p)$, $p$ prime, such that the $S_i$ are simple groups which are either in $\text{Lie}(p')$ or sporadic. Then $|H| \leq c^n$, where $c \leq 2^5$. 
As a consequence of R. Knörr’s work [Kn] on the $k(GV)$ problem Iranzo, Navarro, and Monasor [INM] proved that the inequality $k(G/O_p(G)) \leq |G|_{p'}$ holds for soluble groups and conjectured that the same is true for $p$-soluble groups. We prove the following.

Theorem 9. Let $G$ be a finite group and $p$ a prime. Then $k(G/O_p(G)) \leq |G|_{p'}$.

In [KR, 4.2] it is proved that if $G$ is a finite subgroup of $GL(n, \mathbb{C})$ then every subgroup of $G/F(G)$ has at most $c^n$ conjugacy classes for some very large constant $c$ (which was not explicitly computed). In Section 2 using Theorem 3 we give a very short proof of this, showing that one may take $c = 103$ (see Theorem 2.5). At the end of the paper, we note that this implies [KR, 4.1] (which states that if $G$ is $p$-soluble with $|F^*(G)| = p^r > 1$ then $k(G) \leq (cp^r)$), again with $c = 103$.

The layout of the paper is as follows. Section 1 contains the proofs of Theorems 1 and 2. In Section 2, we prove Theorems 3 and 4, and obtain consequences of these concerning linear groups (Theorem 2.5) and permutation groups (Corollary 2.15). Finally, Section 3 contains the proof of Theorems 7, 8, and 9.

1. ALMOST SIMPLE GROUPS

In this section we establish Theorems 1 and 2. We first prove Theorem 1 in a series of lemmas.

Lemma 1.1. If $G$ is a finite group and $H$ is a subgroup of $G$, then

$$k(H)/|G:H| \leq k(G) \leq |G:H|k(H).$$

If $H$ is a normal subgroup of $G$, then $k(G) \leq k(H)k(G/H)$.

If $p$ is a prime, let $k_p(G)$ be the number of conjugacy classes of $p$-elements in $G$, and $k_p(G)$ the number of classes of $p'$-elements.

Lemma 1.2. Let $G$ be a finite group and $Z$ be a subgroup of $Z(G)$.

(i) Then $k(G/Z) \leq k(G)$.

(ii) If $p$ is a prime and $Z$ is a $p'$-group, then $k_p(G/Z) = k_p(G)$.

Proof. Part (i) is trivial. For (ii) note first that if $gZ$ is a $p$-element in $G/Z$, then $g^{p^r} \in Z$ for some $a$, and hence $g^{p^r} = z^{p^r}$ for some $z \in Z$ (as $Z$ is a $p'$-group). Therefore $gZ = g'Z$ with $g' = gz^{-1}$ a $p$-element. In other words, every $p$-element in $G/Z$ is of the form $uZ$ for some
p-element \( u \in G \). Now if \( u, v \) are \( p \)-elements of \( G \) and \( uZ \) is conjugate in \( G/Z \) to \( vZ \), then \( u^v = vz \) for some \( g \in G \), \( z \in Z \). As \( z \) is a \( p' \)-element commuting with \( v \) we must have \( z = 1 \), hence \( u \) conjugate to \( v \) in \( G \). Part (ii) follows.

In the next result, \( GL^\epsilon_n(q) (\epsilon = \pm) \) stands for the group \( GL_n(q) \) when \( \epsilon = + \) and for \( GU_n(q) \) when \( \epsilon = - \). Likewise \( GO^\epsilon_n(q) (\epsilon = \pm) \) stands for one of the two types of orthogonal group when \( n \) is even (there is of course only one type when \( n \) is odd).

**Lemma 1.3.** Let \( q \) be a power of a prime \( p \), and let \( G \) be one of the groups \( GL^\epsilon_n(q), Sp^\epsilon_n(q), GO^\epsilon_n(q) \). Then \( k^\epsilon(G) \leq f^\epsilon(n) \), where \( f^\epsilon(n) \) is defined as

<table>
<thead>
<tr>
<th>( G )</th>
<th>( f^\epsilon(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( GL^\epsilon_n(q) )</td>
<td>( p(n) )</td>
</tr>
<tr>
<td>( Sp^\epsilon_n(q) )</td>
<td>( p(2n)2^{(2n)^{1/2}} )</td>
</tr>
<tr>
<td>( GO^\epsilon_n(q) )</td>
<td>( p(n)2^{n^{1/2}} )</td>
</tr>
</tbody>
</table>

(where \( p(n) \) is the partition function).

**Proof.** For \( G = GL_n(q) \) this is clear, as a conjugacy class of unipotent elements determines, and is determined by, the partition of \( n \) corresponding to its Jordan canonical form. The same argument works for \( GU_n(q) \) by [Wa, p. 34, Case (A(ii))] (which states that two elements of \( GU_n(q) \) are conjugate in \( GU_n(q) \) if and only if they are conjugate in \( GL_n(q^2) \)).

Now consider \( G = Sp^\epsilon_n(q) \) with \( q \) odd. By [Wa, p. 36], a unipotent element of \( G \) determines a partition of \( 2n \) (corresponding to its Jordan form) in which the number of parts of each odd size is even. Moreover, for each even part size, there are two possibilities for a certain bilinear form associated with the Jordan blocks of this size (the form \( \psi_{2i} \), in the notation of [Wa]). The partition and choice of bilinear forms determine the conjugacy class in \( G \). Since the number of different even sizes of parts in a partition of \( 2n \) cannot exceed \( (2n)^{1/2} \), we conclude that \( k^\epsilon(G) \leq p(2n)2^{(2n)^{1/2}} \) in this case. When \( G = Sp^\epsilon_n(q) \) with \( q \) even, the same conclusion follows by the same argument, this time using [Wa, 3.7.1 and 3.7.2].

Finally, for \( G = GO^\epsilon_n(q) \), the result follows as for \( Sp^\epsilon_n(q) \), using [Wa, p. 38, Case (C(ii))] for \( q \) odd, and [Wa, 3.7.1 and 3.7.2] for \( q \) even.

In the next lemma, \( \hat{\Omega}^\epsilon_n(q) \) denotes the universal orthogonal group (so that if \( Z = Z(\hat{\Omega}^\epsilon_n(q)) \), then \( \hat{\Omega}^\epsilon_n(q)/Z \) is the simple orthogonal group \( P\Omega^\epsilon_n(q) \)).
**Lemma 1.4.** Let $G_0$ be one of the groups $SL_n^+(q)$, $Sp_{2n}(q)$, $\Omega^+(q)$, $q = p^a$. Then $k_p(G_0) \leq f_2(n)$, where $f_2(n)$ is

<table>
<thead>
<tr>
<th>$G_0$</th>
<th>$f_2(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SL_n^+(q)$</td>
<td>$np(n)$</td>
</tr>
<tr>
<td>$Sp_{2n}(q)$</td>
<td>$p(2n)2^{2n^{1/2}}$</td>
</tr>
<tr>
<td>$\Omega^+(q)$</td>
<td>$2(n,2)p(n)2^{n^{1/2}}$</td>
</tr>
</tbody>
</table>

**Proof.** For $G_0 = SL_n^+(q)$, let $G = GL_n^+(q)$ and observe that $G = (G_0 Z(G)) \cdot (n, q - e)$. Hence a unipotent conjugacy class in $G$ splits into at most $(n, q - e)$ classes in $G_0$, and so $k_p(G_0) \leq (n, q - e)k_p(G) \leq np(n)$ by Lemma 1.3.

For $G_0 = \Omega^+(q)$, choose $Z \leq Z(G_0)$ such that $G_0/Z \cong \Omega^+_n(q)$. Since $Z$ is a $p'$-group (where $q$ is a power of the prime $p$), Lemma 1.2 gives $k_p(G_0) = k_p(G_0/Z)$. Then by Lemma 1.3 and the argument of the first paragraph,

$$k_p(G_0/Z) \leq |GO_n^+(q) : \Omega^+_n(q)Z(GO_n^+(q))|f_1(n)$$

$$\leq 2(2, n)f_2(n) = f_2(n).$$

For the remainder of the proof, $\overline{G}$ denotes a simply connected simple algebraic group of rank $l$ over the algebraic closure of $\mathbb{F}_p$, and $\sigma$ is a Frobenius morphism of $\overline{G}$ such that the fixed point group $\overline{G}_\sigma$ is a group of Lie type over $\mathbb{F}_q$ (as $\overline{G}$ is simply connected, $\overline{G}_\sigma$ will be of universal type).

**Lemma 1.5.** We have $k_p(\overline{G}_\sigma) \leq 6^l$.

**Proof.** If $\overline{G}_\sigma$ is a classical group with natural module of dimension $n$, we have $n \leq 2l + 1$, and if $\overline{G}$ is orthogonal we can assume that $l \geq 3$. The result is immediate from Lemma 1.4 when $l \leq 2$, so assume $l \geq 3$. By Lemma 1.4 then, $k_p(\overline{G}_\sigma) \leq 2(2, n)p(2l + 1)2^{(2l+1)1/2}$. This is less than $6^l$, so the result follows in this case.

When $\overline{G}_\sigma$ is an exceptional group, upper bounds for $k_p(\overline{G}_\sigma)$ are

<table>
<thead>
<tr>
<th>$\overline{G}$</th>
<th>Upper bound for $k_p(\overline{G}_\sigma)$</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_8$</td>
<td>201</td>
<td>[M 12]</td>
</tr>
<tr>
<td>$E_7$</td>
<td>119</td>
<td>[M 12]</td>
</tr>
<tr>
<td>$E_6$</td>
<td>46</td>
<td>[M 11]</td>
</tr>
<tr>
<td>$F_4$</td>
<td>35</td>
<td>[Shi1, Shi2, Sho]</td>
</tr>
<tr>
<td>$G_2$</td>
<td>9</td>
<td>[CR, En, EY, War]</td>
</tr>
<tr>
<td>$D_4(\text{with } \overline{G}_\sigma^{-1}D_4(q))$</td>
<td>7</td>
<td>[Sp]</td>
</tr>
<tr>
<td>$B_3(\text{with } \overline{G}_\sigma^{-2}B_3(q))$</td>
<td>3</td>
<td>[Su1]</td>
</tr>
</tbody>
</table>
Note. For $G_2$, the upper bound 46 is not explicitly given in [M i1]; but [M i1, 6.2] gives representatives $u_i$ of the classes of unipotent elements in the algebraic group $G$ and also the groups $C_{G_2}(u_i)/C_{G_2}(u_i)^0$, from which it follows that $\sum_i|C_{G_2}(u_i)/C_{G_2}(u_i)^0| \leq 46$, and this sum is an upper bound for $k_p(G_2)$ by [SS, I, 3.4].

The result follows immediately from the table.

\textbf{Lemmas 1.6.} We have $k_p(G) \leq q^l$.

\textbf{Proof.} This is immediate from [SS, II, 3.13(c)].

\textbf{Lemmas 1.7.} Let $s$ be a semisimple element of $G$. Then

\begin{enumerate}
  \item $C_{G}(s)$ is connected.
  \item $O^r(C_{G}(s))$ is a commuting product of groups of Lie type over extension fields of $\mathbb{F}_q$, the sum of whose ranks is at most $l$.
  \item $k_p(C_{G}(s)) \leq 6^l$.
\end{enumerate}

\textbf{Proof.} Part (i) follows from [SS, II, 3.9], and (ii) from [G L, 14.1]. For (iii), note that by (ii) and Lemma 1.5, $k_p(C_{G}(s)) \leq 6^{l_1} \cdots 6^{l_l}$ with $l_1 + \cdots + l_l \leq 6$. The conclusion follows.

\textbf{Lemmas 1.8.} We have $k(G) \leq 6^l q^l$.

\textbf{Proof.} For $x \in G$, we have $x = x_u x_s$, a product of unique commuting unipotent and semisimple elements $x_u$ and $x_s$, respectively. For $x, y, g \in G$, we have $y = x^g$ if and only if $y_u = x_u^g$ and $y_s = x_s^g$. Hence, if $s_1, \ldots, s_m$ are representatives of the conjugacy classes of semisimple elements of $G$, then

$$k(G) = \sum_i k_p(C_{G}(s_i)),$$

which is at most $6^l q^l$ by Lemmas 1.6 and 1.7 (iii).

We now complete the proof of Theorem 1. Let $G$ be simple of Lie type over $\mathbb{F}_q$. There is a simply connected simple algebraic group $\overline{G}$ with a Frobenius morphism $\sigma$ such that, with a few exceptions, $G = \overline{G}/Z(\overline{G})$ (in the exceptions, $G = Sp(2l)^{(l)}, G_2(2), G_3(3),$ or $^2F_4(2)$ and $\overline{G}, |G| = 2, 2, 3, 2, 3, 2, 2$ or 2). Excluding the exceptions for the moment, we have

$$k(G) \leq k(\overline{G}),$$

(by Lemma 1.2(i))

$$\leq 6^l q^l,$$

(by Lemma 1.8),

as required. For the exceptions, $k(G) < (6q)^l$ (see [A t], for example). This completes the proof of Theorem 1.
Our first application of Theorem 1 is the upper bound promised in the Introduction for almost simple permutation groups, which, together, with [KR, Sec. 1], gives Theorem 2.

**Proposition 1.9.** If \( G \) is an almost simple subgroup of \( S_n \), then \( k(G) \leq 2^{n-1} \).

**Proof.** Let \( G_0 = F^*(G) \), a simple group. If \( G_0 = A_\nu \) with \( \nu \neq 6 \), then \( n \geq \nu \) and \( k(G) \leq 2p(\nu) < 2^{\nu-1} \leq 2^{n-1} \) (where \( p(\nu) \) is the partition function). If \( G_0 = A_6 \) or \( G_0 \) is sporadic the conclusion is easily obtained using [At]; the precise values of \( k(G) \) can be read from the character tables, while the value of \( n - 1 \) is certainly at least the smallest degree of a nontrivial irreducible character, from which it follows that \( k(G) \leq 2^{n-1} \) in all cases.

Now assume that \( G_0 \) is of Lie type over \( F_q \), and that \( G_0 \neq A_n \). Let \( l = \text{rk}(G_0) \), and denote by \( \text{PG}(G_0) \) the smallest degree of a faithful permutation representation of \( G_0 \). Obviously \( n \geq \text{PG}(G_0) \). Lower bounds for \( \text{PG}(G_0) \) can be found in [KL2, Table 5.2A] for \( G_0 \) classical, and in [KL2, Table 5.3A] for \( G_0 \) exceptional. From these tables we see that one of the following holds:

(i) \( \text{PG}(G_0) \geq (q^{l+1} - 1)/(q - 1) \)

(ii) \( G_0 = L_2(7), L_3(11), G_2(4), 2D_4(2), 2F_4(2)^\prime, 2B_2(q) \) or \( 2G_2(q) \).

Consider first case (i). By Theorem 1 and Lemma 1.1, we have \( k(G) \leq (6q)^l |G:G_0| \), and \( |G:G_0| \leq |\text{Out}(G_0)| \), which is at most \( 2(l+1)!q^{-l} \) if \( G_0 \neq D_4^\prime(q) \), and at most \( 24 \log_q q \) if \( G_0 = D_4^\prime(q) \). We now check that

\[
(6q)^l |\text{Out}(G_0)| \leq 2((q^{l+1} - 1)/(q - 1))^{l-1}
\]

except when \( l = 1 \) or \( l = 2, q = 2 \). The conclusion follows, except in these cases. When \( l = 1 \), we have \( G_0 = L_2(q) \), and we may assume \( q \geq 13 \) (otherwise we are in case (ii), covered below); now \( k(G_0) \leq q + 1 \), whence

\[
k(G) \leq (q + 1).2\log_q q < 2^q \leq 2^{n-1}.
\]

And when \( l = 2, q = 2, G_0 = L_3(2), Sp_4(2)^\prime, G_2(2)^\prime \), isomorphic to \( L_2(7) \) (which is under case (ii)), \( A_6 \) or \( U_3(3) \) (already handled).

It remains to deal with the groups in case (ii). From [At] (and [Su1, War] for the Suzuki and Ree groups), we see that in the respective cases listed in (ii),

\[
P(G_0) = 7, 11, 416, 819, 1600, q^2 + 1, \text{ or } q^3 + 1,
\]

while

\[
k(G) \leq 12, 16, 64, 105, 44, (q + 3)\log_q q, \text{ or } (q + 8)\log_q q.
\]

The result follows. \( \blacksquare \)
2. General Bounds

In this section we prove Theorems 3 and 4, and use them to estimate \( k(G) \) for linear groups.

We begin with another consequence of Theorem 1.

**Lemma 2.1.** If \( G \) is a simple group of Lie type in characteristic \( p \), then

\[ k(G) < |G|_p, \]

or

\[ |G|_p < (l+1)^N, \]

where \( l = \text{rk}(G) \). One checks that this only holds in the following cases:

1. \( G = L_3(q) \)
2. \( G = L_3^*(q), q \leq 32 \)
3. \( G = L_3^*(q) \) with \( q = 2, 3, 4, 5 \) (\( n = 4 \))
4. \( G = PSp_6(q), q \leq 5 \), or \( Sp_6(2) \)
5. \( G = PSp_8(2) \)
6. \( G = PSp_6(q) \)

In case (1), it is well known that for \( q \) odd, \( k(G) = (q+5)/2 \), so \( k(G) < q = |G|_p \) except for \( q = 5 \); and for \( q \) even, \( k(G) = q+1 \) as in conclusion (ii). In (2), one checks from [St, p. 230; Enn, p. 29] that

\[ k\left( PGL_5^*(q) \right) \leq (q^2 + q + 2)(3, q - \varepsilon). \]

Hence \( k(G) < q^3 \) except possibly when \( G = L_3(2) \); but in fact \( k(L_3(2)) = 6 < 8 \), giving the conclusion in this case also.

Now consider (3). Formulae for \( k(GL_n^*(q)) \) are given in [Gr] (for \( \varepsilon = + \)) and in [Wa, p. 34] (for \( \varepsilon = - \)); we find easily for all cases \( n \leq 7 \) in (3), that

\[ k(GL_n^*(q)) < q^N(n, q - \varepsilon) = q^{(n-1)/2}(n, q - \varepsilon), \]

giving the conclusion by Lemmas 1.1 and 1.2(i).

For (6), [Su1] gives \( k(2B_2(q)) = q + 3 < q^2. \)
Finally, all the groups $G$ in (4), (5), and (7) can be found in [At], from which we see that $k(G) < |G|_p$. This completes the proof.

In the next lemma, by an *intravariant* subgroup $S$ of a group $G$ we mean that for all automorphisms $\alpha$ of $G$, the subgroup $S^\alpha$ is $G$-conjugate to $S$.

**Lemma 2.2.** Let $G$ be a direct product of isomorphic copies of a non-abelian finite simple group $T$. Then $G$ has an intravariant nilpotent subgroup $H$ such that $|H| \geq k(G)$.

**Proof.** Consider first the case $G = T$. If $T$ has a Sylow $p$-subgroup $P$ for some prime $p$ such that $k(T) \leq |P|$ then we are done.

It is straightforward to see that $A_n \geq 2^{n-\log_2 n}$. By a result of Erdős [Er] we have $p(n) \leq \exp\sqrt{n/2}$. This implies $k(A_n) \leq 2^{p(n)} \leq |A_n|$ for $n \geq 32$. For alternating groups of degree less than 32 and for sporadic groups one can easily check that $k(T) \leq |T|_p$ for some prime $p$ using [At] (usually $p = 2$ will do).

By Lemma 2.1 the same is true for simple groups of Lie type with the exception of $L_2(q)$, $q$ even. In the latter case however $T$ contains an intravariant cyclic subgroup of order $q - 1 = k(T)$. Moreover, Aut$(G)$ permutes the direct factors of $G$ and this implies that $H$ is intravariant in $G$. This completes the proof.

**Lemma 2.3.** Let $G$ be a finite group and let $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1$ be a normal series with each $G_i \triangleleft G$. Let $G_i = G_{i-1}/G_i$. Let $p$ be a fixed prime. Suppose, for each $i$, that $H_i$ is an intravariant soluble $p'$-subgroup of $G_i$. Then $G$ has a soluble $p'$-subgroup $H$ such that $|H| \geq \prod_{i=1}^r |H_i|$.

**Proof.** This is a special case of [Su2, II. 3.5.17].

**Proof of Theorem 3.** Let $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1$ be a chief series of $G$. For each $i$ the chief factor $G_i$ is a direct product of isomorphic simple groups. If $G_i$ is nonabelian we apply Lemma 2.2 to $G_i$ to find an intravariant soluble subgroup $H_i$ such that $k(G_i) \leq |H_i|$. Otherwise set $H_i = G_i$. By Lemma 2.3, $G$ has a soluble subgroup $H$ such that $|H| \geq \prod_{i=1}^r |H_i|$. Using Lemma 1.1 we obtain that $|H| \geq \prod_{i=1}^r k(G_i) \geq k(G)$ as required.

We next use Theorem 3 to prove Theorem 2.5 below, which is an improvement of a result of Kovács and Robinson [KR, 4.2]. In the proof we require the following lemma, which is taken from [Is, 14.16].

**Lemma 2.4.** Let $G$ be a finite subgroup of $GL(n, \mathbb{C})$. Then there exists an abelian $A \triangleleft G$ such that $|B : B \cap A| \leq 12^n$ for every abelian subgroup $B$ of $G$. 
Theorem 2.5. Let $G$ and $A$ be as in Lemma 2.4. Then for every subgroup $H$ of $G/A$ we have $k(H) \leq c^n$, where $c \leq 103$.

Proof. By Theorem 3 it is sufficient to prove that a soluble subgroup $S$ of $G/A$ has order at most $c^n$. The full preimage of $S$ is a soluble subgroup $S'$ of $G$ containing $A$. By a result of Dornhoff [Do, 36.4], a soluble subgroup $S$ of $GL(n, \mathbb{C})$ has an abelian normal subgroup $B$ with $|S : B| \leq 2^{4n/3} \cdot 3^{10n/9} = d^n$. Using Lemma 2.4 we obtain that $|S| \leq |S : B \cap A| = |S : B|/|B : B \cap A| \leq (12d^n)^n \leq 103^n$ as required.

Note that $SL(2, 5)^m \leq GL(2m, \mathbb{C})$. This has $A_5^m$ as a quotient group which shows that in Theorem 2.5 we must have $c \geq \sqrt{5}$.

For the proof of our second reduction theorem (Theorem 4) we need the following result. In the statement, we use the following notation. For integers $q, i \geq 2$, a primitive prime divisor $q_i$ is a prime which divides $q^i - 1$ but does not divide $q^j - 1$ for $1 \leq j < i$ (by [Zs], $q_i$ exists unless $i = 2$ or $(q, i) = (2, 6)$). Also, for a positive integer $l$ and a prime $p$, we denote the $p$-part of $l$ by $l_p$.

Lemma 2.6. Let $G$ be a simple group of Lie type over $\mathbb{F}_q$ in characteristic $p$, not of type $^2B_2, ^2G_2$, or $^2F_4$, and let $l = \text{rk}(G)$. Then $G$ possesses a soluble intravariant $p'$-subgroup $S$ such that

(i) $|S| \geq q^l + 1$, if $G \neq D_4^\epsilon(q)$ ($\epsilon = \pm, l \geq 4$), and

(ii) $|S| \geq (q^l - \epsilon)l_p/(4, q^l - \epsilon)$, if $G = D_4^\epsilon(q)$ ($\epsilon = \pm, l \geq 4$).

Proof. Assume first that $G$ is classical and not unitary. Let $r$ be a primitive prime divisor of $|G|$ as follows

<table>
<thead>
<tr>
<th>$G$</th>
<th>$r$</th>
<th>Exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_{i+1}(q)$</td>
<td>$q_{i+1}$</td>
<td>$l = 1, (l + 1, q) = (6, 2)$</td>
</tr>
<tr>
<td>$PSp_2(q)$, $P\Omega_{2l+1}(q) (l \geq 2)$</td>
<td>$q_{2l}$</td>
<td>$(l, q) = (3, 2)$</td>
</tr>
<tr>
<td>$P\Omega_2(q) (l \geq 4)$</td>
<td>$q_l$</td>
<td>$(l, q) = (6, 2)$</td>
</tr>
<tr>
<td>$P\Omega_2(q) (l \geq 4)$</td>
<td>$q_{2l}$</td>
<td></td>
</tr>
</tbody>
</table>

Exclude the cases in the exceptions column for the moment. Let $R$ be a Sylow $r$-subgroup of $G$, and define

$$S = O_p(\langle N_G(R) \rangle).$$

Clearly $S$ is invariant.

When $G = L_{i+1}(q)$, $S$ normalizes a subgroup generated by a Singer cycle $s$ in $G$ (of order $(q^{i+1} - 1)/(q - 1)(l + 1, q - 1)$), and $N_G(\langle s \rangle)/\langle s \rangle$ is cyclic of order $l + 1$. Hence $|S| \geq (q^{i+1} - 1)/(q - 1) \geq q^l + 1$ (and $S$ is soluble of $p'$-order), as required.

If $G = PSp_2(q)$, then $G$ has a subgroup $PSp_2(q^l)$, and this contains a subgroup of order $q^l + 1$ normalizing $R$. Hence $|S| \geq q^l + 1$, and $S$ is
easily seen to be soluble. Similarly, $D_{2l+1}(q) (q \text{ odd})$ contains a subgroup of index 2 in $GO_2^+(q^2)$, giving $|S| \geq q^l + 1$ in this case also.

Next, if $G = P\Omega_{2l}^+(q^2) (l \geq 4)$, then $G$ has a subgroup $P\Omega_{2l}^+(q)$ of order divisible by $(q^l + 1)/4, q^l + 1$, containing $R$ as a normal subgroup. Hence $|S| \geq (q^l + 1)/_{4}$. If $l$ is odd then $R$ lies in a subgroup of index $(q - 1)/4$ in a subgroup $GL_l(q)/\langle -1 \rangle$ of $G$, and $S$ normalizes a Singer cycle therein, whence $|S| \geq (q^l - 1)/_{4}$. If $l$ is even then $R$ lies in a subgroup of type $O_l^+(q) \times O_l^-(q)$, whence we see that $|S| \geq (q^l/2 + 1)^2$ (and $S$ is soluble) as in the previous paragraph.

For the excluded exceptions $G = L_3(q)$, we take $S$ to be a subgroup of order $q + 1$, while for the remaining exceptions $L_2(2), \text{Sp}_6(2), \Omega_5^+(2)$ we take $S = O_2^+(N_{G}(R))$, where $R$ is a Sylow 7-subgroup of $G$.

To finish the classical case, consider now $G = U_{l+1}^+(q) (l \geq 2)$. Let $R$ be the image in $G$ of the subgroup of all diagonal matrices in $SU_{l+1}^+(q)$, relative to a fixed orthonormal basis of the underlying unitary space. Then $|R| = (q + 1)^l/(q + 1, l + 1)$ and $N_{G}(R)/R \cong S_{l+1}$. There exists $s \in N_{G}(R)$ acting as an $l + 1$-cycle on the orthonormal basis, and having matrix entries $\pm 1$. Define $S = O_{l}^+(\langle R, s \rangle)$. Then $|S| \geq (q + 1)^l > q^l + 1$, and $S$ is invariant under $A\text{ut} G = \langle G, \delta, \phi \rangle$, where $\delta$ is diagonal and $\phi$ is a field automorphism fixing each element of the orthonormal basis (see [KL2, Sect. 2.3]). This completes the proof for $G$ classical.

Now suppose that $G$ is of exceptional type (not $2B_2, 2G_2, 2F_4$, by hypothesis). Let $\mathcal{G}$ be a simple algebraic group over $\overline{\mathbb{F}}_q$ and $\sigma$ a Frobenius morphism of $\mathcal{G}$ such that $G = O^{\sigma}(\mathcal{G})$. If $G$ is of untwisted type, then we see from [Ca1] that there is a $\sigma$-stable maximal torus $T$ of $G$ such that the order of $T = \mathcal{T}_0 \cap G$ is

| $G$ | $|T|$ | Diagram of $T$ in [Ca1] |
|-----|--------|-------------------|
| $E_8(q)$ | $q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$ | $E_8$ |
| $E_7(q)$ | $(q^7 + 1)/(2, q - 1)$ | $E_7(a_1)$ |
| $E_6(q)$ | $(q^6 + q^5 + 1)/(3, q - 1)$ | $E_6(a_1)$ |
| $F_4(q)$ | $(q + 1)^4$ | $A_1$ |
| $G_2(q)$ | $(q + 1)^2$ | $A_1 + \tilde{A}_1$ |

Moreover, $T$ is invariant in $G$ by [LSS, 1.3]. For types $E_8, F_4, G_2$, take $S = T$; as $|S| \geq q^l + 1$, the result holds for these types. Now let $G$ be of type $E_6$ or $E_7$, and take $S = O_{l}^+(N_{G}(T))$. We assert that $|N_{G}(T)/T| = 9$ or 14 (respectively); for in both cases $C_{G}(T)^0 = T$ (as otherwise $C_{G}(T)$ would contain a fundamental $A = SL_2(q)$ by [SS, II, 4.1], whereas $C_{G}(A) = A_1(q)$ or $D_6(q)$ (respectively) does not contain a subgroup of order $|T|$). Hence $N_{G}(T) = N_{G}(T)$, and by [SS, II, 1.8], $N_{G}(T)/T \cong C_w(w)$ (where $w$ is an
element of the Weyl group \( W \) of \( G \) with diagram as above), which has order 9 or 14 [Ca1]. Hence the assertion. Therefore \(|S| \geq q^6 + q^3 + 1 \) or \( q^3 + 1 \). Clearly \( S \) is soluble, so the conclusion follows in the untwisted case.

If \( G = {}^2E_6(q) \), take \( T \) to be a maximal torus of order \((q^6 - q^3 + 1)/(3, q + 1)\) if \( p \neq 3 \), and of order \((q + 1)^6\) if \( p = 3 \); define \( S = O_{_4}(N_G(T)) \) in the first case, \( S = T \) in the second. Then \( S \) is invariant (again by [LSS, 1.3]), \(|S| \geq 3(q^6 - q^3 + 1)\) if \( p \neq 3 \), and \(|S| = (q + 1)^6\) if \( p = 3 \), giving the conclusion.

The final case is \( G = {}^3D_4(q) \). Here take \( S \) to be a maximal torus of order \((q + 1)(q^3 + 1)\) lying in a subgroup \( X = (SL_2(q) \circ SL_2(q^3)) \cdot (2, q - 1) \). There is an element \( \phi \in \text{Aut} \ G \) of order \( 3 \log_p q \) such that \( \text{Aut} \ G = G \langle \phi \rangle \) and \( \phi \) normalizes \( X \). Thus we may choose \( S \) to be normalized by \( \phi \), whence \( S \) is invariant.

**Lemma 2.7.** Let \( G \) be a simple group of Lie type in characteristic \( p \). Then \( G \) has a soluble, invariant \( p' \)-subgroup \( S \) such that \( k(G) < |S|^4 \).

**Proof.** Assume first that \( G \) is not of type \( {}^2B_2, {}^2G_2, {}^2F_4 \), or \( D_7^r \), so by Lemma 2.6, \( G \) has a soluble invariant \( p' \)-subgroup \( S \) such that \(|S| \geq q^l + 1 \), where \( l = \text{rk}(G) \). By Theorem 1, \( k(G) \leq (6q)^l \). The conclusion follows, since for all \( q \) we have \((6q)^l < (q^l + 1)^4 \).

Now let \( G = D_7^\epsilon(q) \) with \( \epsilon = \pm 1 \), \( l \geq 4 \). By Lemma 2.6, \( G \) has a soluble invariant \( p' \)-subgroup \( S \) with \(|S| \geq (q^l - \epsilon)^l/(4, q^l - \epsilon) \). If \( q \) is even or 4\( |l| \), then \(|S| \geq q^l - 1 \), giving the conclusion as \((6q)^l < (q^l - 1)^4 \) for \( q \geq 2, l \geq 4 \). If \( l \geq 9 \) then also \((6q)^l < |S|^4 \) (note that for the “smallest case” \( q = 3, l = 9 \), we have \((18)^9 < ((3^9 - 1)/4)^4 \)). For \( l = 5 \) or 7 we have \(|S| \geq q^l - 1 \) unless \( p = 5 \) or 7, respectively; in these cases we only need to check that \((30)^5 < ((5^5 - 1)/4)^4 \) and \((42)^7 < ((7^7 - 1)/4)^4 \). Finally, when \( l = 6 \) we have \(|S| \geq (q^6 - 1)/2 \), and we need only check that \((18)^6 < ((3^6 - 1)/2)^4 \). To complete the proof, assume that \( G = {}^2B_2(q), {}^2G_2(q), \) or \( {}^2F_4(q) \). In these cases we see from [Su1, War, Shi1] that \( G \) has invariant tori of orders \( q + \sqrt{q} + 1, q + \sqrt{3q} + 1 \) or \( q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1 \), while \( k(G) = q + 3, q + 8, \) or \( q^2 + 4q + 17 \), respectively (22 for \( {}^2F_4(2) \) [At1]). The conclusion follows.

**Lemma 2.8.** Let \( G \) be a simple group and \( p \) a prime. Then \( G \) has a soluble invariant \( p' \)-subgroup \( S \) such that \( k(G) < |S|^4 \).

**Proof.** The case when \( G \) is of Lie type in characteristic \( p \) is settled by Lemma 2.7. If \( G \) is of Lie type in characteristic \( r \neq p \) then our conclusion follows from Lemma 2.1. If \( G = A_k \) then it is easy to see that we can take \( S \) to be a Sylow 2-subgroup or a Sylow 3-subgroup of \( G \). One can also
check using [At] that if $G$ is sporadic then $G$ has Sylow $p$-subgroups $P$ with $|P|^k > k(G)$ for at least two different primes $p$. The proof is complete.

We will use another consequence of Lemma 2.6.

**Lemma 2.9.** Let $G$ be a simple group and $p$ a prime. Then $G$ has a soluble invariant $p'$-subgroup $S$ such that

$$2|\text{Out}(G)|_p \leq |S|.$$

**Proof.** It is easy to see that for alternating groups and sporadic groups we can take $S$ to be a Sylow $r$-subgroup for some prime $r/p$. One can also check that if $G$ is of Lie type over $F_p$ then $2|\text{Out}(G)|_p \leq |S|$ holds and for $G = B_2(q)$ or $L_2(q)$ (q even), we have $2|\text{Out}(G)|_p \leq q$. When the characteristic of $G$ is $r \neq p$ then this gives us $2|\text{Out}(G)|_p \leq |G|$, unless $G = L_2(q)$, $q$ odd. In this case we have $|G| = q = r^l$ and $2|\text{Out}(G)|_p = 4f$. Therefore $2|\text{Out}(G)|_p \leq |G|$, unless $p = 2$ and $G = L_3(3)$ which is soluble.

It remains to consider the case when $G$ has characteristic $r = p$. In this case it is easy to check that $|\text{Out}(G)|_p \leq q$ holds. Let $S$ be a soluble invariant $p'$-subgroup of $G$ of maximal order. Lemma 2.6 and the discussion in the proof of Lemma 2.7 show that we have $2|\text{Out}(G)|_p \leq |S|$ except possibly if $G = B_2(q), G_2(q)$, or $L_2(q)$, $q$ odd. However, in these cases we have $2|\text{Out}(G)|_p \leq 2f \leq q \leq |S|$. The proof is complete.

We now recall some properties of the generalized Fitting subgroup $F^*(G)$ of a finite group $G$. The components of $G$ are its subnormal quasisimple subgroups and the layer $E(G)$ of $G$ is the subgroup generated by its components. The group $E = E(G)/Z(E(G))$ is a direct product of simple groups, say $E = L_1 \times \cdots \times L_l$. The Fitting subgroup is the direct product of the groups $F_i = O_i(G)$ for the primes $p_i$ dividing $|G|$. The generalized Fitting subgroup of $G$ is $F^*(G) = E(G) \cdot F(G)$. It is well known that $Z = C_{F^*(G)}(F^*(G)) = Z(F^*(G))$, and hence $G/Z$ has an embedding into the group $A = \text{Aut}(E(G)) \times \prod \text{Aut}(F_i)$.

**Lemma 2.10.** With the above notation, denote by $p_i^t$ the order of the Frattini factor group $F_i/\Phi(F_i)$.

(i) There is a normal subgroup $B_0$ of $\text{Out}(E(G))$ such that $B_0$ is isomorphic to a subgroup of $\prod_{i=1}^t \text{Out}(L_i)$ and $\text{Out}(E(G))/B_0$ has an embedding into $S_k$.

(ii) For each $i$ there is a normal subgroup $B_i$ of $\text{Out}(F_i)$ such that $B_i$ is a $p_i$-group and $\text{Out}(F_i)/B_i$ has an embedding into $GL(t_i, p_i)$.

**Proof.** This is [Py2, 2.2].
Lemma 2.11. Let $G$ be a finite group with $O_p(G) = 1$.

(i) There exists a soluble intravariant $p'$-subgroup $S$ in $E = L_1 \times \cdots \times L_k$ such that $|\text{Out}(E(G))|_p \leq |S|$.

(ii) $|\text{Aut}(F(G))|_p \leq |F(G)|^{8/5}$.

Proof. There exist intravariant soluble $p'$-subgroups $S_i$ of maximal order in $L_i$ such that $S_i$ is an intravariant soluble $p'$-subgroup of $E$. The order of a $p'$-subgroup of the symmetric group of degree $k$ is less than $2^k$. By Lemmas 2.10(i) and 2.9

$$|\text{Out}(E(G))|_p \leq 2^k \prod_{i=1}^{k} |\text{Out}(L_i)|_p \leq \prod_{i=1}^{k} |S_i| = |S|.$$ 

This proves (i).

By a result of Wolf [Wo1, Theorem 1.6], $|GL(t, p)|_p \leq p^{8t/5}$. Using Lemma 2.10(ii) we obtain part (ii).

Proof of Theorem 4. Suppose $O_p(G) = 1$. Consider a chief series $\hat{G} = \hat{G}_0 \triangleright \cdots \triangleright \hat{G}_r = \mathbf{1}$ of the group $\hat{G} = G/F^*(G)$ and let $G = G_0 \triangleright \cdots \triangleright G_r = F^*(G)$ be the corresponding series of normal subgroups of $G$. Set $G_{r+1} = F(G)$, $G_{r+2} = \mathbf{1}$. Clearly $G_i/G_{i+1} \cong E$. Let $H_i$ be a maximal soluble intravariant $p'$-subgroup of $\overline{G}_i = G_i/G_{i+1}$; note that $H_{r+1} = F(G)$. By Lemma 2.3, $G$ has a soluble $p'$-subgroup $H$ such that $|H| \geq \prod_{i=1}^{r+1} |H_i|$. Using Lemma 2.8 we obtain that $(\prod_{i=1}^{r+1} |H_i|)^5 |H_{r+1}|$ is greater than the product of $k(\overline{G}_i)$ for all $\overline{G}_i$ which are not $p$-groups. By Lemma 2.11 the product of the orders of the $p$-groups among the $\overline{G}_i$ is at most $|H_{r+1}|^{8/5} |H_r|$. Therefore we have $|H|^5 \geq \prod_{i=1}^{r+1} k(\overline{G}_i) \geq k(G)$ as required.

As noted in the Introduction, Theorem 4 implies that if $G$ is an irreducible subgroup of $GL(n, q)$ then $k(G) \leq q^{10n_2}$ (as stated in Corollary 5). As we will see this in turn implies that “most” primitive permutation groups have a surprisingly small number of conjugacy classes (see Corollary 2.15 below). To prove this, we first record some well-known facts about primitive groups.

Lemma 2.12. There is a constant $c_0$ such that whenever $G$ is a primitive subgroup of $S_n$ other than $A_n$ or $S_n$, then either

(i) $G$ is $S_m$ or $A_m$ acting on 2-sets ($n = \binom{m}{2}$), or $G$ is a subgroup of $S_m$ or $S_2$ containing $A^2_m$ ($n = m^2$), or

(ii) $|G| \leq \exp(c_0 n^{1/3} \log n)$.

Proof. This is immediate from [Cam, Theorem 6.1].
In the next lemma, for a group $G$ we denote by $P^i_i(G)$ the smallest degree of a faithful transitive permutation representation of $G$.

**Lemma 2.13.** If $S_1, \ldots, S_r$ are non-abelian simple groups, then

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

**Proof.** This follows from [KL2, 5.2.7(ii)] and the remark after [KL2, 5.2.7].

**Lemma 2.14.** Let $G$ be a primitive subgroup of $S_n$ with non-abelian socle $S$. Then $G$ has a normal subgroup $K$ containing $S$, such that $|K/S| \leq n$ and $G/K$ has an embedding into $S_r$ with $r \leq \log_2 n$.

**Proof.** We know that $S$ is a direct power of a non-abelian simple group, say $S = L'$. By Lemma 2.13, if $P(L)$ denotes the minimal faithful permutation degree of $L$, then $P(L) \leq n$. It follows that $r \leq \log_2 n$. Now $G$ acts on the direct factors of $S$ by conjugation. The kernel $K$ of this action has an embedding into $\text{Aut}(L')$, and $G/K \leq S_r$. It is easily checked that $|\text{Out}(L)| \leq P(L)$ (see (i), (ii) in the proof of Proposition 1.9), and this gives us $|K/S| \leq n$ as required.

**Corollary 2.15.** Let $G$ be a primitive subgroup of $S_n$ with socle $S = L'$, $L$ simple.

(i) For sufficiently large $n$, we have $k(G) \leq k(S_n)$ and $k(S_n) = (1 + o(1)) \exp (2\pi \sqrt{n} / \sqrt{3}) / 4n\sqrt{3}$.

(ii) If $L$ is not an alternating group then $k(G) \leq n^{11}$.

**Proof.** The asymptotic estimate for $k(S_n) = p(n)$ is a classical result of Hardy and Ramanujan. An asymptotic estimate for $k(A_n)$ appears in [DET]. This shows that $k(A_n)$ is roughly half of $k(S_n)$. It is clear that if $G$ is as in Lemma 2.12(i) then $k(G) \leq \exp(c_n \sqrt{n^{1/2}})$ and in case (ii) of Lemma 2.12 we have $k(G) \leq |G| \leq \exp(c_n \sqrt{n^{1/2}} \log n)$. Part (i) of our statement follows.

To prove (ii) first note that if $S$ is non-abelian then by Theorem 2 and Lemma 2.14 we have $k(G/S) \leq n^{2\sqrt{n}} \leq n^2$. On the other hand using Theorem 1 and the bounds for the minimum degree $P(L)$ listed in the proof of Proposition 1.9 it is straightforward to see that $k(L) \leq P(L)^4$ holds when $L$ is of Lie type; and the same holds for $L$ sporadic by [At]. It follows that if $S$ is non-abelian then we have $k(G) \leq n^6$. If $S$ is abelian of order $p'$ then $G/S$ may be identified with an irreducible subgroup of $GL(r, p)$. Therefore in this case, by Corollary 5, $k(G) \leq p^{11r} = n^{11}$. The proof is complete.
In view of the above estimates it might be possible that there is a polynomial time algorithm for finding representatives of the conjugacy classes of primitive groups $G$ when $L$ is not an alternating group.

We end this section with an estimate for the number of conjugacy classes of arbitrary subgroups of $GL(n, q)$.

**Proof of Corollary 6.** If $G$ is any subgroup of $GL(n, q)$ ($q = p^s$), then $G/O_p(G)$ may be viewed as a completely reducible linear group acting on the direct sum of the composition factors of the natural module for $G$. By Corollary 5, $k(G/O_p(G)) \leq q^{10n}$ holds. By a result of Arregi and Vera-Lopez [AV, p. 2] for any $p$-subgroup $P$ of $GL(n, q)$ we have $k(P) \leq q^{(1/3+o(1))n^3}$. Hence $k(G) \leq k(O_p(G))k(G/O_p(G)) \leq q^{(1/3+o(1))n^7}$ as required. 

### 3. ON THE $k(B)$ PROBLEM

The aim of this section is to prove Theorems 7, 8, and 9. First we will prove Theorem 8.

For a simple group $S$ and a prime $p$, define

$$R_p(S) = \min \{ n : S \leq PGL_n(F_p) \},$$

$$M_p(S) = \min \{ n : S \text{ is a section of } PGL_n(F_p) \}.$$  

Clearly $R_p(S) \geq M_p(S)$; analysis of precisely when the reverse inequality holds is the subject of [FT], a project completed in [KL1]. The following lemma is an immediate consequence of [FT, Sect. 3; KL1, Theorem 3]. Recall that $\text{Lie}(p')$ denotes the collection of all simple groups of Lie type over fields of $p'$-characteristic.

**Lemma 3.1.** Let $p$ be a prime.

(i) If $S$ is a sporadic group, then $M_p(S) = R_p(S)$.

(ii) If $S = S_i(r)$, a group in $\text{Lie}(p')$ over $F_r$ of (untwisted) rank $l$, then

$$M_p(S) \geq \min \{ R_p(S), r^l \}.$$  

**Corollary 3.2.** There is a constant $c$ (e.g., $c = 2^5$ will do) such that if $S \in \text{Lie}(p')$ or $S$ is sporadic, then $|S| < c^{M_p(S)}$.

**Proof.** Assume first that $S \in \text{Lie}(p')$, and let $S = S_i(r)$ as in Lemma 1(ii). Lower bounds for $R_p(S)$ are given by [LS], from which we find that $R_p(S) \geq (r^l - 1)/2$ except when $S = L_2(9), L_3(4), \text{ or } ^2B_2(r)$ (in the latter case, $R_p(S) \geq \sqrt{r}/2(r - 1)$). Exclude these exceptional cases for the mo-
ment. Then $M_p(S) \geq (r' - 1)/2$ by Lemma 3.1(ii). Clearly there is a constant $c$ such that $|S_t(r)|^{c(r' - 1)/2}$ for all groups $S_t(r) \in \text{Lie}(p')$. Simple calculations with the orders of simple groups show that $c = 2^5$ works. For the excluded cases, $c = 2^5$ clearly works also.

Finally, when $S$ is sporadic, we have $M_p(S) = R_p(S)$ by Lemma 3.1(i). Lower bounds for $R_p(S)$ are given in [KL2, 5.3.8]. Comparing these with the orders of the sporadic groups, we find that $|S| < c^{R_p(S)}$ (where $c = 2^5$—indeed this works for much smaller $c$, the best being about $2^{11/3}$ for the group $Suz < PGL_{12}$).

**Proof of Theorem 8.** We prove Theorem 8 by induction on $r$. The case $r = 1$ follows from Corollary 3.2, so assume $r \geq 2$.

Let $S_1, \ldots, S_r$ be simple groups, each either in $\text{Lie}(p')$ or sporadic, and suppose $\Pi S_i$ is a section of $\text{GL}_n(\mathbb{F}_p) = \text{GL}(V)$; assume $n$ is minimal for this. Let $\Pi S_i = H/K$, where $H \leq \text{GL}(V)$ and $K \triangleleft H$, and take $H$ to be minimal for this.

Clearly $H$ is perfect. Observe also that $K$ is nilpotent: for if $M$ is a maximal subgroup of $H$ then $MK < H$ (by minimality of $H$), hence $MK = M$ and so $K \leq M$. Thus $K = \Phi(H)$, the Frattini subgroup of $H$, and hence $K$ is nilpotent. For each $i$, let $H_i$ be the subgroup of $H$ containing $K$ such that $H_i/K = S_i$.

Suppose first that $V \downarrow H$ (the restriction of $V$ to $H$) is irreducible. By Clifford's theorem, we have

$$V \downarrow K = W_1 \oplus \cdots \oplus W_a,$$

a sum of $H$-conjugate homogeneous components $W_i$. Set $b = \dim W_1$. Let $J = \{i : H_i \leq H_{W_i}\}$. Observe that for $i \in J$, we have $H_i \not\leq C_H(W_i)$ (otherwise $H_i$ would act trivially on $V$); hence $\Pi_{i \in J} S_i$ is a section of $H/W_i = H/C_H(W_i)$. Assume $J \neq \{1, \ldots, r\}$. Then by induction, $|\Pi_{i \in J} S_i| < c^b$. On the other hand, the homogeneous components $W_i$ are permuted faithfully and transitively by $\Pi_{i \in J} S_i$, so by Lemma 2.13, we have $a \geq \prod_{i \in J} m_i$, where $m_i = P^i_j(S_i)$. By Corollary 3.2, we have $|S_i| < c^{M^i_j(S_i)}$, so $|S_i| < c^{m_i}$, (since $P^i_j(S_i) \geq M_p(S_i)$). Hence if $b > 1$, then

$$c^n = c^{b^a} \geq c^b c^{a} \geq c^b \prod_{i \in J} c^{m_i} > \prod_{i = 1}^r |S_i|,$$

as in the conclusion of the theorem. And if $b = 1$, then $J = \emptyset$ and $c^n = c^a > \prod |S_i|$ similarly. Hence we may assume that $J = \{1, \ldots, r\}$; in other words, $V \downarrow K = W_1$ is a homogeneous $K$-module.

If $K$ is abelian, then $K$ consists of scalars, hence $K \leq Z(H)$. Then $H$ is a commuting product of quasisimple groups $H_i$, and by [KL2, 5.5.7] we
have \( n \geq \prod R^i_p(S_i) \), which gives the conclusion using Corollary 3.2. Hence we may also assume that \( K \) is non-abelian.

Suppose that \( V \downarrow K \) is reducible. Then there is a tensor decomposition \( V = V_1 \otimes V_2 \) with \( \dim V_1, \dim V_2 > 1 \), such that \( K \leq GL(V_1) \otimes GL(V_2) \), embedded in the obvious way in \( GL(V_1) \otimes GL(V_2) < GL(V) \), with \( K \) irreducible in \( GL(V_1) \) (see [KL2, Remark after 4.4.3]). By [KL2, 4.4.3(ii)], we have \( H \leq N_{GL(V)}(K) \leq GL(V_1) \otimes GL(V_2) \). By the minimality of \( n \), neither \( GL(V_1) \) nor \( GL(V_2) \) has \( \prod S_i \) as a section. Hence there is a proper non-empty subset \( J \) of \( \{1, \ldots, r\} \) such that \( GL(V_1), GL(V_2) \) have sections \( \prod_{i \in J} S_i, \prod_{i \notin J} S_i \) (respectively), and the conclusion follows by induction.

Thus we may suppose that \( V \downarrow K \) is irreducible. Recall that \( K \) is a nilpotent. Choose a prime \( q \) such that \( K \) has a non-abelian Sylow \( q \)-subgroup \( Q \). Then \( Q \leq H \), and as above we may assume that \( V \downarrow Q \) is irreducible. If \( A \) is a characteristic abelian subgroup of \( Q \) then \( A \leq H \), and again as above, we obtain the conclusion unless \( A \) consists of scalars.

Hence we may suppose that every characteristic abelian subgroup of \( Q \) is cyclic; in other words, \( Q \) is a \( q \)-group of symplectic type. The structure of such groups is known, by a well known result of Philip Hall (see [As, 23.9]). In particular, \( Q \) has a characteristic irreducible subgroup \( Q_0 \) which is either an extraspecial group \( q^{1+2m} \), or of the form \( Z_q \otimes 2^{1+2m} \) (with \( q = 2 \)). Then \( n = q^m \) and \( H \leq N_{GL(V)}(Q_0) \). Now \( H/K \) is isomorphic to a subgroup of \( Aut(Q_0)/Inn(Q_0) \), hence to subgroup of \( PSp_{2m}(q) \). Therefore

\[
\prod_{i \in L} S_i \leq |PSp_{2m}(q)| < q^{2m^2+m} < c^q^m = c^n,
\]

giving the conclusion of the theorem.

This completes the proof under the assumption that \( V \downarrow H \) is irreducible. Now suppose \( V \) is a reducible \( H \)-module, and let \( W \) be an irreducible \( H \)-submodule. By the minimality of \( n \), neither \( GL(W) \) nor \( GL(V/W) \) has a section \( \prod S_i \). Hence there is a proper non-empty subset \( L \) of \( \{1, \ldots, r\} \) such that \( H^W = H/C_H(W) \) has a section \( \prod_{i \in L} S_i \), and \( C_H(W)^{V/W} = C_H(W)/(C_H(W) \cap C_H(V/W)) \) has a section \( \prod_{i \in L} S_i \) (note that \( (C_H(W) \cap C_H(V/W)) \) is a \( p \)-group). Writing \( b = \dim W \), we have by induction

\[
\prod_{i \in L} S_i < c^b, \quad \prod_{i \in L} S_i < c^{n-b},
\]

giving the result.

This completes the proof of Theorem 8. \( \blacksquare \)
**Corollary 3.3.** Let \( p \) be a prime and let \( S_1, \ldots, S_r \) be non-abelian simple groups.

(i) If \( S_1 \times \cdots \times S_r \) is a section of \( GL_n(F_p) \), then \( r \leq \lfloor n/2 \rfloor \).

(ii) If each \( S_i \) is an alternating group of degree \( a_i \), then \( \Sigma_1^r a_i \leq 3n \).

**Proof.** If \( r = 1 \) then (i) obviously holds. The induction process used in the proof of Theorem 8 can be used to prove the general case. One only has to observe that when \( n = q^m \) and \( H = S_1 \times \cdots \times S_r \) is a subgroup of \( PSp_{2m}(q) \) then \( H \) is a section of \( GL_{2n}(F_q) \) which implies \( r \leq m < \lfloor n/2 \rfloor \) by induction. Part (ii) can be proved in the same way, this time using [FT; KL2, 5.3.7] to establish the case \( r = 1 \).

In the proof of Theorem 7 it is convenient to use the following similar result for soluble groups, taken from [KR, 3.1].

**Lemma 3.4.** Let \( G \) be a finite soluble group, \( p \) a prime. Suppose that \( |F(G)| = p^r \) where \( r \) is a positive integer. Then \( k(G) \leq 3^{-r}p^r \).

**Proof of Theorem 7.** We have \( F^*(G) = F(G) \). Let \( U = \Phi(O_p(G)) \). Then \( F(G/U) = F(G)/U \) and \( k(G) \leq k(U)k(G/U) \leq \frac{|U|}{|k(G/U)|} \), so it suffices to consider the case where \( U = 1 \) and hence \( G^* = G/F(G) \) acts faithfully as a group of linear transformations of the elementary abelian \( p \)-group \( F(G) \). Set \( |F(G)| = p^r \).

Consider the soluble radical \( O_s(G) \) of \( G \). Then \( F(O_s(G)) = F(G) \), so by Lemma 3.4 we have \( k(O_s(G)) \leq (3p)^r \).

The socle \( S \) of \( G/O_s(G) \) is a direct product of simple groups, say \( S = L_1 \times \cdots \times L_r \). Moreover \( G = G/O_s(G) \) permutes the simple groups \( L_i \). The kernel \( K \) of this action is a subgroup of \( \text{Aut}(L_1) \times \cdots \times \text{Aut}(L_r) \) and \( G/K \) is a subgroup of \( S \). By Corollary 3.3 we have \( r \leq n/2 \) and therefore \( k(G/K) \leq 2^{n/2} \) by Theorem 2.

It remains to estimate \( k(K) \). We will use the following two facts, the first of which is a straightforward consequence of Lemma 2.1, and the second of which can be checked easily using [KL2, Sect. 5.1] for example.

**Fact 1.** If \( L \) is a non-abelian simple group, then \( k(L)\text{Out}(L) \leq |L| \).

**Fact 2.** If \( L \) is a simple group of Lie type in characteristic \( p \), and \( |L|_p = p^i \), then \( |\text{Out}(L)| \leq 2^i \).

It is clear that \( k(K) \leq \prod_{i=1}^r k(L_i)\text{Out}(L_i) \).

If \( L = A_i \), then \( k(L)\text{Out}(L) \leq 2^i \), therefore by Corollary 3.3(ii) the total contribution of alternating groups to the above product is at most \( 2^{3n} \).

By Theorem 8 and Fact 1 the contribution of groups in \( \text{Lie}(p^r) \) and of sporadic groups is at most \( 2^{3n} \).

It follows using Lemma 2.1 and Fact 2 that the contribution of the remaining \( \text{Lie}(p) \) terms is at most \( (2p)^b \) where \( |K|_p = p^b \).
Write \(|G|_p = p^a\). Putting everything together we obtain

\[
k(G) \leq k(O_p(G))k(K)k(G/K) \leq (3p)^a \cdot 2^{n/2} \cdot 2^{2^n} \cdot (2p)^b \leq (2^{11}p)^a.
\]

The proof of Theorem 7 is complete.  

For the proof of Theorem 9 we shall need the following result.

**Lemma 3.5.**  If \(T\) is a non-abelian simple group and \(p\) is a prime, then

\[
2k(T)|\text{Out}(T)|_p < |T|_p
\]

with just the following exceptions: \((T, p) = (A_5, 2)(A_6, 2)(L_3(7), 2)\).

**Proof.**  If \(T\) is sporadic or \(A_n\) \((n \leq 8)\) then our conclusion can easily be checked using [At]. Now let \(T = A_n\) with \(n \geq 9\). We have \(|S_n|_p \leq p^{(n-1)/2} \leq 2^{n-1}\) and \(2k(T) \leq 2^n\). Hence \(2k(T)|\text{Out}(T)|_p |T|_p \leq 2^{2n-1}\) which is less than \(|T| = n!/2\) as required.

Now consider \(T = L_3(q)\), of order \(q(q^2 - 1)/(2, q - 1)\). We may assume \(T \neq A_n\), so \(q \neq 4, 5, 9\).

If \(q\) is even then \(k(T) = q + 1\) and \(|T|_p \geq q(q - 1)\). Hence \(2k(T)|\text{Out}(T)|_p = 2(q + 1) \log q\), and this is less than \(q(q - 1)\) for \(q \geq 8\).

If \(q\) is odd then \(|T|_p \geq q(q - 1)/2\), \(k(T) = (q + 5)/2\) and \(|\text{Out}(T)| = 2 \log q\), so

\[
2k(T)|\text{Out}(T)|_p = (q + 5) \cdot 2 \log q|_p.
\]

This is less than \(q(q - 1)/2\) except when \((q, p) = (7, 2)\), as in the conclusion of the lemma.

Next let \(T = B_2(q)\), of order \(q^3(q^2 + 1)(q - 1)\), with \(q = 2^{2^a + 1} \geq 8\).

Here \(k(T) = q + 3\) by [Su1], and \(|T|_p \geq (q^2 + 1)(q - 1)\). Since \(2(q + 3) \log q < (q^2 + 1)(q - 1)\) for \(q \geq 8\), the result follows.

Suppose now that \(T = L_3(q)\). Since \(L_3(2) \cong L_2(7)\) and \(U_3(2)\) is soluble, we may assume that \(q > 2\). As noted in the proof of Lemma 2.1, we have \(k(PGL_3^+(q)) \leq (q^2 + q + 2)(q^3, q - e)\), whence \(k(T) = k(L_3^+(q)) \leq (q^2 + q + 2)(q^3, q - e)\). Also, \(|T| = q^3(q^3 - e)(q^2 - 1)/(3, q - e)\), from which we see that \(|T|_p \geq (q^3 - e)(q^2 - 1)/(3, q - e)\). We now check that

\[
2k(T)|\text{Out}(T)|_p \leq 2(q^3 + q + 2)(3, q - e)^2 \cdot 2 \log q
\]

\[
< (q^3 - e)(q^2 - 1)/(3, q - e)
\]

except when \((q, e) = (4, +)\) or \((5, -)\). For these cases we see from [At] that \(k(L_3(4)) = 10, k(U_3(5)) = 14\), and the result follows.
We now complete the proof of the lemma. In view of the previous cases, we assume that $T = T(q)$ is of Lie type over $\mathbb{F}_q$, of untwisted rank $l$, and is not isomorphic to $L_2(q), L_3(q)$, or $^2B_2(q)$. (In particular $T$ is not $^2G_2(3)^\circ, G_2(2)^\circ$, or $B_3(2)^\circ$.)

From the orders the simple groups of Lie type (see [KL2, Sec. 5.1] for instance), we check that

**Fact 1.** Provided $T \neq U_q(2)$, we have $|T|_{p'} \geq |T|_{q'}$.

Next, a straightforward calculation gives

**Fact 2.** We have

$$2.(6q)^{l} |\text{Out}(T)| < |T|_{q'},$$

except when $T$ is one of the groups

$$L_2(2), L_3(2), L_5(2), L_6(2), U_2(2), U_3(2), U_5(2), U_6(2),$$

$$\text{PSp}_4(3), \text{PSp}_4(4), \text{Sp}_6(2), \Omega_6^\pm(2), ^2D_4(2), ^2F_4(2)' .$$

Since $k(T) \leq (6q)^l$ by Theorem 1, the result follows from the previous two facts, except when $T$ is in the list of exceptions in Fact 2. Of these groups, all but $L_6(2)$ can be found in [At1], where the values of $k(T)$ are given, from which the conclusion follows. Finally, for $T = L_6(2)$ we see using [Mac, p. 43] that $k(T) = 60$, and again the result follows. This completes the proof of the lemma.

Our proof of Theorem 9 now follows closely the argument given in [INM] for the soluble case.

**Proof of Theorem 9.** We argue by induction on $|G|$. We may assume that $O_p(G) = 1$. If $N$ is a minimal normal subgroup of $G$ and $M/N = O_p(G/N)$ then, by induction we have $k(G/M) \leq |G/N|_{p'}$.

If $M \neq G$ then again by induction we have that $k(M) \leq |N|_{p'}$. Therefore by Lemma 1.1 we obtain that $k(G) \leq k(G/M)k(M) \leq |G|_{p'}$ as required.

Suppose now that $M = G$.

If $N$ is abelian then $G = VP$ where $V$ is a normal elementary abelian $q$-subgroup of $G$ ($q \neq p$) and $P$ is a Sylow $p$-subgroup. Now $V$ is a faithful $\mathbb{F}_qP$-module and by Knörr’s results [Kn] it follows that $k(G) \leq k(VP) \leq |V| = |G|_{p'}$ as required.

Hence we may assume that $G$ has a minimal normal subgroup $N$ which is a direct-power of a non-abelian simple group, say $N = T'$, $G$ has a natural embedding into $\text{Aut}(N) = \text{Aut}(T')_{\text{wr}} S_r$, and $G/N$ is a $p$-group.
The group $\text{Aut}(N)$ has a subnormal series $\text{Aut}(N) = A_0 \triangleright A_1 \triangleright \cdots \triangleright A_{r+1} = 1$ such that $A_0/A_1 = S_i$ and $A_i/A_{i+1} = \text{Aut}(T)$ for $i \geq 1$. Consider the subnormal series $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{r+1}$ of $G$ defined by $G_i = A_i \cap G$.

As $G_0/G_3$ is isomorphic to a $p$-subgroup of $S_n$, it has order at most $2^{n-1}$. For $i \geq 1$, $G_i/G_{i+1}$ is isomorphic to a subgroup $H_i$ of $\text{Aut}(T)$ containing $T$ such that its quotient modulo $T$ is a $p$-group. By Lemma 1.1 we have $k(G) \leq 2^{n-1}k(T)^n(\text{Aut}(T))^{p'}$.

Using Lemma 3.5 we obtain that $k(G) \leq |T'|^p \leq |G|^{p'}$ except possibly if $p = 2$ and $T = A_5, A_6,$ or $L_2(7)$.

However, in these latter cases it can be checked directly using [At] that for any group $H$ with $T < H \leq \text{Aut}(T)$ we have $2k(H) \leq |H'|^2$. It follows that $k(G) \leq 2^{n-1}k(H_1) \cdots k(H_r) \leq |G|^{2^n}$ as required. The proof of the theorem is complete.

Let us finally clarify a connection between our results and one of those in [KR]. Theorem 4.1 of [KR] states that there is a constant $c$ such that if $G$ is a finite $p$-soluble group with $|F^*(G)| = p^r > 1$ then $k(G) \leq (cp)^r$. Taking $c = 3.2^{21}$, this follows from our Theorem 7, for if the $p$-soluble group $G \leq \text{GL}(n, p)$ is completely reducible then $|G|_{p'} \leq 3^n$ by [Wo2] (and [KR, 4.1] reduces to the case where $F^*(G)$ is elementary abelian and $G$ acts completely reducibly). In fact, combining the arguments of [KR] with Theorem 2.5, we see that the above mentioned theorem [KR, 4.1] holds for $c = 103$.

ACKNOWLEDGMENTS

We are indebted to G. R. Robinson for numerous valuable remarks.

REFERENCES


[St] R. Steinberg, The representations of \( GL(3, q) \), \( GL(4, q) \), \( PGL(3, q) \) and \( PGL(4, q) \), *Canad. Math. J.* **3** (1951), 225–235.


