J. Aust. Math. Soc. **79** (2005), 257–276

THE $k(GV)$-PROBLEM REVISITED

THOMAS MICHAEL KELLER

(Received 14 April 2004; revised 10 November 2004)

Communicated by E. A. O'Brien

Abstract

Suppose that the finite group G acts faithfully and irreducibly on the finite G-module V of characteristic p not dividing $|G|$. The well-known $k(GV)$-problem states that in this situation, if $k(GV)$ is the number of conjugacy classes of the semidirect product GV, then $k(GV) \leq |V|$. For p-solvable groups, this is equivalent to Brauer's famous $k(B)$-problem. In 1996, Robinson and Thompson proved the $k(GV)$-problem for large p. This ultimately led to a complete proof of the $k(GV)$-problem. In this paper, we present a new proof of the $k(GV)$-problem for large p.

2000 *Mathematics subject classification*: primary 20C15, 20C20.

1. Introduction

The subject of this paper is a classical open problem in the modular representation theory of finite groups, known as Brauer's $k(B)$-problem and dating back to the 1950s.

Recall that in modular representation theory, for a given prime p and a finite group G, the set of all irreducible complex and p-Brauer characters of G is partitioned into subsets called the p-blocks of G, and one assigns to each p-block B a certain p-subgroup D of G, called the defect group of B, which is uniquely determined up to conjugacy. If $|D| = p^{d(B)}$, then $d(B)$ is called the defect of B. (For an introduction to the subject, we refer the reader to [18].)

With these notions Brauer's $k(B)$-problem states that for any p-block B of G the number $k(B)$ of irreducible complex characters in B is bounded above by the order of the defect group D of B, that is, $k(B) \leq p^{d(B)}$.

The best general bound to date is due to Brauer and Feit and states that $k(B) \leq p^{2d(B)-2}$.

https://doi.org/10.1017/S144678870001048X Published online by Cambridge University Press

If G is p-solvable, it has been known for a long time that Brauer's $k(B)$-problem is equivalent to the following conjecture which is known as the $k(GV)$-problem.

$k(GV)$-PROBLEM. *If the group G acts faithfully and irreducibly on the finite G-module V and if $(|G|, |V|) = 1$, then the number $k(GV)$ of conjugacy classes of the semidirect product GV is bounded above by the order of V, that is, $k(GV) \leq |V|$.*

Over the past two decades this conjecture attracted the interest of a number of mathematicians, and in a huge effort its proof has finally been completed in [8]. For a detailed history of this fascinating problem, we refer the reader to [12] and [21]. We point out, however, that the whole line of attack on the problem is based on some fundamental ideas introduced by R. Knörr in the 1980s, which eventually led to the celebrated paper [22] by Robinson and Thompson, where they were able to settle the conjecture for large primes p (more precisely, for $p > 5^{30}$). All subsequent work on the problem is based on the results in [22].

In this paper, we will provide a new proof of the $k(GV)$-problem for large p, that is, for $p > K$ where K is a suitable constant. Our approach is independent of [22] and more straightforward, and the new proof in many instances gives bounds stronger than $k(GV) \leq |V|$. It turns out to be yet another application of character and fixed point ratio estimates (see, for example, [4, 15, 23] for other important examples), thus demonstrating once again their usefulness and power. Some of the ideas behind this approach to the $k(GV)$-problem were already developed in [11], but the proof in that paper was long and worked only for solvable groups.

Our strategy is as follows: We proceed by induction on $|GV|$. Clearly V is induced from a submodule W that is a primitive and faithful $\overline{N}$-module, where $\overline{N} = N_G(W)/C_G(W)$ (possibly $W = V$). We will reduce the problem to one of the following situations:

(1) $k(\overline{N}W) \leq |W|/T$ for some $T \in \mathbb{N}$ or
(2) $W < V$ and $k(\overline{N})$ is small relative to $|W|$ or
(3) $\overline{N} \lesssim \Gamma(q)$, where q is a power of p and $\Gamma(q)$ is the semilinear group on $GF(q)$.

This reduction process involves an analysis of the structure of coprime primitive linear groups which are large relative to the module they act on (see Theorem 3.5). The results obtained in this context are of independent interest and can be understood as qualifying the general result of Gambini and Gambini-Weigel [6] on the order of such groups. The proof is based on character ratio estimates which were proved by Gluck and Magaard in [7] for different purposes, and it ultimately makes use of an argument of Liebeck [13] that already had proved useful in the Robinson-Thompson paper. Thus the reduction to Cases (1), (2) and (3) depends on CFSG.

In Case (1), if $V = W$, we are done, and if $W < V$, an easy induction argument will show that $k(GV) \leq |V|$. In Case (2), an elementary induction (see Lemma 2.2) will do the job. In Case (3), if $W = V$, the conclusion can be shown directly. The inductive arguments used up to this point are of an elementary and purely group theoretical nature. We are left with Case (3) and $W < V$. This case not surprisingly requires a more sophisticated inductive treatment presented in Lemma 2.3. While formally similar to Lemma 2.2, it requires some basic character theory and also a technical argument from [11] on stabilizers in the action of a group on the set of conjugacy classes of a subgroup.

The paper is organized as follows: Section 2 contains the inductive arguments, Section 3 deals with the structure of primitive linear groups. In Section 4, we prove the main theorem.

Note that since the focus of the paper is on the methods and in order to keep the tedious parts of the proofs short, no effort has been made to keep the constant K small.

The notation used is standard and is as in [11]. In particular, $n(G, V)$ denotes the number of orbits of G on V. If F is a field, by the natural F-module V for S_n respectively A_n we mean the deleted permutation module of S_n respectively A_n, that is, $V = \{(x_1, \dots, x_n) \mid x_i \in F \text{ for all } i, \sum_{i=1}^{n} x_i = 0\}$ with components permuted naturally by S_n respectively A_n.

We will frequently use the fact that $k(G) \le 2^{n-1}$ for any subgroup G of the symmetric group S_n (see [14]), and that if V is an S_n- or A_n-module for $n > 6$ with $\mathrm{char}(V) > n$, then $\dim V \ge n - 1$ (see [24]). Also basic estimates for $k(G)$ such as $k(G) \le k(G/N)k(N)$ for $N \trianglelefteq G$ and the basic formulas for $k(GV)$ (see, for example, [11]) will freely be used, as well as the fact that if G acts faithfully on V with $(|G|, |V|) = 1$, then $|G| < |V|^2$ (see [20]).

2. The key lemmas

We begin with an auxiliary result.

LEMMA 2.1. *Let G be a group acting on a finite set Ω. Suppose that $|C_\Omega(g)| \ge |\Omega|/2$ for all $g \in G$. Then there exists an $\omega \in \Omega$ such that $\omega^g = \omega$ for all $g \in G$.*

PROOF. This is immediate from the Cauchy-Frobenius orbit counting formula. □

Now we can prove a crucial lemma in the spirit of [11, Lemma 3.8 and Remark 3.9].

LEMMA 2.2. *Let G be a finite group and V be a finite G-module with $(|G|, |V|) = 1$. Suppose that $N \trianglelefteq G$ and $V_N = V_1 \oplus \cdots \oplus V_n$ for an $n \in \mathbb{N}$, where the V_i are N-modules, and assume that G/N permutes the V_i transitively and faithfully. Put $H = N_G(V_1)$.*

Let $W \le V$ be a G-submodule with $|W| \ge |V|^\delta$ for some $0 \le \delta \le 1$. Moreover, suppose that the following hold:

https://doi.org/10.1017/S144678870001048X Published online by Cambridge University Press

(i) $k(HW) \leq |W|$;
(ii) $k(U) \leq \left(1/\sqrt{n+1}\right)|W|^{1/2-3/(8\delta)}$ *for all* $U \leq G$.

Then $k(GW) \leq |W|$.

PROOF. We may assume that $n \geq 2$. Let $M = \{g \in G \mid g$ normalizes at least $n/2$ of the $V_i\}$ and observe that $N \subseteq M$ and M is a normal subset of G, that is, $M^g = M$ for all $g \in G$. Let $T = \{v^G \mid v \in W$ and $C_G(v) \not\subseteq M\}$; so $v^G \in T$ means that there is a $g \in G - M$ such that g fixes an element of v^G, that is, $v^G \cap C_V(g) \neq \emptyset$. Hence $v^G \cap C_V(g^h) \neq \emptyset$ for all $h \in G$. This shows that if g_i, $i = 1, \dots, t$ are representatives of the conjugacy classes of G which are not in M, then

$$T \subseteq \bigcup_{i=1}^{t} \{v^G \mid v \in V \text{ and } v^G \cap C_V(g_i) \neq \emptyset\}$$

and thus $|T| \leq t \max_{i=1,\dots,t} |C_V(g_i)|$.

Now by definition of M clearly if $g \in G - M$, then g normalizes at most $n/2$ of the V_i which immediately implies that $|C_V(g)| \leq |V|^{3/4}$. Thus

$$|T| \leq k(G)|V|^{3/4} \leq k(G)|W|^{3/(4\delta)}.$$

Now consider $v \in W$ with $v^G \notin T$. Thus $C_G(v) \subseteq M$, so that $C_G(v)N/N$ is a permutation group on $\{V_1, \dots, V_n\} =: \Omega$ and all elements of $C_G(v)N/N$ have at least $n/2$ fixed points on Ω. By Lemma 2.1, there is an $i \in \{1, \dots, n\}$ with $C_G(v) \leq N_G(V_i)$, so by replacing v by another representative of v^G we may assume that $C_G(v) \leq H$. Thus $C_G(v) = C_H(v)$, and so $|v^G| > |v^H|$. Therefore, if $w_1, \dots, w_k \in v^G$ are representatives of the orbits of H on v^G with $w_1 = v$, then $k \geq 2$, and if we write $w_i = v^{g_i}$ for some $g_i \in G$ $(i = 2, \dots, k)$, then by [5, Formula (2)] for $i = 2, \dots, k$ we have

$$\begin{aligned} k(C_H(v)) = k(C_G(v)) = k(C_G(w_i)) &\leq |C_G(w_i) : C_H(w_i)| k(C_H(w_i)) \\ &\leq |G : H| k(C_H(w_i)) = nk(C_H(w_i)) \end{aligned}$$

and hence $k(C_H(w_i)) \geq (1/n)k(C_H(v))$ for $i = 2, \dots, k$. With this we obtain that

$$\begin{aligned} \sum_{j=1}^{k} k(C_H(w_j)) &\geq k(C_H(w_1)) + (k-1)\frac{1}{n} k(C_H(v)) \\ &= \frac{n+k-1}{n} k(C_H(v)) \geq \frac{n+1}{n} k(C_H(v)), \end{aligned}$$

the last inequality being true as $k \geq 2$.

Since the above considerations hold for any $v \in W$ with $v^G \notin T$, we conclude that if $v_i \in W$ $(i = 1, \dots, n(G, W))$ are representatives of the orbits of G on W and for any i the w_{ij} ($j = 1, \ldots, k_i$) are representatives of the orbits of H on v_i^G (so that clearly the w_{ij} for all i, j are representatives of all orbits of H on W), then we may assume that for all i with $v_i^G \notin T$ we have $C_G(v_i) \leq H$, and then the above yields

$$\sum_{i \text{ with } v_i^G \notin T} k(C_G(v_i)) = \sum_{i \text{ with } v_i^G \notin T} k(C_H(v_i)) \leq \frac{n}{n+1} \sum_{i \text{ with } v_i^G \notin T} \sum_{j=1}^{k_i} k(C_H(w_{ij}))$$
$$\leq \frac{n}{n+1} \sum_{i=1}^{n(G,W)} \sum_{j=1}^{k_i} k(C_H(w_{ij})) = \frac{n}{n+1} k(H, W).$$

Hence altogether with our hypotheses we obtain

$$\begin{aligned} k(GW) &= \sum_{i \text{ with } v_i^G \in T} k(C_G(v_i)) + \sum_{i \text{ with } v_i^G \notin T} k(C_G(v_i)) \\ &\leq |T| \frac{1}{\sqrt{n+1}} |W|^{1/2-3/(8\delta)} + \frac{n}{n+1} k(HW) \\ &\leq k(G)|W|^{3/(4\delta)} \frac{1}{\sqrt{n+1}} |W|^{1/2-3/(8\delta)} + \frac{n}{n+1} |W| \\ &\leq \frac{1}{\sqrt{n+1}} |W|^{1/2-3/(8\delta)} |W|^{3/(4\delta)} \frac{1}{\sqrt{n+1}} |W|^{1/2-3/(8\delta)} + \frac{n}{n+1} |W| = |W|, \end{aligned}$$

as desired. □

We next prove another lemma of a similar flavor. For this we will need Gallagher's goodness property. Recall that in [5] Gallagher defines, for $N \trianglelefteq G$, $\psi \in \mathrm{Irr}(N)$ and $g \in C_G(\psi)$ (the inertia group of ψ in G), that g is *good* for ψ if an extension ψ_0 of ψ to $N\langle g\rangle$ is invariant under $C_G(\psi) \cap L$, where $L = \{h \in G \mid (gN)^h = gN\}$. Goodness is independent of the choice of ψ_0 and depends only on the conjugacy class of gN in $C_G(\psi)/N$. Then as in [11, Example 3.4 (b)] for $N \leq U \leq G$ we define

$$P(U/N, \psi) = \{M \in \mathrm{cl}(C_{U/N}(\psi)) \mid \text{there is a } g \in M \text{ that is good for } \psi\},$$

then P is a goodness property in the sense of [11, Definition 3.1] which we call Gallagher's goodness property, and from [11, Example 3.4 (b)] we know that for any $N \leq U \leq G$ we have

$$k(U) = \alpha_P(U/N, \mathrm{Irr}(N)) = \sum_{\chi \in \mathrm{Irr}(N)} \frac{|C_{U/N}(\chi)| k_P(C_{U/N}(\chi))}{|U/N|},$$

where $k_P(C_{U/N}(\chi))$ is the number of conjugacy classes of elements of $C_{U/N}(\chi)$ which are good for χ.

LEMMA 2.3. *Let G be a finite group and V be a finite faithful G-module. Suppose that $N \trianglelefteq G$ and $V_N = V_1 \oplus \cdots \oplus V_n$ where the V_i are N-modules, and assume that G/N permutes the V_i transitively and faithfully. Furthermore assume that $N/C_N(V_1) \lesssim \Gamma(V_1)$ and write $q = |V_1|$. Let $W \leq V$ be a G-submodule with $|W| \geq |V|^{15/16}$. Put $H = N_G(V_1)$ and suppose that the following hold:*

(i) $k(HW) \leq |W|$;
(ii) $q > 2^{400}$.

Then $k(GW) \leq |W|$.

PROOF. We may assume that $n > 1$. Write $\Gamma(q) = \Gamma(V_1)$. Clearly

$$N \lesssim \Gamma(V_1) \times \cdots \times \Gamma(V_n) \cong \Gamma(q)^n.$$

Identifying N with its isomorphic subgroup in $\Gamma(q)^n$, we write $T = \Gamma_0(q)^n$ and $M = N \cap T_1$ so that M is an abelian normal subgroup of G and $|N/M| \leq (\log_2 q)^n$.

We consider the action of G/M on $\Omega := \mathrm{Irr}(MW)$. If $\omega \in \Omega$, we will write ω^G for the orbit of ω under G and $\omega\uparrow^G$ for the induced character. Let P be Gallagher's goodness property with respect to this action. Then we have $k(HW) = \alpha_P(H/M, \Omega)$ and $k(GW) = \alpha_P(G/M, \Omega)$. Now let $R = \{gM \in G/M \mid gM$ normalizes at least $n/2$ of the $V_i\}$, so R is a normal subset of G/M. Let $T = \{\omega^{G/M} \mid \omega \in \Omega$ and $C_{G/M}(\omega) \nsubseteq R\}$, so $\omega^{G/M} \in T$ means that there is a $gM \in G/M - R$ such that gM fixes an element of $\omega^{G/M}$, that is, $\omega^{G/M} \cap C_\Omega(gM) \neq \emptyset$. Hence $\omega^{G/M} \cap C_\Omega(g^h M) \neq \emptyset$ for all $h \in G$. This shows that if $g_i M$, $i = 1, \ldots, t$, are representatives of the conjugacy classes of G/M which are not in R, then

$$T \subseteq \bigcup_{i=1}^{t} \left\{\omega^{G/M} \mid \omega \in \Omega \text{ and } \omega^{G/M} \cap C_\Omega(g_i M) \neq \emptyset\right\}$$

and thus $|T| \leq t \max_{i=1,\ldots,t} |C_\Omega(g_i M)| \leq k(G/M) \max_{gM \in G/M-R} |C_\Omega(gM)|$. Now as $G/N \lesssim S_n$, we have $k(G/M) \leq k(G/N)k(M/N) \leq 2^{n-1}(\log_2 q)^n$. Furthermore, if $gM \in G/M - R$, then gM has at most $n/2$ fixed points in its permutation action on $\{V_1, \ldots, V_n\}$. Hence we may apply [11, Lemma 4.7 (c)] to the action of $\langle g, N\rangle$ on V which yields that if $\Omega_1 = \mathrm{cl}(MV)$ is the set of conjugacy classes of MV, then $|C_{\Omega_1}(g)| \leq 4^n q^{7n/8}$. Let $\Omega_0 = \mathrm{Irr}(MV)$. Since there is a G-module W' such that $V = W \oplus W'$, clearly $MW \cong MV/W'$ and hence $\Omega \subseteq \Omega_0$. Now G/M acts on Ω_1 and Ω_0 by conjugation, and so Brauer's permutation lemma (see, for example, [10, Theorem 18.5 (b)]) yields

$$|C_\Omega(gM)| \leq |C_{\Omega_0}(gM)| = |C_{\Omega_1}(gM)| = |C_{\Omega_1}(g)| \leq 4^n q^{7n/8}.$$

Hence we conclude that

$$|T| \leq 2^{n-1}(\log_2 q)^n 4^n q^{7n/8}.$$

https://doi.org/10.1017/S144678870001048X Published online by Cambridge University Press

Now consider ω with $\omega^{G/M} \not\subseteq T$. Then $C_{G/M}(\omega) \subseteq R$, so all elements of $C_G(\omega)N/N$ have at least $n/2$ fixed points on $\{V_1, \dots, V_n\}$. By Lemma 2.1 there is an $i \in \{1, \dots, n\}$ with $C_G(\omega) \leq N_G(V_i)$, and so we may assume that $C_G(\omega) \leq H$. As $H < G$, it follows that $|\omega^{G/M}| > |\omega^{H/M}|$, and so if $\omega_1, \dots, \omega_k \in \omega^{G/M}$ are representatives of the orbits of H/M on $\omega^{G/M}$ with $\omega_1 = \omega$, then $k \geq 2$, and by the theorem in [5] and [10, Exercise E17.2] we see that, for $i = 2, \dots, k$, we have

$$\begin{aligned} k_P(C_{H/M}(\omega)) &= k_P(C_{G/M}(\omega)) = k_P(C_{G/M}(\omega_i)) \\ &= |\{\psi \in \operatorname{Irr}(C_{GV}(\omega_i)) \mid \psi \text{ is a constituent of the induced} \\ &\qquad \text{character } \omega_i \uparrow^{C_{GV}(\omega_i)}\}| \\ &\leq |C_{GV}(\omega_i) : C_{HV}(\omega_i)| \\ &\quad \times |\{\Theta \in \operatorname{Irr}(C_{HV}(\omega_i)) \mid \Theta \text{ is a constituent of } \omega_i \uparrow^{C_{HV}(\omega_i)}\}| \\ &\leq |G : H| \cdot k_P(C_{H/M}(\omega_i)) = n k_P(C_{H/M}(\omega_i)). \end{aligned}$$

Hence, as in the previous lemma, we obtain

$$\sum_{j=1}^{k} k_P(C_{H/M}(\omega_j)) \geq \frac{n+k-1}{n} k_P(C_{H/M}(\omega)) \geq \frac{n+1}{n} k_P(C_{H/M}(\omega)).$$

Since these considerations hold for any $\omega^{G/M} \not\subseteq T$, we conclude that if $\omega_i \in \Omega$ ($i = 1, \dots, n(G/M, \Omega)$) are representatives of the orbits of G/M on Ω and the ω_{ij} ($j = 1, \dots, k_i$) are representatives of the orbits of H/M on $\omega_i^{G/M}$, then we may assume that for all i with $\omega_i^{G/M} \not\subseteq T$ we have $C_{G/M}(\omega_i) \leq H/M$, and then the above yields

$$\begin{aligned} \sum_{i \text{ with } \omega_i^{G/M} \not\subseteq T} k_P(C_{G/M}(\omega_i)) &= \sum_{i \text{ with } \omega_i^{G/M} \not\subseteq T} k_P(C_{H/M}(\omega_i)) \\ &\leq \frac{n}{n+1} \sum_{i \text{ with } \omega_i^{G/M} \not\subseteq T} \sum_{j=1}^{k_i} k_P(C_{H/M}(\omega_{ij})) \\ &\leq \frac{n}{n+1} \alpha_P(H/M, \Omega) = \frac{n}{n+1} k(HW). \end{aligned}$$

Hence altogether with hypothesis (i) we obtain

$$\begin{aligned} k(GW) = \alpha_P(G/M, \Omega) &= \sum_{i \text{ with } \omega_i^{G/M} \subseteq T} k_P(C_{G/M}(\omega_i)) + \sum_{i \text{ with } \omega_i^{G/M} \not\subseteq T} k_P(C_{G/M}(\omega_i)) \\ &\leq |T| \max_{i=1,\dots,n(G/M,\Omega)} k_P(C_{G/M}(\omega_i)) + \frac{n}{n+1} k(HW) \\ &\leq 2^{n-1}(\log_2 q)^n 4^n q^{7n/8} \max_{U \leq G/M} k(U) + \frac{n}{n+1} |W|. \end{aligned}$$

https://doi.org/10.1017/S144678870001048X Published online by Cambridge University Press

Since for any $U \leq G/M$ we have $k(U) \leq 2^{n-1}|N/M| \leq 2^{n-1}(\log_2 q)^n$, we further conclude that

$$k(GW) \leq (2^{n-1}(\log_2 q)^n)^2 4^n q^{7n/8} + \left(1 - \frac{1}{n+1}\right)|W|,$$

which implies $k(GW) \leq |W|$ whenever $2^{2n-2}(\log_2 q)^{2n}4^n q^{7n/8} \leq |W|/(n+1)$. As $|W| \geq |V|^{15/16} = q^{15n/16}$, for this it suffices that $2^{4n-2}(\log_2 q)^{2n}(n+1) \leq q^{n/16}$. This will be satisfied whenever $2^{5n}(\log_2 q)^{2n} \leq q^{n/16}$ or, equivalently, $32(\log_2 q)^2 \leq q^{1/16}$. But this is the case since, by our hypothesis, $q > 2^{400}$, and so the lemma is proved. □

3. Primitive linear groups

The next lemma is essentially from [7].

LEMMA 3.1. *Let G be a finite group, and let W be a faithful irreducible $GF(q)G$-module, where q is a prime power such that $(|G|, q) = 1$. Suppose further that W is primitive and that G has no component which is an alternating group of degree at least* 10. *Then for every $1 \neq g \in G$ we have $|C_W(g)| \leq |W|^{79/80}$. In particular, for every $\delta > 0$ and for every $H \leq G$ with $|H| \geq |G|^\delta$, we have*

$$n(H, W) \leq \frac{2|W|}{\min\{|G|^\delta, |G|^{1/160}\}}.$$

PROOF. The first assertion follows immediately from the proof of [7, Proposition 2.8] (note that the assumption $\dim W > 88$ in that proof is not needed for the argument). Now by Cauchy-Frobenius we have

$$\begin{aligned} n(H, W) &= \frac{|W|}{|H|} + \frac{1}{|H|}\sum_{1 \neq g \in H} |C_W(g)| \\ &\leq \frac{|W|}{|H|} + \frac{|H|-1}{|H|}|W|^{79/80} \leq \left(\frac{1}{|H|} + \frac{1}{|W|^{1/80}}\right)|W|. \end{aligned}$$

As $|G| < |W|^2$, we further conclude that

$$n(H, W) \leq \left(\frac{1}{|G|^\delta} + \frac{1}{|G|^{1/160}}\right)|W|$$

which implies the assertion. □

Next we need to slightly generalize Liebeck's well-known regular orbit theorem.

https://doi.org/10.1017/S144678870001048X Published online by Cambridge University Press

LEMMA 3.2. *Let $T \geq 1$. There exists a function $f : [1, \infty) \to \mathbb{N}$ such that the following holds: If p is a prime with $p > f(T)$ and G is a p'-group and V is a faithful $GF(p)G$-module such that G has a quasisimple normal subgroup H which is irreducible on V, then one of the following holds:*

(a) $\sum_{g \in G-\{1\}} |C_V(g)| \leq |V|/T$; *in particular,* $k(UV) \leq (T + |U| + 1)|V|/T|U|$ *for any* $U \leq G$.

(b) $H = A_c$, $c < p$, *and V is the natural $GF(p)$-module for H.*

PROOF. This can be shown by slightly adjusting the proof of the main theorem in [13] in an obvious way as follows (we use the notation of that paper): The assumption (†) now reads $|V|/T < \sum_{g \in G-\{1\}} |C_V(g)|$. Lemma 1 reads $q < 6T|\operatorname{Aut}(\overline{H})|$, and Lemma 2 (iii) and (iv) read $q^2 \leq 6T|\operatorname{Aut}(\overline{H})|$ and $q \leq (3T|\operatorname{Aut}(\overline{H})|)^{r/(n-rt+r)}$, respectively, with the obvious adjustments in their proofs. Most of the changes to be made in the proof of Lemma 4 are obvious; the inequality on page 1140 needs to be changed to $2c! \geq (1/T)q^{5n/(c+22)} - \cdots$ (the rest is not modified), and right after that it should read: Since $q > c \geq 20$ and $n \geq c(c-3)/2$, for $q > f(T)$ (given that $f(T)$ has been chosen large enough) the second, third, fourth, and fifth terms of the right-hand side are all less than $(1/8T)q^{5n/(c+22)}$, and hence, $(1/T)q^{5n/(c+22)} \leq 4c!$. Hence for $c \geq 20$ we obtain, as $n \geq c(c-3)/2$, that $q^{5c(c-3)/2} \leq (4Tc^c)^{c+22}$ which for $q > f(T)$ and $f(T)$ large enough yields a contradiction. Therefore $c < 20$. $(\ldots)$ Then Lemma 2 (iii) gives $p^2 \leq 6T\,c! \leq 6(19!)T$, whence $p < 5^{30}T$, a contradiction if $f(T)$ is chosen greater than $5^{30}T$. And if $c < 12$, then Lemma 1 gives $p \leq 6(12!)T < 5^{30}T$, again a contradiction. To complete the proof, suppose now that $t > 1$. We know that if $f(T)$ is large enough, then $c \neq 6$ (by Lemma 1), ... The remaining modifications of the proof of Lemma 4 are obvious.

The first line of the proof of Lemma 5 should read: By Lemma 1, $p \leq 6T|\operatorname{Aut}(\overline{H})|$; hence if $f(T) > 5^{30}T$, then $6|\operatorname{Aut}(\overline{H})| > 5^{30}$. The remaining modifications are obvious; the last line of the proof should read: Then Lemma 2 (iv) shows that p is bounded by a function of T, so if $f(T)$ is greater that that function, we get a contradiction.

Similar adjustments are needed in the proof of Lemma 6, and then the proof of the main result is complete.

The bound for $k(UV)$ in Case (a) is easily obtained with the elementary argument demonstrated in the proof of [12, Lemma 5.3], namely

$$\begin{aligned} k(UV) &= \sum_{g \in U} \frac{|C_U(g)|}{|U|}\, n(C_U(g), C_V(g)) \\ &= \frac{1}{|U|}\left(\sum_{g \in U} |C_V(g)| + \sum_{1 \neq g \in U} |C_U(g)|\, n(C_U(g), C_V(g)) \right) \end{aligned}$$

https://doi.org/10.1017/S144678870001048X Published online by Cambridge University Press

$$\leq \frac{|V|}{|U|} + \frac{|U|+1}{|U|} \sum_{1 \neq g \in U} |C_V(g)| \leq \frac{|V|}{|U|} + \frac{|U|+1}{|U|} \frac{|V|}{T},$$

from which the assertion follows. □

The next lemma is probably well known.

LEMMA 3.3. *Suppose that G is a finite group and V is a finite $GF(q)G$-module for a prime power q not dividing $|G|$. Suppose that $V = V_1 \oplus V_2$ for G-modules V_i $(i = 1, 2)$. Then $k(GV) \leq n(G, V_1) \max_{v_1 \in V_1} k(C_G(v_1) V_2)$.*

PROOF. First note that the formulas in [11, Corollary 3.7] are also true (with essentially the same proof) in the more general situation that G acts coprimely on an abelian group V, and using this we obtain

$$\begin{aligned} k(GV) &= \frac{1}{|G|} \sum_{v_1 \in V_1,\ v_2 \in V_2} |C_G(v_1 + v_2)| k(C_G(v_1 + v_2)) \\ &= \frac{1}{|G|} \sum_{v_1 \in V_1,\ v_2 \in V_2} |C_{C_G(v_1)}(v_2)| k(C_{C_G(v_1)}(v_2)) \\ &= \sum_{v_1 \in V_1} \frac{|C_G(v_1)|}{|G|} \left(\frac{1}{|C_G(v_1)|} \sum_{v_2 \in V_2} |C_{C_G(v_1)}(v_2)| k(C_{C_G(v_1)}(v_2)) \right) \\ &= \sum_{v_1 \in V_1} \frac{|C_G(v_1)|}{|G|} k(C_G(v_1) V_2) \leq \left(\max_{v_1 \in V_1} k(C_G(v_1) V_2) \right) n(G, V_1), \end{aligned}$$

as wanted. □

We need another easy lemma.

LEMMA 3.4. *Let q be a prime power, $m \in \mathbb{N}$, G a finite group and let V_i $(i = 1, \ldots, m)$ be finite, faithful $GF(q)G$-modules. Write $V_0 = \bigoplus_{i=1}^m V_i$. Then the following hold:*

(a) $n(G, V_0) \leq \big((q^m + |G| - 1)/(q^m |G|)\big) |V_0|$.
(b) *If* $(|G|, q) = 1$ *and* $\max\{k(UV_1) \mid U \leq G\} \leq |V_1|$, *then*

$$k(GV_0) \leq \frac{q^{m-1} + |G| - 1}{q^{m-1}|G|} |V_0| \leq \frac{2}{\min\{|G|, q^{m-1}\}} |V_0|.$$

PROOF. (a) Clearly $C_{V_i}(g) \neq V_i$ for all i and $g \in G - \{1\}$, so $|C_{V_i}(g)| \leq |V_i|/q$ for all i and $g \neq 1$, and thus

$$n(G, V_0) = \frac{1}{|G|} \sum_{g \in G} |C_{V_0}(g)| \leq \frac{|V_0|}{|G|} + \frac{1}{|G|} \sum_{1 \neq g \in G} \frac{|V_0|}{q^m} = \frac{q^m + |G| - 1}{q^m |G|} |V_0|.$$

https://doi.org/10.1017/S144678870001048X Published online by Cambridge University Press

(b) By Lemma 3.3 and the hypothesis we have $k(GV_0) \leq |V_1| n\big(G, \bigoplus_{i=2}^m V_i\big)$ which with (a) implies the assertion. □

THEOREM 3.5. *Let $\epsilon > 0$ and $T \in \mathbb{N}$ with $T \geq 2$. There exist constants D_ϵ, F_ϵ, H_ϵ depending only on ϵ and a constant $K_{\epsilon,T}$ depending only on ϵ, T such that the following holds: Let G be a finite group, and let W be a faithful irreducible $GF(q)G$-module, where q is a prime power such that $(|G|, q) = 1$. Suppose further that W is primitive and that $|G| > |W|^\epsilon/2$. Put $Z = Z(F^*(G))$.*

(a) *Suppose that $q > H_\epsilon$. Let $k \in \mathbb{N}$ be minimal subject to $|Z| \mid q^k - 1$.*
 (1) *If $F^*(G) = F(G)$, then $|G| < D_\epsilon |Z| k$.*
 (2) *If $F^*(G) \neq F(G)$, then there is an $N \trianglelefteq G$ such that $F^*(N) = G_1 Z$ and $Z = Z(N)$ for a quasisimple group G_1, and $|G| < F_\epsilon |N| k$.*

(b) *If $q = p$ is a prime and $p > K_{\epsilon,T}$, then the following hold:*
 (1) *If $F^*(G) = F(G)$, then $G \leq \Gamma(W)$, or $k(HW) \leq |W|/T$ for any $H \leq G$ such that also $|H| > |W|^\epsilon/2$.*
 (2) *Suppose $F^*(G) \neq F(G)$ and let G_1 be as in (a). Assume in addition that if $W = V_1 \oplus V_2$ for nontrivial G_1-modules V_i $(i = 1, 2)$, then $\max\{k(UV_2) | U \leq G_1\} \leq |V_2|$. Then if $p > K_{\epsilon,T}$, one of the following holds:*
  (α) *$k(U) \leq |W|^{1/200}/8$ for all $U \leq G$, or*
  (β) *$k(HW) \leq |W|/T$ for any $H \leq G$ such that $|H| > |W|^\epsilon/2$.*

NOTE. The additional hypothesis in (b) (2) is of a technical nature only and will be automatically satisfied (for large p) once the $k(GV)$-conjecture has been proved, because as W is homogeneous as G_1-module, clearly each $U \leq G_1$ acts faithfully on V_2.

PROOF. (a) As W is primitive, every normal abelian subgroup of G is cyclic. Hence if $Z = Z(F^*(G))$, then Z is cyclic and $W_Z = V_1 \oplus \cdots \oplus V_s$ for an $s \in \mathbb{N}$ and isomorphic irreducible Z-modules V_i. Put $k = (\dim V)/s$ so $|V_1| = q^k$, and let $K_1 = GF(q^k)$. By [17, Example 2.7] k is the smallest integer such that $|Z| \mid q^k - 1$. Then, by [9, II, Hilfssatz 3.11], G acts as a semilinear group (over $GF(q)$) on $V_0 := V(s, q^k)$, and the permutation actions of G on W and on V_0 are equivalent. Moreover, $G_0 := C_G(Z) \leq GL(s, q^k)$ and $|G/G_0| \mid |\mathrm{Gal}(GF(q^k)/GF(q))| = k$. So we have $|G| \leq k|G_0|$ and $\dim W = k \dim V_0$ and $F^*(G) = F^*(G_0)$. Also note that as Z acts fixed point freely on V_1, clearly $|Z| \mid |K_1| - 1$, in particular, $|Z| < |K_1|$.

Now let W_1 be an irreducible $F^*(G)$-submodule of V_0. It is well-known that if $K = \mathrm{End}_{K_1 F^*(G)}(W_1)$ and W_2 is an irreducible summand of $W_1 \otimes K$, then W_2 is an absolutely irreducible $KF^*(G)$-module and the permutation action of $F^*(G)$ on vectors of W_1, W_2, respectively, are permutation isomorphic (see, for example, [22, Lemma 10]). In particular, $|W_2| = |W_1| \leq |V_0| = |W|$ and $\dim W \geq k \dim W_1 \geq k \dim W_2$. Now for the generalized Fitting subgroup $F^*(G)$ we have the decomposition

$$F^*(G) = E(G)F(G) = (G_1 \cdots G_m)(P_1 \times \cdots \times P_{l_1})(P_{l_1+1} \times \cdots \times P_l)$$

as the elementwise-commuting product of the components G_i and the Sylow subgroups $P_1, \ldots, P_l$ of $F(G)$, where by [17, Corollary 1.4] the $P_i \leq Z(F^*(G))$ $(i = l_1 + 1, \ldots, l)$ are cyclic of prime order, and the P_i $(i = 1, \ldots, l_1)$ are extraspecial of exponent an odd prime, or the central product of an extraspecial 2-group of exponent 4 and a group T which is dihedral, quaternion or semidihedral. Hence $|P_j/\Phi(P_j)| \leq p_j^{2m_j+2}$ $(j = 1, \ldots, l_1)$ for suitable primes p_j and nonnegative integers m_j, and $|P_j| = p_j$ $(j = l_1 + 1, \ldots, l)$ for suitable primes p_j. Note that $\prod_{j=l_1+1}^{l} P_j \leq Z$.

Now by [1, (3.16) (2)] we obtain that $W_2 \cong X_1 \otimes \cdots \otimes X_m \otimes Y_1 \otimes \cdots \otimes Y_{l_1}$, where each $X_i \leq W$ is an absolutely irreducible KG_i-module and each $Y_i \leq W$ is an absolutely irreducible KP_i-module. Write $x_i = \dim_K X_i$ and $y_j = \dim_K Y_j$. Then clearly $x_i \geq 2$ for all i and $y_j \geq p_j^{m_j}$ with $m_j \geq 1$ for all j and

$$\dim W \geq k \dim W_2 = k \left(\prod_{i=1}^{m} x_i \right) \left(\prod_{j=1}^{l_1} y_j \right) \geq k \left(\prod_{i=1}^{m} x_i \right) \left(\prod_{j=1}^{l_1} p_j^{m_j} \right).$$

Also note that $\prod_{j=1}^{l} p_j \mid |Z| < |K_1| \leq |K|$.

Now if $G^* = \bigcap_{i=1}^{m} N_{G_0}(G_i)$, then $F^*(G) \leq G^* \trianglelefteq G_0$ and $G_0/G^* \lesssim S_m$, and as $\prod_{j=l_1}^{l} P_j \leq Z$ and $G_0 = C_G(Z)$, we further have

$$G^*/F(G) \lesssim \left(\mathop{\times}_{i=1}^{m} \operatorname{Aut}(\overline{G}_i) \right) \times \left(\mathop{\times}_{j=1}^{l_1} \operatorname{Aut}(\overline{P}_j) \right),$$

where $\overline{G}_i = G_i/Z(G_i)$ is simple and $\overline{P}_j = P_j/\Phi(P_j)$ for all i, j (see, for example, [16, Proposition 6.1]). Hence

$$\begin{aligned} |G| &= |G/G_0||G_0/G^*||G^*/F(G)||F(G)/Z||Z| \\ &\leq km^m \left(\prod_{i=1}^{m} |\operatorname{Aut}(\overline{G}_i)| \right) \left(\prod_{j=1}^{l_1} |\mathrm{GL}(2m_j + 2, p_j)| \right) \left(\prod_{j=1}^{l_1} p_j^{2m_j+2} \right) |Z|. \end{aligned}$$

As $|Z| < |K|$, we further obtain

$$\text{(1)} \qquad \begin{aligned} |G| &\leq km^m \left(\prod_{i=1}^{m} |\operatorname{Aut}(\overline{G}_i)| \right) \left(\prod_{j=1}^{l_1} p_j^{(2m_j+2)^2} \right) \left(\prod_{j=1}^{l_1} p_j^{2m_j+2} \right) |Z| \\ &< km^m \left(\prod_{i=1}^{m} |\operatorname{Aut}(\overline{G}_i)| \right) \left(\prod_{j=1}^{l_1} p_j^{4m_j^2+6m_j+6} \right) |K|. \end{aligned}$$

Therefore by hypothesis we have

$$km^m\left(\prod_{i=1}^{m}|\operatorname{Aut}(\overline{G}_i)|\right)\left(\prod_{j=1}^{l_1}p_j^{4m_j^2+6m_j+6}\right)|K|$$
$$>\frac{1}{2}|W|^{\epsilon}\geq\frac{1}{2}|W_2|^{\epsilon}\geq\frac{1}{2}|K|^{\left(\prod_{i=1}^{m}x_i\right)\left(\prod_{j=1}^{l_1}p_j^{m_j}\right)\epsilon}$$

Now from the Atlas [2] one can derive that for some constant C we have

(2) $$|\operatorname{Aut}(H)|<C|H|\ln^2|H|$$

for any finite simple group H (see [19, Section 6]).

Moreover, since our actions are all coprime, we have $|\overline{G}_i|\leq|G_i|\leq|X_i|^2$, and this yields $|\operatorname{Aut}(\overline{G}_i)|<C|X_i|^2\ln^2(|X_i|^2)\leq 4C|X_i|^3=4C|K|^{3x_i}$. Using this estimate in the above formula yields

(3) $$km^m4^{m+1}C^m|K|^{1+3\sum_{i=1}^{m}x_i}\left(\prod_{j=1}^{l_1}p_j^{4m_j^2+6m_j+6}\right)>|K|^{\left(\prod_{i=1}^{m}x_i\right)\left(\prod_{j=1}^{l_1}p_j^{m_j}\right)\epsilon}.$$

Note that $k\leq\log_2|K|$. Hence from (3) it is easy to see that there is a constant A_ϵ (depending only on ϵ) such that

(4) $$\prod_{j=1}^{l_1}p_j^{m_j}\leq A_\epsilon,$$

no matter what $|K|$ and m and the x_i are.

Suppose that $m\geq 1$. We may assume that $x_1\geq x_2\geq\cdots\geq x_m$. Hence from (3) we get

$$|K|^{1+3mx_1}\log_2|K|\left(m^m4^{m+1}C^m\prod_{j=1}^{l_1}p_j^{4m_j^2+6m_j+6}\right)>|K|^{x_1\left(\prod_{i=2}^{m}x_i\right)\left(\prod_{j=1}^{l_1}p_j^{m_j}\right)\epsilon}.$$

Since $x_i\geq 2$ for all i and by (1), clearly $\prod_{j=1}^{l_1}p_j^{4m_j^2+6m_j+6}\leq B_\epsilon$ for some B_ϵ depending only on ϵ, we see that there is a C_ϵ depending only on ϵ such that

(5) $$\prod_{i=2}^{m}x_i\leq C_\epsilon.$$

From (1), (4) and (5) it follows that there are constants D_ϵ, E_ϵ such that if $m=0$, then

(6) $$|G|<D_\epsilon k|Z|\leq D_\epsilon|K|\log_2|K|$$

and if $m \geq 1$, then as $|G| > |W|^\epsilon/2$, we see from (1), (4) and (5) that we can choose H_ϵ such that for $q > H_\epsilon$ we have that $\overline{G}_1$ is not isomorphic to any of the $\overline{G}_i$ for $i \geq 2$. Hence $G_1 \trianglelefteq G$ and thus for $M := \left(\prod_{i=2}^m G_i\right)\left(\prod_{j=1}^{l_1} P_j\right) \trianglelefteq G$ we have $|MZ/Z| \leq E_\epsilon$, and as

$$G^*/C_{G^*}(M) \lesssim \operatorname{Aut}(M) \lesssim \mathop{\times}_{i=2}^{m} \operatorname{Aut}(\overline{G}_i) \times \mathop{\times}_{j=1}^{l_1} \operatorname{Aut}(P_j),$$

with [17, Lemma 1.5] we obtain $|C_{G_0}(P_j Z/Z)| \leq |P_j Z/Z| = |P_j/Z(P_j)|$ and hence

$$\begin{aligned}|G_0/C_{G_0}(M)| &\leq m^m \prod_{i=2}^{m} |\operatorname{Aut}(\overline{G}_i)| \prod_{j=1}^{l_1} (|\operatorname{Aut}(P_j Z/Z)||C_{G_0}(P_j Z/Z)|)\\ &\leq m^m \prod_{i=2}^{m} |\operatorname{Aut}(\overline{G}_i)| \prod_{j=1}^{l_1} (|\operatorname{Aut}(P_j Z/Z)||P_j/Z(P_j))|)\\ &\leq F_\epsilon\end{aligned}$$

for a constant F_ϵ depending on ϵ only. Therefore in this case we obtain, using (2), that $|G| = |G/G_0||G_0/C_{G_0}(M)||C_{G_0}(M)| \leq kF_\epsilon|C_{G_0}(M)|$. Put $N = C_{G_0}(M) = C_G(M) \trianglelefteq G$ and observe that $F^*(N) = G_1 Z$. So (a) is proved.

(b) Let $H \leq G$ such that $|H| > |W|^\epsilon/2$ and put $H_0 = H \cap G_0$, $Z_0 = H \cap Z$. Next observe that since the permutation action of G on W and V_0 are equivalent and $G_0 = C_G(Z)$ acts linearly on V_0, we have $k(H_0 W) = k(H_0 V_0)$ and hence $k(HW) \leq k \cdot k(H_0 W) = k \cdot k(H_0 V_0)$.

First assume $m = 0$, that is, $F^*(G) = F(G)$. Now as Z acts fixed point freely, we have $k(Z_0 W) = (|W| - 1)/|Z_0| + |Z_0|$. Suppose that G is not isomorphic to a subgroup of $\Gamma(W)$. Then $F(G)$ is not cyclic, and thus $l_1 \geq 1$ and $|Z| \leq |W|^{1/2}$. Therefore

$$k(Z_0 W) = \frac{|W| + |Z_0|^2 - 1}{|Z_0|} \leq \frac{|W| + |W|}{|Z_0|} \leq \frac{2|W|}{|Z_0|}$$

and so

$$k(HW) \leq k((HW)/(Z_0 W))k(Z_0 W) \leq |H/Z_0| k(Z_0 W) \leq \frac{2kD_\epsilon}{|Z_0|}|W|.$$

As $D_\epsilon|Z_0|k \geq |H| \geq |W|^\epsilon/2$ and $k \leq \log_2|W|$, we see that $|Z_0| \geq |W|^\epsilon/2D_\epsilon k$ and

$$k(HW) \leq \frac{2k^2 D_\epsilon^2}{|W|^\epsilon}|W| \leq 2D_\epsilon^2 \frac{(\log_2|W|)^2}{|W|^\epsilon}|W|.$$

As $|W| > p$, it is clear from this that if $K_{\epsilon,T}$ is chosen large enough, then for any $p > K_{\epsilon,T}$ we will have $k(HW) \leq |W|/T$, and the first part of (b) is proved.

So now suppose that $m \geq 1$, that is, $F^*(G) \neq F(G)$. First suppose that $\overline{G}_1 = G_1/Z(G_1) \cong A_n$ for some $n \in \mathbb{N}$; clearly $n \geq 5$. Also $N/Z \lesssim \operatorname{Aut}(\overline{G}_1)$. It is well-known that then $\dim V_0 \geq n-1$ (see [24]). Hence $|V_0| \geq |K_1|^{n-1} = (p^k)^{n-1}$. Suppose that $n \leq 1000$. Then there is a constant $D \in \mathbb{R}$ such that $|G| \leq F_\epsilon D|Z|k$, and $|Z| \leq |K_1| \leq |W|^{1/2}$, as $n-1 \geq 2$. So just as above in the case $m=0$ we can deduce that $k(HW) \leq |W|/T$ if $p > K_{\epsilon,T}$ and $K_{\epsilon,T}$ has been chosen large enough. Thus now we may assume that $n \geq 1000$. Then $N/Z \lesssim \mathrm{Aut}(A_n) = S_n$ and thus $k(L/Z) \leq 2^{n-1}$ for any $Z \leq L \leq N$. Thus for $U \leq G$ we have $k(U) \leq kF_\epsilon 2^{n-1}p^k \leq F_\epsilon 2^{n-1}|K_1|^2$. Hence if $K_{\epsilon,T}$ is sufficiently large, then for $p > K_{\epsilon,T}$ it follows that $k(U) \leq \frac{1}{8}|K_1|^{(n-1)/200} \leq \frac{1}{8}|V_0|^{1/200}$ for all $U \leq G$, and we are done in this case.

So for the rest of the proof we may assume that $\overline{G}_1$ is not an alternating group.

Suppose that G_1 acts irreducibly on W. Then choose $K_{\epsilon,T}$ large enough so that $K_{\epsilon,T} \geq \max\{(2T+2)^{1/\epsilon}, f(T^2), 3\}$, where f is as in Lemma 3.2 and suppose that $p > K_{\epsilon,T}$. Then $|H| > |W|^\epsilon/2 \geq p^\epsilon/2 \geq T+1$ and hence

$$T^2+1 = (T-1)(T+1)+2 \leq (T-1)(T+2) \leq (T-1)|H|,$$

so that $(T^2+|H|+1)/(T^2|H|) < 1/T$. Now by Lemma 3.2 (a)

$$k(HW) \leq \frac{T^2+|H|+1}{T^2|H|}|W| \leq \frac{|W|}{T},$$

as wanted.

Therefore, now we may assume that G_1 does not act irreducibly on W. Then we can write $W = W_1 \oplus W_2$ for nontrivial G_1-modules W_1, W_2, and we may assume that W_1 is irreducible, and clearly it is faithful as G_1-module.

Suppose that W_1 is not primitive as G_1-module. Then $W_1 = X_1 \oplus \cdots \oplus X_t$ for a $1 < t \leq \dim W$ and subspaces X_i, which are transitively permuted by G_1, and if $Z_1 \trianglelefteq G_1$ is the kernel of that permutation action, then $Z_1 \leq Z(G_1)$ and $G_1/Z_1 \lesssim S_t$ and $t \geq 5$. If $t \leq 1000$, then there is a constant $E \in \mathbb{R}$ such that

$$|G| \leq kF_\epsilon|N/Z|\,|Z| \leq kF_\epsilon C|\overline{G}_1|\big(\ln^2|\overline{G}_1|\big)|Z| \leq kF_\epsilon E|Z|,$$

and as $|Z| \leq |K_1| \leq |W|^{1/2}$ (since $t \geq 5$), once again just as above in the case $m=0$ we deduce that $k(HW) \leq |W|/T$ for $p > K_{\epsilon,T}$ and sufficiently large $K_{\epsilon,T}$. So let $t > 1000$. Then for any $U \leq G$ we obtain

$$k(U) \leq kF_\epsilon C\ln^2|G_1|k(G_1/Z_1)|Z_1| \leq kF_\epsilon C\ln^2(|W|^2)2^t|Z_1|,$$

and as $k \leq \log_2|K_1| \leq \log_2|W|$ and $|Z_1| \leq |X_1| \leq |W_1|^{1/1000}$, we further see that $k(U) \leq F_\epsilon C\ln^3(|W|^2)2^{\dim W}|W|^{1/1000}$, which implies our assertion in (b) (2) (α) for $p > K_{\epsilon,T}$ if $K_{\epsilon,T}$ is chosen large enough. So we are done in this case and henceforth assume that W_1 is a primitive G_1-module.

If as above again we write $Z_0 = H \cap Z$, then, as seen earlier, $k(Z_0 W) \leq 2|W|/Z_0$, and as $k(HW) \leq |H/Z_0|k(Z_0 W)$ and $|H/Z_0| \leq kF_\epsilon C|\overline{G}_1| \ln^2|\overline{G}_1|$, we may assume that $|Z_0| \leq 2TkF_\epsilon C|\overline{G}_1| \ln^2|\overline{G}_1|$, because otherwise we are done. Hence

$$|H| = |H/Z_0||Z_0| \leq 2Tk^2F_\epsilon^2C^2|\overline{G}_1|^2 \ln^4|\overline{G}_1|. \tag{7}$$

Now remember from the beginning of the proof that $G_0 = C_G(Z) \leq \mathrm{GL}(s, p^k)$, and clearly $G_1 \leq G_0$. Now as $p^{k\epsilon}/2 \leq |W|^\epsilon/2 \leq |H|$, by (7) we see that by choosing p large, then also $|\overline{G}_1|$ must get large, and as $|\overline{G}_1|$ is large, then by Jordan's Theorem as proved by Blichfeldt (see [3, Theorem 30.4]) also s gets large (as p does not divide $|G|$). So we may choose $K_{\epsilon,T}$ large enough such that for $p > K_{\epsilon,T}$ we have

$$s \geq 200(F_\epsilon + C + 4000/\epsilon + 5)$$

and

$$F_\epsilon C|\overline{G}_1|^{\epsilon/320} \ln^2|\overline{G}_1| \leq \frac{1}{2T} \min\left\{|G_1|^{\epsilon/8}, |G_1|^{1/160}\right\}.$$

Consider the case that $|Z| \leq |\overline{G}_1|^{\epsilon/640}$ and write $H_1 = H \cap G_1$. Then we have

$$|G| = |G/Z|\,|Z| \leq kF_\epsilon C|\overline{G}_1|\left(\ln^2|\overline{G}_1|\right)|\overline{G}_1|^{\epsilon/640},$$

and so, as $k \leq |Z|$ (by Fermat's little theorem), we see that

$$\begin{aligned}|H/H_1| \leq |G/G_1| &\leq \frac{|G|}{|\overline{G}_1|} \leq kF_\epsilon C|\overline{G}_1|^{\epsilon/640} \ln^2|\overline{G}_1| \\ &\leq F_\epsilon C|\overline{G}_1|^{\epsilon/320} \ln^2|\overline{G}_1| \leq \frac{1}{2T} \min\left\{|G_1|^{\epsilon/8}, |G_1|^{1/160}\right\}.\end{aligned}$$

Next observe that we may assume that $|H_1| \geq |G_1|^{\epsilon/8}$, because otherwise

$$\begin{aligned}\frac{1}{2}|W|^\epsilon < |H| &\leq kF_\epsilon|(N \cap H)/(Z \cap H)|\,|Z| \\ &\leq kF_\epsilon C|H_1|\left(|\ln^2|\overline{G}_1|\right)|Z| \leq F_\epsilon C|G_1|^{\epsilon/8} \ln^2|\overline{G}_1|\,|Z|^2 \\ &\leq F_\epsilon C|G_1|^{\epsilon/8+\epsilon/320} \ln^2|G_1| \leq F_\epsilon C|W_1|^{\epsilon/4+\epsilon/160} \ln^2(|W_1|^2),\end{aligned}$$

which for $K_{\epsilon,T}$ sufficiently large and $p > K_{\epsilon,T}$ leads to a contradiction. Hence, for $p > K_{\epsilon,T}$, by Lemma 3.1 we have $n(H_1, W_1) \leq 2|W_1|/\min\{|G_1|^{\epsilon/8}, |G_1|^{1/160}\}$. So together with Lemma 3.3 and our hypothesis we get

$$k(H_1 W) \leq n(H_1, W_1) \max_{v_1 \in W_1} k(C_{H_1}(v_1) W_2) \leq \frac{2T}{\min\{|G_1|^{\epsilon/8}, |G_1|^{1/160}\}} \frac{|W|}{T}.$$

Thus altogether $k(HW) \leq |H/H_1|k(H_1 W) \leq |W|/T$, and so we are done in this case.

It remains to consider the case that $|Z| > |\overline{G}_1|^{\epsilon/640}$. As $|Z| \leq p^k$, we then have $|\overline{G}_1| \leq |Z|^{640/\epsilon} \leq p^{1280k/\epsilon}$, and so we obtain

$$\begin{aligned}|G| &\leq kF_\epsilon C|\overline{G}_1|\left(\ln^2|\overline{G}_1|\right)|Z| \leq F_\epsilon C|\overline{G}_1|^3|Z|^2\\ &\leq F_\epsilon C p^{4000k/\epsilon} p^{2k} \leq p^{(\lceil \log_2 F_\epsilon + \log_2 C + 4000/\epsilon + 2)k}.\end{aligned}$$

Hence as $|W| = p^{sk}$ and $s \geq 200(F_\epsilon + C + 4000/\epsilon + 5)$, we see that $|G| \leq \frac{1}{8}|W|^{1/200}$, and so $k(U) \leq \frac{1}{8}|W|^{1/200}$ for all $U \leq G$. This concludes the proof of the theorem. □

4. The main result

We are now ready to prove the $k(GV)$-problem for large primes.

THEOREM 4.1. *There is a constant K with the following property: If G is a finite group and V is a finite faithful $GF(p)G$-module, where p is a prime not dividing $|G|$ such that $p > K$, then $k(GV) \leq |V|$.*

PROOF. Let (G, V) be a counterexample with $|G||V|$ minimal. It is routine to show that we may assume that V is irreducible (see, for example, the proof of [11, Theorem 4.8]).

Next suppose that G acts primitively on V. Let $J \trianglelefteq G$ be the product of $F(G)$ and all components of G which are not alternating groups of degree at least 10. Note that this is the same J that is defined in the proof of [7, Proposition 2.8]. Put $B = C_G(J) \trianglelefteq G$. Then as in the proof of [7, Proposition 2.8] we conclude that with $\epsilon_0 := 79/80$ we have $|C_V(g)| \leq |V|^{\epsilon_0}$ for all $g \in G - B$.

Now suppose that $B < G$. First suppose that $k(U) \leq |V|^{\epsilon_1}/2$ for all $U \leq G$, where $\epsilon_1 = (1 - \epsilon_0)/2 = 1/160$. Let P be the goodness property of [11, Example 3.4 (a)]. Then by induction we have $|V| \geq k(BV) = \alpha_P(B, V)$, and so [11, Remark 3.9] yields $k(GV) = \alpha_P(G, V) \leq |V|$, contradicting our choice of G and V.

So now assume $k(U) > |V|^{\epsilon_1}/2$ for some $U \leq G$, and assume the notation of Theorem 3.5 and suppose that $K > H_{\epsilon_1}$. If $K > K_{\epsilon_1,1}$, then as $k(GV) > |V|$ we conclude by induction and Theorem 3.5 that $G \leq \Gamma(V)$ in which case it is well known that $k(GV) \leq |V|$. (This follows most easily from Knörr's early result that if there is a $v \in V$ with $C_G(v)$ abelian, then $k(GV) \leq |V|$, but for large p it is also not too difficult to establish this using elementary estimates for $k(GV)$.) This contradicts our choice of G and V.

So now suppose that $B = G$. Hence $J = Z(G) =: Z$, and so there are an $l \in \mathbb{N} \cup \{0\}$ and $n_i \in \mathbb{N}$ $(i = 1, \ldots, l)$ with $n_i \geq 10$ for all i such that $F^*(G) = Z \times \bigtimes_{i=1}^{l} A_{n_i}$, and so if G_0 is the normalizer of all the components of G, then we have $G/G_0 \lesssim S_l$ and $G_0/Z \lesssim \bigtimes_{i=1}^{l} S_{n_i}$. Let $k \in \mathbb{N}$ be minimal such that $|Z| \mid p^k - 1$ and let $K = GF(p^k)$.

Then let V_0 be as in the proof of Theorem 3.5, but this time, as $G = C_G(Z)$, we see by [9, II, Hilfssatz 3.11] that $k(GV) = k(GV_0)$ and Z acts on V_0 by scalar multiplication.

Assume that $l \geq 2$ and put $s = \lfloor l/2 \rfloor$, so $1 \leq s < l$. Clearly we may assume that $\sum_{i=1}^{s} n_i \leq \sum_{i=s+1}^{l} n_i$. Let $T = Z \times \bigtimes_{i=s+1}^{l} A_{n_i} \trianglelefteq G_0$. Then as by [24] the least degree of a faithful linear representation of the alternating group A_n over a field of positive characteristic not dividing n is $n-1$, we see that if X is an irreducible T-submodule of V_0, then V_0 is the direct sum of at least

$$\frac{\dim_K V_0}{\dim_K X} \geq \prod_{i=1}^{s} (n_i - 1) =: m > 1$$

irreducible T-modules. Hence, by induction and Lemma 3.4, we conclude that

$$\begin{aligned} k(GV) = k(GV_0) &\leq k(G/G_0)k(G_0/T)k(TV_0) \\ &\leq k(G/G_0)k(G_0/T)\frac{2}{\min\{|T|, p^{k(m-1)}\}}|V_0|. \end{aligned}$$

Now as $k(G/G_0) \leq 2^{l-1}$ and $k(G_0/T) \leq 2^l \prod_{i=1}^{s} 2^{n_i - 1}$, we see that

$$t := 2k(G/G_0)k(G_0/T) \leq 2^{2l} \prod_{i=1}^{s} 2^{n_i - 1} = 2^{2(2s+1)} \frac{1}{2^s} \prod_{i=1}^{s} 2^{n_i} \leq 2^{\sum_{i=1}^{s}(n_i+5)}.$$

As $n_i \geq 10$ for all i, observe that $(n_i!)/2 \geq 2^{n_i+5}$, and therefore

$$|T| = |Z| \prod_{i=s+1}^{l} \left(\frac{n_i!}{2}\right) \geq \prod_{i=s+1}^{l} 2^{n_i+5} = 2^{\sum_{i=s+1}^{l}(n_i+5)} \geq 2^{\sum_{i=1}^{s}(n_i+5)} \geq t.$$

Moreover as $n_i \geq 10$ for all i, we also have $2m \geq \sum_{i=1}^{s}(n_i + 5)$, and so for $p \geq 16$ we get $p^{k(m-1)} \geq 2^{4m-4} \geq 2^{2m} \geq 2^{\sum_{i=1}^{s}(n_i+5)} \geq t$, so that altogether $k(GV) \leq |V_0| = |V|$, a contradiction.

Hence $l \leq 1$. If $l = 0$, then $G = Z$ and clearly $k(GV) \leq |V|$ in this case. So $l = 1$ and $G \leq S_{n_1} \times Z \leq S_{n_1} \times \Gamma(p^k)$. But then using induction and Lemma 2.2 (with $\delta = 1$) we easily obtain $k(GV) \leq |V|$, a contradiction. This concludes the case that V is primitive.

So now assume that V is an imprimitive G-module. Hence we can write $V = V_1 \oplus \cdots \oplus V_n$ for an $n > 1$ and subspaces V_i such that G transitively permutes the V_i and if $H = N_G(V_1)$, then V_1 is a primitive (and thus irreducible) H-module. Hence if $N = \bigcap_{g \in G} H^g$, then $G/N \lesssim S_n$. Define successively $N_0 = N$ and $N_i = N_{i-1}/C_{N_{i-1}}(V_i)$ for $i = 1, \ldots, n$. Then

$$k(GV) \leq k(G/N) \prod_{i=1}^{n} k(N_i V_i) \leq 2^{n-1} \prod_{i=1}^{n} k(N_i V_i). \tag{8}$$

https://doi.org/10.1017/S144678870001048X Published online by Cambridge University Press

Clearly by induction $k(N_iV_i) \leq |V_i|$ for all i, and also $|N_i| \leq |V_i|^2$. Moreover, $k(G) \leq 2^{n-1}\prod_{i=1}^n k(N_i)$.

Assume that we have $k(U) \leq |V_1|^{1/16}/4$ for all $U \leq N_i$ for $\lceil 31n/32 \rceil$ values of i. Then for any $U \leq G$ we have

$$\begin{aligned} k(U) &\leq 2^{n-1}\left(\frac{|V_1|^{1/16}}{4}\right)^{\lceil 31n/32\rceil}\left(|V_1|^2\right)^{n-\lceil 31n/32\rceil} \\ &\leq \frac{1}{2}|V|^{(1/16)(31/32)+1/16} \leq \frac{1}{2}\frac{|V|^{1/8}}{|V|^{1/512}} \leq \frac{1}{2}\frac{1}{\sqrt{n+1}}|V|^{1/8}, \end{aligned}$$

where the last inequality holds if $p > K$ and K is chosen sufficiently large. So by induction and Lemma 2.2 (with $\delta = 1$) we obtain $k(GV) \leq |V|$, a contradiction.

Therefore there are at least $n - (\lceil 31n/32 \rceil - 1) \geq n/32$ values of i such that there is a $U_i \leq N_i$ with $k(U_i) > |V_1|^{1/16}/4 \geq |V_1|^{1/32}/2$ (for large p). Let $I \subseteq \{1, \ldots, n\}$ be the set of those indices i. In particular, $|N_1| > |V_1|^{1/32}/2$, and as V_1 is a primitive faithful N_1-module, Theorem 3.5 applies. So let the notation (as far as possible) be as in that lemma.

If $N_1 \leq \Gamma(V_1)$, then we are done by Lemma 2.3.

Hence by Theorem 3.5 there are two cases to consider:

(1) $k(U) \leq |V_1|^{1/200}/$ for all $U \leq N_1$; or

(2) $k(UV_1) \leq |V_1|/T$ for all $U \leq N_1$ with $|U| > |V_1|^{1/32}/2$, if $p > K_{1/32,T}$.

Observe that $N_i \lessapprox N_1$ for all i, and so as $I \neq \emptyset$, Case (1) cannot occur. Hence suppose (2) and put $T_0 = 2^{32}$. Clearly $|N_i| \geq |U_i| \geq k(U_i) > |V_1|^{1/32}/2$ for $i \in I$. Therefore, (8) yields

$$k(GV) \leq 2^{n-1}\prod_{i\in I}k(N_iV_i)\prod_{i\notin I}k(N_iV_i) \leq 2^{n-1}\left(\frac{|V_1|}{T_0}\right)^{|I|}|V_1|^{n-|I|} \leq \frac{2^{n-1}}{T_0^{n/32}}|V| \leq |V|,$$

contradicting our choice of (G, V). This final contradiction completes the proof of the theorem. □

References

[1] M. Aschbacher, 'On the maximal subgroups of the finite classical groups', *Invent. Math.* **76** (1984), 469–514.

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

[3] L. Dornhoff, *Group representation theory. Part A: Ordinary representation theory* (Marcel Dekker, New York, 1971).

[4] D. Frohardt and K. Magaard, 'Composition factors of monodromy groups', *Ann. of Math. (2)* **154** (2001), 327–345.
[5] P. X. Gallagher, 'The number of conjugacy classes in a finite group', *Math Z.* **118** (1970), 175–179.
[6] A. Gambini Weigel and T. S. Weigel, 'On the orders of primitive linear p'-groups', *Bull. Austral. Math. Soc.* **48** (1993), 495–521.
[7] D. Gluck and K. Magaard, 'Base sizes and regular orbits for coprime affine permutation groups', *J. London Math. Soc.* **58** (1998), 603–618.
[8] D. Gluck, K. Magaard, U. Riese and P. Schmid, 'The solution of the $k(GV)$-problem', *J. Algebra* **279** (2004), 694–719.
[9] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).
[10] ———, *Character theory of finite groups* (deGruyter, Berlin, 1998).
[11] T. M. Keller, 'A new approach to the $k(GV)$-problem', *J. Austral. Math. Soc.* **75** (2003), 193–219.
[12] ———, 'Orbits in finite group actions', in: *Groups St. Andrews 2001 in Oxford*, London Math. Soc. Lecture Notes Series 305 (Cambridge University Press, 2003) pp. 306–331.
[13] M. W. Liebeck, 'Regular orbits of linear groups', *J. Algebra* **184** (1996), 1136–1142.
[14] M. W. Liebeck and L. Pyber, 'Upper bounds for the number of conjugacy classes of a finite group', *J. Algebra* **198** (1997), 538–562.
[15] M. W. Liebeck and A. Shalev, 'Diameters of finite simple groups: sharp bounds and applications', *Ann. of Math. (2)* **154** (2001), 383–406.
[16] R. Lyons, *Finite group theory*, Notes for Math. 555, unpublished, 1999.
[17] O. Manz and T. R. Wolf, *Representations of solvable groups*, London Math. Soc. Lecture Notes Series 185 (Cambridge University Press, 1993).
[18] G. Navarro, *Characters and blocks of finite groups*, London Math. Soc. Lecture Notes Series 250 (Cambridge University Press, 1998).
[19] I. Pak, 'On probability of generating a finite group', unpublished manuscript, 1999.
[20] P. P. Pálfy and L. Pyber, 'Small groups of automorphisms', *Bull. London Math. Soc.* **30** (1998), 386–390.
[21] U. Riese, 'On the number of irreducible characters in a block', *Algebra Colloq.* **10** (2003), 381–390; see `www-math.mit.edu/~pak/research.html`.
[22] G. R. Robinson and J. G. Thompson, 'On Brauer's $k(B)$-problem', *J. Algebra* **184** (1996), 1143–1160.
[23] A. Shalev, 'Fixed point ratios, character ratios, and Cayley graphs', in: *Combinatorial and computational Algebra (Hong Kong, 1999)*, Contemp. Math. 264 (2000) pp. 49–59.
[24] A. Wagner, 'The faithful linear representations of least degree of S_n and A_n over a field of odd characteristic', *Math. Z.* **154** (1977), 103–114.

Department of Mathematics
Texas State University
601 University Drive
San Marcos, TX 78666
USA
e-mail: keller@txstate.edu