J. Aust. Math. Soc. 75 (2003), 193–219

A NEW APPROACH TO THE $k(GV)$-PROBLEM

THOMAS MICHAEL KELLER

(Received 20 November 2001; revised 22 May 2002)

Communicated by R. B. Howlett

Abstract

This paper is concerned with the well-known and long-standing $k(GV)$-problem: If the finite group G acts faithfully and irreducibly on the finite $GF(p)$-module V and p does not divide the order of G, is the number $k(GV)$ of conjugacy classes of the semidirect product GV bounded above by the order of V?

Over the past two decades, through the work of numerous people, by using deep character theoretic arguments this question has been answered in the affirmative except for $p = 5$ for which it is still open. In this paper we suggest a new approach to the $k(GV)$-problem which is independent of most of the previous work on the problem and which is mainly group theoretical. To demonstrate the potential of the new line of attack we use it to solve the $k(GV)$-problem for solvable G and large p.

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

1. Introduction

A long-standing problem (dating back to the 1950s) in the modular representation theory of finite groups is Brauer's $k(B)$-problem stating that if B is a p-block of a finite group G, then the number $k(B)$ of ordinary irreducible characters in B is bounded above by the order of the defect group of B. For p-solvable groups Nagao [20] showed that this problem is equivalent to what has become known as the $k(GV)$-problem:

If V is a finite irreducible faithful $GF(p)G$-module of the finite group G such that $(|G|, |V|) = 1$, then the number $k(GV)$ of conjugacy classes of the semidirect product GV is bounded above by the number of elements of V, that is, $k(GV) \leq |V|$.

This difficult problem has been thoroughly investigated during the past two decades and for a long time stubbornly resisted all efforts to solve it, but by now through the combined efforts of many mathematicians major results have been obtained. The first

https://doi.org/10.1017/S1446788700003724 Published online by Cambridge University Press

significant breakthrough is due to Knörr [13] who proved the $k(GV)$-problem for supersolvable groups. Even more important than this actual result are the character theoretic techniques that he developed in his influential paper. Most remarkably, all other significant contributions to the solution of the problem are extensions of Knörr's approach. Early extensions due to Gluck, Knörr, Gow, Robinson and others culminated in the well-known paper [25] by Robinson and Thompson solving the problem for arbitrary groups and large p. The proof heavily depends on deep character theoretic arguments.

Since then, all efforts concerning the $k(GV)$-problem centered around refining this proof to make it work for smaller primes p, and by work of Robinson [24], Goodwin [6, 7], Gluck and Magaard [4], Koehler and Pahlings [14], Schmid and Riese [22], Riese [21] the problem has been solved for all primes for which the Robinson-Thompson method can be applied. Recently in work of Gluck [5] and Riese and Schmid [23] all the remaining primes have been settled with the exception of $p = 5$.

So while the actual results to the $k(GV)$-problem are very satisfying, the methods used to solve it, which Gluck in his review of Gow's paper called 'powerful, but rather mysterious' (see MR 94i:20020), remain so even today. Thus a deeper insight into the mechanics of the problem remains highly desirable.

In this work, therefore, we will present a powerful 'Knörr-free' approach to the problem. As such this paper is independent of most of the work previously done on the $k(GV)$-problem. (For a different approach of a somewhat similar spirit, see [18, 19].)

One of the main difficulties is that the $k(GV)$-problem has a bad inductive behaviour which is why slightly stronger, but with respect to induction better behaved conditions were sought to make proofs work. Our approach however is elementary (albeit highly nontrivial) and based on the inductive behaviour of $k(GV)$ itself. At the same time it deals with another curiosity of the history of the $k(GV)$-problem. Namely there are some very elementary and beautiful formulas for $k(GV)$ which one would expect to play a major role in any serious approach to the $k(GV)$-problem—but they do not. They even have been hardly of any use at all so far. In this paper now we will slightly, but decisively, generalize these formulas such as to rendering them more suitable for an inductive argument, and then we will heavily use them, thus showing that they are more useful than they appeared to be.

The power of our new approach to the $k(GV)$-problem will be demonstrated by using it to settle the $k(GV)$-problem for solvable groups and large primes p. Just as was the case with Knörr's strategy, the method presented here has potential of being extended to work for arbitrary groups (and large primes), but the approach developed here is more group-theoretical and as such more elementary. It is hoped that the ideas developed in this paper eventually will lead to an elementary, possibly purely group-theoretical, solution of the $k(GV)$-problem in general.

The paper is organized as follows: In Section 3 we will generalize well-known formulas for the class number of a group and outline the key ideas of the new line of attack on the $k(GV)$-problem, which in Section 4 will be used to solve it for solvable groups and large primes p. It will become obvious that the proof for $|G|$ odd is a lot easier than the proof for $|G|$ even; Lemmas 4.5–4.7 are needed exclusively to deal with a special case in which $|G|$ is even. Finally in Section 5 we will give a brief outlook on possible extensions of this work and open questions that arise from it.

2. Notation

All groups in this paper are finite. $A \lesssim B$ means that the group A is isomorphic to a subgroup of B. If a finite group G acts on a finite vector space V, then by $n(G, V)$ we denote the number of orbits in the action of G and V, that is, $n(G, V) = |\{v^G | v \in V\}|$.

By $\mathrm{cl}(G)$ we denote the set of conjugacy classes of a group G, and $k(G) = |\mathrm{cl}(G)|$, and if S is a set, then $\mathscr{P}(S)$ is its power set. $\mathrm{Irr}(G)$ is the set of irreducible complex characters of G.

When we say that a group G acts on a set Ω, this means that every $g \in G$ permutes the elements of Ω and for any $g, h \in G$ and $\omega \in \Omega$ we have $(\omega^g)^h = \omega^{gh}$. In particular, the permutation action of G on Ω need not be faithful. For $g \in G$ we write $C_\Omega(g)$ for the set of fixed points of g on Ω, so $C_\Omega(g) = \{\omega \in \Omega \mid \omega^g = \omega\}$ (where the group action is written exponentially), and for $\omega \in \Omega$ let $C_G(\omega) = \{g \in G \mid \omega^g = \omega\}$.

Moreover, if a group G acts on a group V such that the corresponding semidirect product GV is a Frobenius group, then we say G acts fixed point freely on V, and an element $g \in G$ is said to act fixed point freely on V if $\langle g \rangle V$ is a Frobenius group.

As in [17, Section 2], for $V = GF(q^m)$ (where q is a prime power and $m \in \mathbb{N}$) we let $\Gamma(V) = \{x \mapsto ax^\sigma | a \in GF(q^m)^\#,\ \sigma \in \mathrm{Gal}(GF(q^m)/GF(q))\}$ and $\Gamma_0(V) = \{x \mapsto ax | a \in GF(q^m)^\#\} \leq \Gamma(V)$. Moreover we use $\dot\bigcup$ to indicate disjoint unions.

3. Goodness

We first introduce the notion of a goodness property and study a few important examples, which will yield group theoretical proofs for two well-known formulas for $k(GV)$ (see Corollary 3.7).

DEFINITION 3.1. Let G be a group acting (not necessarily faithfully) on the finite set Ω. Let S be the set of all subgroups of G, and put $T = \bigcup_{U \in S} \mathscr{P}(\mathrm{cl}(U))$. Suppose that there is a function $P : S \times \Omega \to T$ such that for any $U \leq G$, $\omega \in \Omega$ we have $P(U, \omega) \subseteq \mathrm{cl}(C_U(\omega))$. Then we call P a *goodness property* and say that the classes in $P(U,\omega)$ are *P-good* for ω in U. Moreover, if $g \in C_U(\omega)$ and $g^{C_U(\omega)}$ is P-good for ω in U, then we say that g is P-good for ω in U. For any $U \le G$, $g \in U$ put

$$\Omega(U,g) = \{\omega \in C_\Omega(g) \mid g \text{ is } P\text{-good for } \omega \text{ in } U\}.$$

We also write $P(U,\omega) =: \mathrm{cl}_P(C_U(\omega))$, and $|P(U,\omega)| =: k_P(C_U(\omega))$ is the number of P-good classes for ω in U.

Finally the goodness property P is *special* if for all $U \le G$, $\omega \in \Omega$, $u \in U$ we have $k_P(C_U(\omega)) = k_P(C_U(\omega^u))$.

DEFINITION 3.2. Let G be a group that (not necessarily faithfully) permutes the elements of the finite set Ω and let P be a goodness property. Then we define

$$\alpha_P(G,\Omega) = \sum_{\omega\in\Omega} \frac{|C_G(\omega)|\, k_P(C_G(\omega))}{|G|}.$$

If P is special, then clearly $\alpha_P(G,\Omega) = \sum_{i=1}^{n(G,\Omega)} k_P(C_G(\omega_i))$ (where ω_i, $i = 1,\dots, n(G,\Omega)$, are representatives of the orbits of G on Ω).

REMARK 3.3. Suppose P is special. Using the Cauchy-Frobenius orbit counting formula (also known as Burnside's lemma), we obtain

$$\begin{aligned}
\alpha_P(G,\Omega) &= \frac{1}{|G|}\sum_{\omega\in\Omega} |C_G(\omega)| k_P(C_G(\omega)) \\
&= \frac{1}{|G|}\sum_{\omega\in\Omega} |C_G(\omega)| \frac{1}{|C_G(\omega)|} \sum_{\substack{g\in C_G(\omega),\\ g \text{ is } P\text{-good for } \omega \text{ in } G}} |C_{C_G(\omega)}(g)| \\
&= \frac{1}{|G|}\sum_{\omega\in\Omega} \sum_{\substack{g\in C_G(\omega),\\ g \text{ is } P\text{-good for } \omega \text{ in } G}} |C_G(\omega)\cap C_G(g)| \\
&= \frac{1}{|G|}\sum_{g\in G} \sum_{\substack{\omega\in C_\Omega(g),\\ \text{with } g\ P\text{-good for } \omega \text{ in } G}} |C_G(\omega)\cap C_G(g)| \\
&= \frac{1}{|G|}\sum_{g\in G} \sum_{\omega\in\Omega(G,g)} |C_{C_G(g)}(\omega)|.
\end{aligned}$$

Thus if $\Omega(G,g)$ is $C_G(g)$-invariant for all $g \in G$, then we further conclude (using the orbit counting formula again) that

$$\begin{aligned}
\alpha_P(G,\Omega) &= \frac{1}{|G|}\sum_{g\in G} |C_G(g)| \frac{1}{|C_G(g)|} \sum_{\omega\in\Omega(G,g)} |C_{C_G(\omega)}(\omega)| \\
&= \frac{1}{|G|}\sum_{g\in G} |C_G(g)|\, n(C_G(g), \Omega(G,g))
\end{aligned}$$

If in addition $n(C_G(g), C_{\Omega(G,g)}(g)) = n(C_G(g^h), \Omega(G, g^h))$ for any $h \in G$, then even $\alpha_P(G, \Omega) = \sum_{i=1}^{k(G)} n(C_G(g_i), \Omega(G, g_i))$ where g_i $(i = 1, \dots, k(G))$ are representatives of the conjugacy classes of G.

EXAMPLE 3.4. The following special cases of goodness properties are of particular interest:

(a) Let G be a group acting on the finite set Ω and put $P(U, \omega) = \mathrm{cl}(C_U(\omega))$. Clearly this is a special goodness property, and for $U \leq G$ and $g \in U$ obviously $\Omega(U, g) = C_\Omega(g)$.

(b) Let G be a group and $N \trianglelefteq G$. Then G/N acts on $\mathrm{Irr}(N)$, and if $\psi \in \mathrm{Irr}(N)$ and $N \leq U \leq G$, then in [2, p. 177] Gallagher defines what it means for a conjugacy class of $C_{U/N}(\psi)$ to be *good* for ψ, and shows that it depends only on ψ and the conjugacy class in $C_{U/N}(\psi)$. Thus if we define

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

then clearly P is a goodness property, and by the Theorem in [2], $k_P(C_{U/N}(\psi))$ is equal to the number of irreducible characters of G lying above ψ. In particular, from this it is clear that P is special. We call P *Gallagher's goodness property*. Observe that by [2] it follows that $k(U) = \alpha_P(U/N, \mathrm{Irr}(N))$ for any $N \leq U \leq G$.

We next develop a group theoretical counterpart to Gallagher's goodness property.

DEFINITION 3.5. Let G be a group and $N \trianglelefteq G$. Let $\Omega = \Omega_N(G) := \{g^N \mid g \in G\}$ be the set of N-orbits as N acts on G by conjugation. Clearly G/N acts on Ω by conjugation. Note that for $g \in G$ obviously $g^N \subseteq gN$, as for $x \in N$ we have $g^x = g[g, x]$. Let $N \leq U \leq G$, $g \in U$ and $\omega \in \Omega$. We say that $gN \in U/N$ is *good* for ω in U/N if $\omega \subseteq gN$. Note that if $cN \in C_{U/N}(\omega)$, then also $\omega \subseteq (gN)^{cN} = g^cN$, that is, also $g^cN = (gN)^{cN}$ is good for ω in U/N. Hence we can define that $(gN)^{C_{U/N}(\omega)}$ is good for ω in U/N if $\omega \subseteq gN$. Therefore if we define

$$P(U/N, \omega) = \{(gN)^{C_{U/N}(\omega)} \mid \omega \subseteq gN \in C_{U/N}(\omega)\} \subseteq \mathrm{cl}(C_{U/N}(\omega)),$$

then P is a goodness property. It is easy to see that P is special. Clearly $P(U/N, \omega) = \{xN\}$ for any $x \in \omega$ and thus $k_P(C_{U/N}(\omega)) = 1$ for all ω.

LEMMA 3.6. *Let the notation be as in Definition* 3.5. *Then the following hold*:

(a) *Let g_iN $(i = 1, \dots, k(G/N))$ be representatives of the conjugacy classes of G/N. Then $k(G) = \sum_{i=1}^{k(G/N)} n(C_{G/N}(g_iN), \Omega(G/N, g_iN))$, where (in accordance with Definition* 3.1) $\Omega(G/N, gN) = \{\omega \in \Omega \mid \omega \subseteq gN\}$.

(b) $k(G) = \alpha_P(G/N, \Omega) = n(G/N, \Omega)$.

PROOF. (a) Let $h_i \in G$ $(i = 1, \dots, |G/N|)$ be representatives of the cosets of N in G. Let $g \in G$. Then $g = h_i v$ for some i and some $v \in N$. We may assume that $i = 1$. Thus $g^G = (h_1 v)^G = \bigcup_{i=1}^{|G/N|} (h_1 v)^{Nh_i} \subseteq \bigcup_{i=1}^{|G/N|} (h_1 N)^{h_i} = \bigcup_{i=1}^{|G/N|} h_1^{h_i} N$. Now also let $g' \in G$ so that $g' = h_l v_0$ for some l and some $v_0 \in N$. Then likewise

$$(g')^G = \bigcup_{i=1}^{|G/N|} (h_l v_0)^{Nh_i} \subseteq \bigcup_{i=1}^{|G/N|} h_l^{h_i} N.$$

Now we observe the following:
(1) If $g^G = (g')^G$, then $h_1 v \in h_l^{h_i} N$ for some i, so $h_1 \in h_l^{h_i} N$ for some i, whence $h_1 = h_l^{h_i} x$ for some i and some $x \in N$. This is equivalent to saying $h_1 N = h_l^{h_i} N$ which means that $h_1 N$ and $h_l N$ are in the same conjugacy class of G/N.
(2) Suppose that $h_1 N$ and $h_l N$ are G/N-conjugate, so that $h_1^{h_{j_0}} N = h_l N$ for some j_0. Write $h_l = h_1^{h_{j_0}} y$ for some $y \in N$ and $z = (y v_0)^{h_{j_0}^{-1}} \in N$. Then $g' = h_l v_0 = h_1^{h_{j_0}} y v_0 = (h_1 z)^{h_{j_0}}$ and so $(g')^G = (h_1 z)^G = \bigcup_{i=1}^{|G/N|} ((h_1 z)^N)^{h_i}$.

Next let $d_i \in G$ $(i = 1, \dots, m := |(G/N)/C_{G/N}(h_1 N)|)$ such that the $d_i N$ are representatives of the right cosets of $C_{G/N}(h_1 N)$ in G/N. Moreover let $l_i \in G$ $(i = 1, \dots, n := |C_{G/N}(h_1 N)|)$ such that $C_{G/N}(h_1 N) = \{e_i N \mid i = 1, \dots, n\}$. Then

$$G/N = \dot{\bigcup_{i=1}^{m}} C_{G/N}(h_1 N) d_i = \{N e_j d_i \mid j = 1, \dots, n,\ i = 1, \dots, m\},$$

and the $e_j d_i$ are representatives of the cosets of N in G. We then may assume that $\{h_1, \dots, h_{|G/N|}\} = \{e_j d_i \mid j = 1, \dots, n;\ i = 1. \dots, m\}$ and that $h_1 = e_1 d_1$. Moreover, as $(h_1 N) = (h_1 N)^{e_j N} = h_1^{e_j} N_1$, clearly $h_1^{e_j} = h_1 n_j$ for some $n_j \in N$ (for all j). Hence we obtain

$$\begin{aligned} g^G &= \bigcup_{i=1}^{|G/N|} (h_1 v)^{Nh_i} = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} (h_1 v)^{N e_j d_i} = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} (h_1 n_j v^{e_j})^{N d_i} \\ &= \bigcup_{i=1}^{m} \left(h_1^{d_i} \bigcup_{j=1}^{n} \{(n_j v^{e_j})^{d_i}\} \right)^N \subseteq \bigcup_{i=1}^{m} h_1^{d_i} N. \end{aligned}$$

Observe that for all $i_1, i_2 \in \{1, \dots, m\}$ we have $h_1^{d_{i_1}} N \cap h_1^{d_{i_2}} N = \emptyset$, and so we even have

$$g^G = \dot{\bigcup_{i=1}^{m}} \left(h_1^{d_i} \bigcup_{j=1}^{n} \{(n_j v^{e_j})^{d_i}\} \right)^N .$$

Now analogously we obtain

$$(g')^G = (h_1 z)^G = \dot{\bigcup_{i=1}^{m}} \left(h_1^{d_i} \bigcup_{j=1}^{n} \{(n_j z^{e_j})^{d_i}\} \right)^N$$

and so we see that $g^G = (g')^G$ if and only if

$$\left(h_1^{d_i}\bigcup_{j=1}^{n}\{(n_j v^{e_j})^{d_i}\}\right)^N = \left(h_1^{d_i}\bigcup_{j=1}^{n}\{(n_j z^{e_j})^{d_i}\}\right)^N \quad \text{for } i = 1, \dots, m,$$

that is,

$$(*) \qquad \left(h_1\bigcup_{j=1}^{n}\{n_j v^{e_j}\}\right)^N = \left(h_1\bigcup_{j=1}^{n}\{n_j z^{e_j}\}\right)^N$$

Now the left-hand side of $(*)$ equals

$$\bigcup_{j=1}^{n}(h_1 n_j v^{e_j})^N = \bigcup_{j=1}^{n}(h_1 v)^{Ne_j} = \bigcup_{j=1}^{n}(g^N)^{e_j} = \bigcup_{j=1}^{n}(g^N)^{e_j N} = \bigcup_{x\in C_{G/N}(h_1N)}(g^N)^x,$$

and analogously the right-hand side of $(*)$ equals

$$\bigcup_{j=1}^{n}(h_1 z)^{Ne_j} = \bigcup_{j=1}^{n}((g')^{h_{j_0}^{-1}})^{Ne_j} = \bigcup_{x\in C_{G/N}(h_1N)}((g')^{h_{j_0}^{-1}})^{Nx}.$$

Consequently, $g^G = (g')^G$ if and only if $g^N = (h_1 v)^N$ and $((g')^{h_{j_0}^{-1}})^N = (h_1 z)^N$ lie in the same orbit of $C_{G/N}(h_1N) = C_{G/N}(gN)$ on $\Omega(G/N, gN)$ (note that $g^N \subseteq gN$ and $((g')^{h_{j_0}^{-1}})^N \subseteq (g')^{h_{j_0}^{-1}}N = h_1 zN = h_1 N = gN$).

Combining our findings in (1) and (2) yields that for any $g, g' \in G$ we have $g^G = (g')^G$ if and only if (i) $(gN)^t = g'N$ for some $t \in G$ and (ii) g^N and $((g')^{t^{-1}})^N$ lie in the same orbit of $C_{G/N}(gN)$ on $\Omega(G/N, gN)$. From this we see that (a) follows.
(b) Observe that for any $gN, hN \in G/N$ we have

$$n(C_{G/N}(gN), \Omega(G/N, gN)) = n(C_{G/N}(g^hN), \Omega(G/N, g^hN))$$

and furthermore clearly $\Omega(G/N, gN)$ is $C_{G/N}(gN)$-invariant for all $g \in G$. So the assertion follows from Remark 3.3 and the fact that $k_P(C_{U/N}(\omega)) = 1$ for all $\omega \in \Omega$, and the lemma is proved. $\square$

Note that from the formula in Lemma 3.6 (a) it is clear that for any $N \leq U \leq G$ we have

$$k(U) = \sum_{i=1}^{k(U/N)} n(C_{U/N}(h_iN), \Omega(G/N, h_i))$$

(where the h_iN are representatives of the conjugacy classes of U/N), because $\Omega(G/N, h_i) = \Omega(U/N, h_i)$.

Lemma 3.6 is a generalization of a well-known formula for $k(GV)$ in the setting of the $k(GV)$-problem, as we shall see next.

https://doi.org/10.1017/S1446788700003724 Published online by Cambridge University Press

COROLLARY 3.7. *Let G be a group and V be a finite G module with $(|G|, |V|) = 1$. Then the following hold:*

(a) *Let $g_i \in G$ $(i = 1, \dots, k(G))$ be representatives of the conjugacy classes of G. Then*

$$k(GV) = \sum_{i=1}^{k(G)} n(C_G(g_i), C_V(g_i)) = \frac{1}{|G|}\sum_{g\in G}|C_G(g)|n(C_G(g), C_V(g)).$$

(b) *Let $v_i \in V$ $(i = 1, \dots, n(G, V))$ be representatives of the orbits of G on V. Then*

$$k(GV) = \sum_{i=1}^{n(G,V)} k(C_G(v_i)) = \frac{1}{|G|}\sum_{v\in V}|C_G(v)|k(C_G(v)).$$

PROOF. (a) Apply Lemma 3.6 (a) to the group GV with the normal subgroup V and write the addition on V multiplicatively.

Observe that

$$\begin{aligned}\Omega(GV/V, gV) &= \{(hv)^V \mid h \in G, v \in V \text{ with } (hv)^V \subseteq gV\}\\ &= \{(gv)^V \mid v \in V\} = \{g^V v \mid v \in V\} = \{g[\langle g\rangle, V]v \mid v \in V\},\end{aligned}$$

where the last equality holds as $[\langle g\rangle, V] = \{[g, v] \mid v \in V\}$ by the well-known rules for commutators and because V is abelian. Now as $(|G|, |V|) = 1$, we see that $\{[\langle g\rangle, V]v \mid v \in V\} = V/[\langle g\rangle, V] \cong C_V(g)$ (as $C_G(g)$-module), and so clearly $\Omega(GV/V, gV) \cong gC_V(g) \cong C_V(g)$ as $C_G(g)$-modules. So by Lemma 3.6 (a) the first formula follows, and the second formula easily follows from the first.

(b) Let P be the (trivial) goodness property from Example 3.4 (a) with respect to the action of G on V. Then we observe that $\Omega(G, g) = C_V(g)$ and also that P is special and $\Omega(G, g)$ is $C_G(g)$-invariant for all $g \in G$. Hence Remark 3.3 yields the second formula in (b), and the first formula is an immediate consequence of the second. The proof of the corollary is thus complete. □

The formula in (b) can also be seen as a special case of the formula for $k(G)$ in Example 3.4 (b).

Note that the formulas in Corollary 3.7 have been known for a long time, since they are special cases of the well-known group theoretic fact that if π is a set of primes and G a finite group, then $k(G)$ is the sum of the number of conjugacy classes of π'-elements of $C_G(x)$ as x runs over a set of representatives of the conjugacy classes of π-elements of G.

Observe that another consequence of Lemma 3.6 is the well-known formula $k(G) \leq k(G/N)k(N)$ for $N \trianglelefteq G$, as is easy to see. We will use this formula freely in the remainder of this paper.

We now present the key idea that our approach to the $k(GV)$-problem is based on. It is the following easy lemma.

LEMMA 3.8. *Let G be a group acting on the finite set Ω, and let P be a goodness property. Suppose that there is a $b \in \mathbb{N}$, a $0 < \epsilon < 1$ and an $N \leq G$ such that the following hold*:

(i) $\alpha_P(N, \Omega) \leq b$;

(ii) $|C_\Omega(g)| \leq b^\epsilon$ *for all* $g \in G - N$;

(iii) $|G| \leq b^{(1-\epsilon)/2}/\sqrt{2}$.

Then $\alpha_P(G, \Omega) \leq b$.

PROOF. Clearly we may assume that $N < G$. Let $T = \{\omega \in \Omega \mid C_G(\omega) \not\leq N\}$. Observe that $\omega \in T$ means that there is a $g \in G - N$ with $\omega \in C_\Omega(g)$. Hence $T \subseteq \bigcup_{g \in G-N} C_\Omega(g)$ and thus $|T| \leq |G - N|b^\epsilon \leq |G|b^\epsilon$.

With this we find

$$\begin{aligned}
\alpha_P(G, \Omega) &= \sum_{\omega \in T} \frac{|C_G(\omega)|\, k_P(C_G(\omega))}{|G|} + \sum_{\omega \in \Omega - T} \frac{|C_G(\omega)| k_P(C_G(\omega))}{|G|} \\
&\leq |T||G| + \frac{1}{|G:N|} \sum_{\omega \in \Omega} \frac{|C_N(\omega)|\, k_P(C_N(\omega))}{|N|} \\
&\leq |G|^2 b^\epsilon + \frac{1}{|G:N|} \alpha_P(N, \Omega) \\
&\leq |G|^2 b^\epsilon + \frac{1}{2} b \leq \frac{1}{2} b^{1-\epsilon} b^\epsilon + \frac{1}{2} b \leq b,
\end{aligned}$$

as wanted. $\square$

REMARK 3.9. If in Lemma 3.8 in addition we assume that P is special and $N \trianglelefteq G$, then we can replace Hypothesis (iii) by the weaker hypothesis

(iii′) $k(U) \leq b^{(1-\epsilon)/2}/\sqrt{2}$ for all $U \leq G$.

To see this, let $T_1 = \{\omega^G \mid \omega \in \Omega \text{ with } C_G(\omega) \not\leq N\}$; so $\omega^G \in T_1$ means that there is a $g \in G - N$ such that g fixes an element of ω^G, that is, $\omega^G \cap C_\Omega(g) \neq \emptyset$. Hence $\omega^G \cap C_\Omega(g^h) \neq \emptyset$ for all $h \in G$. This shows that if g_i, $i = 1, \ldots, t$, are representatives of the conjugacy classes of G which are not in N, then

$$T_1 \subseteq \bigcup_{i=1}^{t} \{\omega^G \mid \omega \in \Omega \text{ and } \omega^G \cap C_\Omega(g_i) \neq \emptyset\}$$

and thus $|T_1| \leq t \max_{i=1,\ldots,t} |C_\Omega(g_i)| \leq k(G)b^\epsilon$. Now consider $\omega^G \notin T_1$. Thus $C_G(\omega) = C_N(\omega)$ and so $|\omega^G| > |\omega^N|$, and as G/N permutes the orbits of N on Ω, we

https://doi.org/10.1017/S1446788700003724 Published online by Cambridge University Press

see that ω^G is the disjoint union of at least two mutually distinct G-conjugate N-orbits on Ω. Hence if ω_i ($i = 1, \dots, n(G, \Omega)$) are representatives of the orbits of G on Ω, then

$$\begin{aligned} \sum_{i \text{ with } \omega_i^G \notin T_1} k_P(C_N(\omega_i)) &= \frac{1}{2} \sum_{i \text{ with } \omega_i^G \notin T_1} 2k_P(C_N(\omega_i)) \\ &\leq \frac{1}{2} \sum_{j=1}^{n(N,\Omega)} k_P(C_N(\alpha_j)) = \frac{1}{2}\alpha_P(N, \Omega), \end{aligned}$$

where the α_j are representatives of the N-orbits on Ω.

So altogether with our hypothesis we obtain

$$\begin{aligned} \alpha_P(G, \Omega) &= \sum_{i \text{ with } \omega_i^G \in T_1} k_P(C_G(\omega_i)) + \sum_{i \text{ with } \omega_i^G \notin T_1} k_P(C_N(\omega_i)) \\ &\leq |T_1| \cdot \frac{1}{\sqrt{2}} b^{(1-\epsilon)/2} + \frac{1}{2}\alpha_P(N, \Omega) \\ &\leq k(G) b^{\epsilon} \frac{1}{\sqrt{2}} b^{(1-\epsilon)/2} + \frac{1}{2} b \leq b^{\epsilon} \frac{1}{2} b^{1-\epsilon} + \frac{1}{2} b = b, \end{aligned}$$

as desired.

4. On the $k(GV)$-problem

In this section we give a new proof of the $k(GV)$-conjecture for solvable groups and large primes p, that is, $p > K$ for some constant $K \in \mathbb{N}$, using the ideas developed in Section 3. Note that no effort has been made to keep K small, but rather we are satisfied with large K to make the proofs as short and smooth as possible. Due to the nature of the problem still some technicalities cannot be avoided.

We begin with a series of auxiliary lemmas, some of which may be of independent interest.

The first lemma studies the case of quasiprimitive group actions, and therefore we will make use of the detailed analysis of solvable groups whose normal abelian subgroups are all cyclic, which can be found in [17, Section 1] (see, in particular, Corollary 1.10 of that book). We recall from there that if $F = F(G)$ is the Fitting subgroup of G, then there exist normal subgroups E, T of G such that $F = ET$, $Z = E \cap T$ and $T = C_F(E)$. Moreover, all Sylow subgroups of E are cyclic of prime order or extraspecial of exponent a prime or 4, and there exists a $U \leq T$ of index at most 2 with U cyclic, $U \trianglelefteq G$ and $C_T(U) = U$.

LEMMA 4.1. *Let G be a solvable group acting faithfully and irreducibly on a finite vector space V over $GF(p)$, where p is a prime. Suppose that the action of G on V*

is quasiprimitive so that every normal abelian subgroup of G is cyclic, and we adopt the above notation and write $e^2 = |E/Z|$. Then the following hold:

(a) $|G| \le k|U|e^{13/2}$, *where k is the dimension of any irreducible Z-submodule of V.*
(b) *If $p > 3^{112}$ and $e \ge 9$, then $|G| \le (1/3)|V|^{1/8}$.*
(c) *If $(|G|, |V|) = 1$ and $p > 2^{112}$, then $k(GV) \le |V|$.*

PROOF. Write $n = \dim V$. Observe that by hypothesis V_Z is homogeneous, so write $V_Z = s \cdot X$ for an $s \in \mathbb{N}$ and an irreducible Z-module X. By [9, II, Hilfssatz 3.11] it is clear that $G/C_G(Z) \lesssim \mathrm{Aut}(GF(p^{n/s}) : GF(p))$, so in particular $|G/C_G(Z)| \le n/s = \dim X$. Write $k = \dim X$. Then $|G/C_G(Z)| \cdot |T| \le 2k|U|$. Using this estimate and the proof of [17, Corollary 3.7] yields $|G| \le 2k|U|e^{13/2}/2 = k|U|e^{13/2}$. This is (a).

Now if W is an irreducible U-submodule of V, then $|U| \mid |W| - 1$ and clearly $k \le \dim W =: l$. Therefore obviously $|G| \le lp^l e^{13/2}$. On the other hand, by [17, Corollary 2.6] $V_U = teW$ for a $t \in \mathbb{N}$ and hence $|V| = p^{tle}$. Hence if $p > 3^{112}$ and $e \ge 9$, then $|G| \le lp^l e^{13/2} \le p^{le/8}/3 \le |V|^{1/8}/3$. This is (b).

Moreover, if $p > 5^{28}$, and $e \ge 5$, then

$$k(G) \le |G| \le lp^l e^{13/2} \le p^{le/4}/2 \le |V|^{1/4}/2 \tag{1}$$

Now let $(|G|, |V|) = 1$ and recall that by Corollary 3.7 (a)

$$k(GV) = \sum_{i=1}^{k(G)} n(C_G(g_i), C_V(g_i)),$$

where $g_1 = 1, g_2, \dots, g_{k(G)}$ are representatives of the conjugacy classes of G. Now as $|C_V(g)| \le |V|^{3/4}$ for $1 \ne g \in G$ (see part (a) of the proof of [17, Proposition 4.10]) and $n(C_G(g), C_V(g)) \le |C_V(g)|$ for $g \in G$, we have

$$k(GV) \le n(G, V) + (k(G) - 1)|V|^{3/4}.$$

Moreover, by the Cauchy-Frobenius formula we have

$$n(G, V) = \frac{1}{|G|}\sum_{g \in G}|C_V(g)| \le \frac{|V|}{|G|} + \frac{|G|-1}{|G|}|V|^{3/4} \le \frac{|V|}{2} + |V|^{3/4}.$$

Therefore,

$$k(GV) \le |V|/2 + k(G)|V|^{3/4}, \tag{2}$$

and together with (1) this clearly yields (c) for $e \ge 5$. It remains to prove (c) in case that $e \le 4$. If $e = 1$, then by [17, Corollary 2.3 (b)] $G \le \Gamma(V)$, in which case it is well-known (and easy to see using the formulas in Corollary 3.7) that

$k(GV) \leq |V|$. So we may assume that $2 \leq e \leq 4$. Suppose now that $p > 2^{112}$. By (a) $|G/U| \leq ke^{13/2} \leq l\,2^{13}$. Now if $|U| \leq p^{l/8}$, then

$$k(G) \leq |G| \leq l\,2^{13}p^{l/8} \leq p^{l/4}/2 \leq |W|^{1/4}/2 \leq |V|^{1/4}/2$$

(as $p \geq 2^{112}$) and thus with (2) we obtain the conclusion. We thus may assume that $|U| > p^{l/8}$. Now as UV is a Frobenius group, we easily see (with the formulas in Corollary 3.7) that $k(UV) = (|V|-1)/|U| + |U| \leq |V|/p^{l/8} + p^l$ and therefore

$$k(GV) \leq k(G/U)k(UV) \leq 2^{13}\,l\left(\frac{|V|}{p^{l/8}} + p^l\right) = \frac{2^{13}l}{p^{l/8}}|V| + 2^{13}lp^l.$$

Hence it suffices to show that $(2^{13}l)/p^{l/8}\,|V| + 2^{13}lp^l \leq |V|$ which is equivalent to

$$2^{13}lp^l \leq \left(1 - \frac{2^{13}l}{p^{l/8}}\right)|V| = \left(1 - \frac{2^{13}l}{p^{l/8}}\right)p^{tle}$$

For this, it suffices to show that

$$2^{13}lp^l \leq \left(1 - (2^{13}l)/p^{l/8}\right)p^{2l} \quad \text{or} \quad 2^{13}l \leq \left(1 - (2^{13}l)/p^{l/8}\right)p^l.$$

As $p \geq 2^{112}$, this is certainly true and so also the proof of (c) is complete. □

LEMMA 4.2. *Let G be a solvable group and $V \neq 0$ a faithful, irreducible and finite G-module. Suppose that $V = W^G$ for an irreducible H-module W for some $H \leq G$ (possibly $H = G$). Assume further that $|H/C_H(W)| \leq |W|^{1/8}/3$. Then $|G| \leq |V|^{1/8}/3$.*

PROOF. Since $V = W^G$, we may write $V = X_1 \oplus \cdots \oplus X_m$ for subspaces X_i of V that are transitively permuted by G with $W = X_1$. Let N be the kernel of this permutation action. Then G/N is a solvable subgroup of S_m, and by [1, Theorem 3] we know that $|G/N| \leq 24^{(m-1)/3} \leq 3^{m-1}$. Moreover, $N/C_N(V_i) \lesssim N_G(X_i)/C_G(X_i) \cong H/C_H(W)$ for $i = 1, \ldots, m$, and thus $|N/C_N(V_i)| \leq (1/3)|V_i|^{1/8}$ for all i. As $\bigcap_{i=1}^m C_N(V_i) = 1$, we have $N \lesssim \bigtimes_{i=1}^m N/C_N(V_i)$ and therefore we see that

$$|N| \leq \prod_{i=1}^{m}\left(\frac{|V_i|^{1/8}}{3}\right) = |V|^{1/8}/3^m.$$

Hence altogether we have $|G| = |G/N|\,|N| \leq 3^{m-1}(|V|^{1/8}/3^m) = |V|^{1/8}/3$, as wanted. □

LEMMA 4.3. *Let G be a solvable group and V be a G-module over an arbitrary field. Suppose that there are $N \trianglelefteq G$ and N-submodules V_i $(i = 1, \ldots, m)$ for $m \in \mathbb{N}$ such that $V = \bigoplus_{i=1}^m V_i$ and G/N permutes V_i primitively and faithfully. Then for any $g \in G - N$ we have $|C_V(g)| \leq |V|^{3/4}$.*

PROOF. Let $g \in G - N$. Obviously we may assume that g is of prime order. Then g permutes the V_i $(i = 1, \dots, m)$ nontrivially. If $n(g)$ is the number of orbits of $\langle g \rangle$ on $\Omega := \{V_1, \dots, V_m\}$ (that is, $n(g)$ is the number of cycles of g on Ω), then it is clear that $|C_V(g)| \leq |V_1|^{n(g)}$, because if $i \in \{1, \dots, m\}$ and $\mathscr{C} = \{V_i^{g^j} \mid j \in \mathbb{Z}\}$ is the orbit containing V_i and $X_i = \sum_{j \in \mathbb{Z}} V_i^{g^j}$, then $|C_{X_i}(g)| \leq |V_i| = |V_1|$. Now by [17, Lemma 5.1] we know that $n(g) \leq 3m/4$, and thus $|C_V(g)| \leq |V_1|^{n(g)} \leq |V_1|^{3m/4} = |V|^{3/4}$, as claimed. □

LEMMA 4.4. *Let G be a solvable group acting faithfully on a finite G-module V over $GF(q)$ (q a prime) such that $V = V_1 \oplus \cdots \oplus V_n$ for an $n \in \mathbb{N}$ with $n \geq 2$ and G-invariant subspaces V_i $(i = 1, \dots, n)$ of V. Let GV be the semidirect product with respect to this action and suppose that there are automorphisms Θ_i of GV such that $V_1^{\Theta_i} = V_i$ $(i = 1, \dots, n)$; so in particular the semidirect products $(G/C_G(V_i))V_i$ $(i = 1, \dots, n)$ are all isomorphic. Assume that $Z(F(G))C_G(V_1)/C_G(V_1)$ (which clearly is nontrivial) is cyclic and acts fixed point freely on V_1. Suppose further that $\overline{G_1} := G/C_G(V_1)$ contains a normal cyclic subgroup $\overline{Z_1} = Z_1/C_G(V_1)$ where $Z_1 \leq G$ such that $Z(F(G))C_G(V_1) \leq Z_1$ (thus, in particular, $\overline{Z_1}$ acts fixed point freely on V_1).*

Put $\overline{G}_i = G/C_G(V_i)$ and let $\overline{Z_i} = \overline{Z_1}^{\Theta_i}$ be the corresponding subgroup in $\overline{G_i}$. As G acts faithfully on V, clearly $\bigcap_{i=1}^n C_G(V_i) = 1$ and so there is a $U \leq \times_{i=1}^n \overline{G_i}$ and an isomorphism $\phi : G \to U$ (namely, $\phi(g) = (gC_G(V_1), \dots, gC_G(V_n))$ for $g \in G$). Now let $Z := \phi^{-1}(U \cap \times_{i=1}^n \overline{Z_i})$ and put $s = d(Z)$. Then the following hold:

(a) *$Z = \bigcap_{i=1}^n Z_i$ and $1 < Z/C_Z(V_i) \lesssim \overline{Z_i}$ for $i = 1, \dots, n$ and Z is an abelian normal subgroup of G which acts nontrivially on each V_i $(i = 1, \dots, n)$.*

(b) *There exist an $s_0 \in \mathbb{N}$ with $s \leq s_0 \leq n$ and $N_i \trianglelefteq G$, $W_i \leq V$ $(i = 0, \dots, s_0)$ such that each W_i is the sum of some of the V_j and if we put $N_0 = 1$, $W_0 = 0$, then $N_0 < N_1 < \cdots < N_{s_0} = G$, $W_i \cap W_j = 0$ for all $i \neq j$, $d(Z \cap N_i) \leq i$ for all i, N_i acts trivially on $V/\left(\bigoplus_{j=0}^i W_j\right)$ for all $i = 0, \dots, s_0$, G/N_i acts faithfully on $V/\left(\bigoplus_{j=0}^i W_j\right)$ and N_{i+1}/N_i acts faithfully each V_j with $V_j \leq W_{i+1}$ $(i = 0, \dots, s_0 - 1)$, and $(Z \cap N_{i+1})N_i/N_i$ (possibly $= 1$) acts fixed point freely on W_{i+1}. In particular, $V = \bigoplus_{i=1}^{s_0} W_i$ and $k(GV) \leq \prod_{i=0}^{s_0-1} k((N_{i+1}/N_i)W_{i+1})$.*

(c) *Suppose that $|\overline{G_1}/\overline{Z_1}| \leq kd$ for $d = \dim V_1$ and some $k \geq 1$, and also suppose that $|Z| \geq |V|^\epsilon / l^n$ for some $l \geq 1$ and some $0 < \epsilon < 1/2$ and that $V_1|_{\overline{Z_1}}$ in the direct sum of at least two irreducible $\overline{Z_1}$-modules. Suppose that $q > (2^{\epsilon+1} l^\epsilon k)^{2/\epsilon^2}$. Then $k(GV) \leq |V|/2^n$.*

PROOF. (a) It is obvious from the definition of Z that $Z \trianglelefteq G$ and Z is abelian. Let $H = \bigcap_{i=1}^n Z_i$ and $C_i = C_G(V_i)$ for all i. Now if $g \in H$, then clearly $gC_i \in \overline{Z_i}$ for all i and thus $\phi(g) \in \times_{i=1}^n \overline{Z_i}$ which shows that $g \in Z$. Thus $H \leq Z$. On the other hand, if $g \in Z$, then $gC_i \in \overline{Z_i}$ for all i and thus $g \in Z_i$ for all i, that is, $g \in H$ and so $Z \leq H$. So indeed $H = Z$. Moreover clearly $Z/C_Z(V_i) \cong ZC_i/C_i \leq Z_i/C_i = \overline{Z_i}$ for all i.

https://doi.org/10.1017/S1446788700003724 Published online by Cambridge University Press

Now clearly $Z(F(G)) \leq Z$ and $Z(F(G))$ acts nontrivially on every V_i $(i = 1, \ldots, n)$, so $1 < Z/C_Z(V_i)$ for all i. So (a) is proved.

(b) We prove the assertion by induction on i. For $i = 0$ there is nothing to show. So let $i \geq 0$ and $Z > 1$ and suppose that we already have W_j $(j \leq i)$ and N_i. Then let $V = \left(\bigoplus_{j=1}^{i} W_j\right) \bigoplus X_i$ for a G-invariant X_i which is the sum of some of V_j. Clearly $X_i \cong V/\bigoplus_{j=1}^{i} W_j$ as G-module, and so (by induction) we know that G/N_i acts faithfully on X_i and N_i centralizes X_i. Moreover by induction we have $d(Z \cap N_i) \leq i$.

If $Z \leq N_i$ then as Z acts nontrivially on each V_i and N_i acts trivially on $V/\bigoplus_{j=1}^{i} W_j$, this implies that $V = \bigoplus_{j=1}^{i} W_j$, and if we put $s_0 = i$, then $s_0 = i \geq d(Z \cap N_i) = d(Z) = s$ and we are obviously done. In particular, if we put $L_i = \bigoplus_{j=1}^{i} W_j$ for $i = 0, \ldots, s_0$, then in GV we have the normal series

$$1 = N_0 L_0 \trianglelefteq N_1 L_1 \trianglelefteq \cdots \trianglelefteq N_{s_0} L_{s_0} = GV$$

with $N_{j+1}L_{j+1}/N_j L_j \cong (N_{j+1}/N_j)W_{j+1}$ for all j. Therefore clearly

$$k(GV) \leq \prod_{j=0}^{s_0-1} k(N_{j+1}L_{j+1}/N_j L_j) = \prod_{j=0}^{s_0-1} k((N_{j+1}/N_j)W_{j+1}).$$

So next we have to consider the case that $Z/Z \cap N_i > 1$. Observe that any element $g \in Z$ acts either fixed point freely or trivially on V_j (for any fixed $j \in \{1, \ldots, n\}$). Now let $t \in \mathbb{Z}$ be minimal such that there is a $g \in G$ acting nontrivially on t of the V_j with $V_j \leq X_i$ and trivially on all the other V_j with $V_j \leq X_i$. Clearly $t \geq 1$, and by renumbering the V_i we may assume that $W_i = \bigoplus_{j=1}^{k_1} V_j$ for some $k_1 \in \mathbb{N} \cup \{0\}$ and that there is a $g \in G$ acting nontrivially on $W_{i+1} := \bigoplus_{j=1}^{t} V_{k_1+j}$ and trivially on $Y_{i+1} := \bigoplus_{j=k_1+t+1}^{n} V_j \cong V/W_{i+1}$ (as G-modules). Put $N_{i+1} = C_G(Y_{i+1})$. Clearly $N_i \leq N_{i+1} \trianglelefteq G$, $W_{i+1} \cap W_j = 0$ for $j = 1, \ldots, i$. By our construction $(Z \cap N_{i+1})/(Z \cap N_i) \cong (Z \cap N_{i+1})N_i/N_i$ (which might be trivial) acts fixed point freely on W_{i+1} and thus is cyclic; so as (by induction) $d(Z \cap N_i) \leq i$ and $d((Z \cap N_{i+1})/(Z \cap N_i)) \leq 1$, it follows that $d(Z \cap N_{i+1}) \leq i + 1$. Moreover, as G/N_i acts faithfully on X_i and N_{i+1} acts trivially on Y_{i+1}, N_{i+1}/N_i must act faithfully on W_{i+1} and by our minimal choices of t obviously N_i/N_{i+1} even acts faithfully on each V_j with $V_j \leq W_{i+1}$. So N_{i+1}, W_{i+1} have all the properties asserted in (b), and (b) is proved.

(c) As $|V|^{\epsilon}/l^n \leq |Z| \leq |\overline{Z_1}|^n$, we have $|\overline{Z_1}| \geq |V|^{\epsilon}/l$, and as $\overline{Z_1}$ acts fixed point freely on V_1 and $V_1|_{\overline{Z_1}}$ is the sum of at least two irreducible $\overline{Z_1}$-modules, clearly $|\overline{Z_1}| \leq |V_1|^{1/2}$. So altogether $|V_1|^{\epsilon}/l \leq |\overline{Z_1}| \leq |V_1|^{1/2}$. Now if we put

$$Z^*_{i+1} = (Z \cap N_{i+1})/(Z \cap N_i) \cong (Z \cap N_{i+1})N_i/N_i$$

for $i = 0, \ldots, s_0 - 1$, then $|Z| = \prod_{i=0}^{s_0-1} |Z^*_{i+1}|$. Put

$$a = \left|\left\{i \mid i \in \{0, \ldots, s_0 - 1\},\ |Z^*_{i+1}| \geq |V_1|^{\epsilon/2}/l\right\}\right|$$

https://doi.org/10.1017/S1446788700003724 Published online by Cambridge University Press

We claim that $a \geq n\epsilon$ (*).

To see this, assume $a < n\epsilon$. As $|Z_i^*| \leq |\overline{Z_i}| \leq |V_1|^{1/2}$, it follows that

$$\frac{|V|^\epsilon}{l^n} \leq |Z| = \prod_{i=0}^{s_0-1} |Z_{i+1}^*| \leq |V_1|^{a/2}\left(\frac{|V_1|^{\epsilon/2}}{l}\right)^{n-a}$$
$$\leq |V_1|^{n\epsilon/2}\left(\frac{|V_1|^{\epsilon/2}}{l}\right)^{(1-\epsilon)n} \leq |V|^{\epsilon/2}\frac{|V|^{\epsilon/2-\epsilon^2/2}}{l^{(1-\epsilon)n}} = \frac{|V|^{\epsilon-\epsilon^2/2}}{l^{(1-\epsilon)n}}.$$

This implies $|V|^{\epsilon^2/2} \leq l^n/l^{(1-\epsilon)n}$ and so $|V|^{\epsilon/2} \leq l^n$. Now $|V| = |V_1|^n \geq q^n$, and with our hypothesis on q we obtain $(2^{\epsilon+1}l^\epsilon k)^{n/\epsilon} \leq l^n$ which implies $2^n\, l^n\, k^{n/\epsilon} \leq l^n$ or $2\, k^{1/\epsilon} \leq 1$, a contradiction. This establishes the claim (*).

Now let $\{0, 1, \ldots, s_0 - 1\} = M_1 \cup M_2$, where $M_1 = \{i \mid |Z_{i+1}^*| \geq |V_1|^{\epsilon/2}/l\}$ and $M_2 = \{0, 1, \ldots, s_0 - 1\} - M_1$.

Let $i \in M_1$ and choose m such that $V_m \leq W_{i+1}$, and write $Y = (Z_m \cap N_{i+1})N_i/N_i$. As by (b) N_{i+1}/N_i acts faithfully on each $V_j \leq W_{i+1}$, we see that Y is cyclic and acts fixed point freely on V_m. Moreover $Y \geq (Z \cap N_{i+1})N_i/N_i$ which is cyclic and acts fixed point freely on W_{i+1}; also observe that $(Z \cap N_{i+1})N_i/N_i > 1$ because with our hypothesis on q we conclude that

$$|(Z \cap N_{i+1})N_i/N_i| = |Z_{i+1}^*| \geq |V_1|^{\epsilon/2}/l \geq q^{\epsilon/2}/l > 1.$$

This forces Y to act fixed point freely on W_{i+1}. Now we have

$$k\left((N_{i+1}/N_i)\, W_{i+1}\right) \leq k\left((N_{i+1}/N_i)/Y\right) k(Y W_{i+1})$$
$$= k\left(N_{i+1}/(Z_m \cap N_{i+1})N_i\right) k(Y W_{i+1}).$$

Now as N_{i+1}/N_i acts faithfully on V_m, we see that $|N_{i+1}/(Z_m \cap N_{i+1})N_i| \mid |\overline{G_m}/\overline{Z_m}|$ and thus by hypothesis $|N_{i+1}/(Z_m \cap N_{i+1})N_i| \leq kd$. Moreover, as Y acts fixed point freely on W_{i+1}, we clearly have (for example by the formulas in Corollary 3.7)

$$k(Y W_{i+1}) = \frac{|W_{i+1}| - 1}{|Y|} + |Y|.$$

Since $i \in M_1$, we have $|Y| \geq |Z_{i+1}^*| \geq |V_1|^{\epsilon/2}/l$ and also $|Y| \leq |\overline{Z_m}| = |\overline{Z_1}| \leq |V_1|^{1/2}$. Therefore

$$k(Y W_{i+1}) \leq \frac{|W_{i+1}| - 1}{|V_1|^{\epsilon/2}/l} + |V_1|^{1/2} \leq l\frac{|W_{i+1}|}{|V_1|^{\epsilon/2}} + |V_1|^{1/2} \leq 2l\frac{|W_{i+1}|}{|V_1|^{\epsilon/2}}$$

(where the last inequality holds true because $|W_{i+1}| \geq |V_1| \geq |V_1|^{1/2}\,|V_1|^{\epsilon/2}$ and $l \geq 1$). Now if $i \in M_2$, then we simply use the trivial estimate that

$$k\big((N_{i+1}/N_i)\, W_{i+1}\big) \leq kd\,|W_{i+1}|.$$

Thus altogether we get

$$k((N_{i+1}/N_i)\,W_{i+1}) \le \begin{cases} kd\,2l\,|W_{i+1}|/|V_1|^{\epsilon/2} & \text{if } i \in M_1;\\ kd|W_{i+1}| & \text{if } i \in M_2.\end{cases}$$

Thus with (b) we conclude that

$$\begin{aligned} k(GV) &\le \prod_{i\in M_1}\left(kd\,2l\frac{|W_{i+1}|}{|V_1|^{\epsilon/2}}\right)\prod_{i\in M_2}(kd|W_{i+1}|)\\ &= \prod_{i=0}^{s_0-1}(kd|W_{i+1}|)\prod_{i\in M_1}\frac{2l}{|V_1|^{\epsilon/2}}\\ &= k^{s_0}d^{s_0}|V|\left(\frac{(2l)}{|V_1|^{\epsilon/2}}\right)^a \le k^n d^n|V|\left(\frac{2l}{|V_1|^{\epsilon/2}}\right)^a. \end{aligned}$$

Now note that by our hypothesis $(2l)/|V_1|^{\epsilon/2} \le (2l)/q^{\epsilon/2} \le 1$, so that with $(*)$ we find that

$$k(GV) \le |V|k^n d^n\left(\frac{2l}{|V_1|^{\epsilon/2}}\right)^{n\epsilon} = \left(\frac{(2l)^\epsilon kd}{|V_1|^{\epsilon^2/2}}\right)^n|V|.$$

Now $|V_1| = q^d$, and as by our hypothesis clearly $q^{\epsilon^2/2} \ge 2$, we see that

$$\frac{d}{|V_1|^{\epsilon^2/2}} = \frac{d}{\left(q^{\epsilon^2/2}\right)^d} \le \frac{1}{q^{\epsilon^2/2}}$$

and thus $k(GV) \le \left((2l)^\epsilon k/q^{\epsilon^2/2}\right)^n|V|$ and as $((2l)^\epsilon k)/q^{\epsilon^2/2} \le 1/2$ by our hypothesis, we obtain $k(GV) \le |V|/2^n$, and the proof of the lemma is complete. □

LEMMA 4.5. *Let $n \in \mathbb{N}$ and $A, B \in \mathbb{R}$ with $A \ge 1$ and $1 \le B \le A^n$. Let*

$$U = \left\{(x_1,\dots,x_n) \in \mathbb{R}^n \;\middle|\; 1 \le x_i \le A \text{ for all } i \text{ and } \prod_{i=1}^n x_i = B\right\} \subseteq \mathbb{R}^n,$$

and consider the function $f : \mathbb{R}^n \to \mathbb{R}$ defined by $f(x_1,\dots,x_n) = \prod_{i=1}^n (A/x_i + 1)$. Let $s \in \mathbb{N}\cup\{0\}$ be maximal subject to $A^s \le B$. Write $x = (x_1,\dots,x_n)$ for elements in $\mathbb{R}^n$. Then $\max_{x\in U} f(x) = 2^s(A+1)^{n-s-1}\left(A^{s+1}/B + 1\right)$.

PROOF. Let $(x_1,\dots,x_n) \in U$, and choose a pair of indices, i and j. If $x_ix_j > A$, then put $y_i = (x_jx_j)/A$ and $y_j = A$. If $x_ix_j \le A$, then put $y_i = 1$ and $y_j = x_ix_j$. Also let $y_k = x_k$ for $k \notin \{i,j\}$. Then clearly $(y_1,\dots,y_n) \in U$, and it is easy to check that $f(y_1,\dots,y_n) - f(x_1,\dots,x_n) \ge 0$.

Repeatedly applying this procedure shows that $f(x_1, \dots, x_n) \le f(z_1, \dots, z_n)$ for a $(z_1, \dots, z_n) \in U$ such that there is at most one index i with $z_i \notin \{1, A\}$. But then necessarily s of the z_j have to equal A and $n - s - 1$ of them have to be 1. Thus $f(z_1, \dots, z_n) = 2^s(A+1)^{n-s-1}(A^{s+1}/B + 1)$, and the lemma is proved. □

We remark that with the method of the Lagrange multipliers it can easily be shown that the function f in Lemma 4.5 has an absolute minimum at $x_1 = \cdots = x_n = \sqrt[n]{B}$.

COROLLARY 4.6. *Let $n \in \mathbb{N}$, let q be a prime power, and suppose that V_i, $i = 1, \dots, n$, are G_i-modules, where $|V_i| = q$, G_i is a cyclic group of order $q - 1$ and G_i acts fixed point freely on V_i for all i. Let $G = G_1 \times \cdots \times G_n$ act on $V = V_1 \oplus \cdots \oplus V_n$ such that G_i acts trivially on V_j whenever $i \neq j$ (so that with the notation of* [17, Chapter 2] *we have $GV \cong A\Gamma_0(q)^n$). Let $M \le G$. Then*

$$n(M, V) \le 2^s q^{n-s} = (2/q)^s\,|V|$$

where $s \in \mathbb{N} \cup \{0\}$ is chosen maximal subject to $(q-1)^s \le |M|$.

PROOF. For $i = 1, \dots, n$ define

$$x_i = \left| C_M\left(\bigoplus_{j=1}^{i-1} V_j\right) \Big/ C_M\left(\bigoplus_{j=1}^{i} V_j\right)\right|$$

and observe that $1 \le x_i \le q - 1$ for all i and $\prod_{i=1}^n x_i = |M|$. Next we claim that

$$(**) \qquad n(M, V) \le \prod_{j=1}^{n}\left(\frac{q-1}{x_i} + 1\right).$$

We prove this by induction on n. If $n = 1$, then $M \le G_1$ and $|M_1| = x_1$, and as G_1 acts fixed points freely on V, the assertion follows.

Let $n \ge 2$ and write $W = V_2 \oplus \cdots \oplus V_n$. Now we have (by Cauchy-Frobenius)

$$\begin{aligned}
n(M, V) &= \frac{1}{|M|}\sum_{v \in V} |C_M(v)| \\
&= \frac{1}{|M|}\sum_{v_1 \in V_1}\sum_{w \in W} |C_M(v_1) \cap C_M(w)| \\
&= \sum_{v_1 \in V_1} \frac{1}{|M/C_M(v_1)|}\frac{1}{|C_M(v_1)|}\sum_{w \in W} |C_{C_M(v_1)}(w)| \\
&= \sum_{v_1 \in V_1} \frac{1}{|M/C_M(v_1)|} n(C_M(v_1), W) \\
&= n(M, W) + \sum_{v_1 \in V_1 - \{0\}} \frac{1}{x_1} n(C_M(V_1), W),
\end{aligned}$$

where the last equality holds as for $0 \neq v_1 \in V_1$, we clearly have $C_M(v_1) = C_M(V_1)$. So we further conclude that

$$n(M, V) = n(M, W) + \frac{q-1}{x_1} n(C_M(V_1), W) \leq \left(\frac{q-1}{x_1} + 1\right) n(C_M(V_1), W).$$

Now $C_M(V_1) \leq G_2 \times \cdots \times G_n$, $C_M(V_1)$ acts faithfully on $V_2 \oplus \cdots \oplus V_n$, and

$$x_i = \left| C_{C_M(V_1)}\left(\bigoplus_{j=2}^{i-1} V_j\right) \Big/ C_{C_M(V_1)}\left(\bigoplus_{j=2}^{i} V_j\right)\right| \quad \text{for } j = 2, \ldots, n.$$

Thus we may apply induction which yields $n(C_M(V_1), W) \leq \prod_{j=2}^{n}\left((q-1)/x_j + 1\right)$. So altogether $(**)$ follows.

Now $(**)$ and Lemma 4.5 (with $A = q-1$, $B = |M|$) imply that

$$n(M, V) \leq 2^s q^{n-s-1}\left(\frac{(q-1)^{s+1}}{|M|} + 1\right),$$

and since by definition of s clearly $(q-1)^{s+1}/|M| \leq q-1$, the assertion of the corollary now follows. $\square$

LEMMA 4.7. *Let G be a group and V be a finite faithful G-module. Suppose that $N \trianglelefteq G$ such that G/N is cyclic, and suppose that $V = V_1 \oplus \cdots \oplus V_n$ for some $n \in \mathbb{N}$ and N-modules V_i $(i = 1, \ldots, n)$ such that the following hold:*

(i) *$N/C_N(V_i) \lesssim \Gamma(V_i) = \Gamma(q)$ for all i and a prime power q, and the semidirect products $(N/C_N(V_i))V_i$ $(i = 1, \ldots, n)$ are mutually isomorphic.*

(ii) *G/N permutes the V_i $(i = 1, \ldots, n)$, and if $l \in \mathbb{N}$ is the number of fixed points of G/N on $\{V_1, \ldots, V_n\}$, then $l \leq n/2$.*

Then the following hold:

(a) *$N \lesssim \Gamma(V_1) \times \cdots \times \Gamma(V_n) \cong (\Gamma(V_1))^n$. We identify N with its isomorphic subgroup in $\Gamma(V_1)^n$ and write $T = (\Gamma_0(V_1))^n$ and $M = N \cap T$. Then M is an abelian normal subgroup of G, and each nonidentity element of M acts fixed point freely on at least one of the V_i.*

(b) *Let $g \in G - N$ such that $G/N = \langle gN \rangle$, and put $\Omega = \{V_1, \ldots, V_n\}$ and $m = n(\langle g \rangle, \Omega) - l$. Then g has on Ω exactly l orbits of length 1 and m orbits of length ≥ 2. Suppose that $\{V_i\}$, $i = 1, \ldots, l$ are the orbits of length 1 and let $\mathcal{O}_i$ $(i = 1, \ldots, m)$ be the orbits of length ≥ 2. Define*

$$R_i = \{(h_1, \ldots, h_m) \mid h_i \in \Gamma_0(V_1),\ h_j = 1 \text{ for } j \neq i\} \leq T$$

for $i = 1, \ldots, l$, and

$$R_i^* = \bigtimes_{j \text{ with } V_j \in \mathcal{O}_i} \Gamma_0(V_j) \leq T$$

as well as $W_i = \bigoplus_{j \text{ with } V_j \in \mathcal{O}_i} V_j \leq V$ *for* $j = 1, \dots, m$. *Moreover put* $S_i = C_{R_i}(g)$ $(i = 1, \dots, l)$ *and* $S_i^* = C_{R_i^*}(g)$ $(i = 1, \dots, m)$. *Then* $C_M(g) \leq C_T(g) = S_1 \times \cdots \times S_l \times S_1^* \times \cdots \times S_m^* =: T_1$, *and all the* S_i, S_j^* *are cyclic (possibly trivial)*; S_i *acts fixed point freely on* V_i *for* $i = 1, \dots, l$ *and* S_i^* *acts fixed point freely on* W_i *for* $i = 1, \dots, m$. *In particular,* $d(C_M(g)) \leq l + m \leq l + (n-l)/2 = (n+l)/2$.

(c) *Let* $\Omega_1 = \mathrm{cl}(MV)$ *and let* g *be as in* (b). *Then* $C_{\Omega_1}(g) = \{h[\langle h\rangle, V]X \mid h \in C_M(g),\ X \text{ is an orbit of } M \text{ on } C_V(h) \text{ with } X^g = X\}$. *Moreover,* $|C_{\Omega_1}(g)| \leq 4^n q^{(7/8)n}$.

PROOF. (a) As G acts faithfully on V and thus $\bigcap_{i=1}^n C_G(V_i) = 1$, we have $N \lesssim \times_{i=1}^n N/C_N(V_i) \cong \times_{i=1}^n \Gamma(V_i) \cong \Gamma(V_1)^n$. The rest of (a) is easy to see.

(b) Obviously $g \in N_G(R_i)$ for $i = 1, \dots, l$, and also $g \in N_G(R_i^*)$ for $i = 1, \dots, m$ and moreover by reordering the V_i we may assume that $M = R_1 \times \cdots \times R_l \times R_1^* \times \cdots \times R_m^*$. Hence $C_M(g) \leq C_T(g) = S_1 \times \cdots \times S_l \times S_1^* \times \cdots \times S_m^*$, and clearly the S_i are cyclic and act fixed point freely on V_i $(i = 1 \dots l)$.

It remains to show that the S_i^* are cyclic and act fixed point freely on W_i $(i = 1, \dots, m)$. For this fix $i \in \{1, \dots, m\}$. Without loss of generality we may assume that $i = 1$ and $W_1 = V_{l+1} \oplus \cdots \oplus V_{l+l'}$ for some $l' \in \mathbb{N}$ with $V_{l+j} = GF(q)$ for $j = 1, \dots, l'$. Clearly we may assume that

$$V_{l+j}^g = \begin{cases} V_{l+j+1} & \text{if } 1 \leq j \leq l'-1; \\ V_{l+1} & \text{if } j = l'. \end{cases}$$

Thus $R_1^* = \Gamma_0(V_{l+1}) \times \cdots \times \Gamma_0(V_{l+1})$, and these direct factors are permuted by g correspondingly. Now there exist functions $f_j : GF(q) \to GF(q)$ $(j = 1, \dots, l')$ such that for all $x_j \in \Gamma(V_{l+j})$, $j = 1, \dots, l'$, we have

$$(x_1, \dots, x_{l'})^g = (f_{l'}(x_{l'}), f_1(x_1), \dots, f_{l'-1}(x_{l'-1})),$$

and obviously $f_i(x) = 1$ if and only if $x = 1$ for all i. This shows that if there is an $1 \neq x = (x_1, \dots, x_{l'}) \in C_T(g)$, then we see that $x_i \neq 1$ for all i, and thus x acts fixed point freely on W_i. Consequently S_i^* acts fixed point freely on W_i and thus is cyclic. This proves (b).

(c) Similarly as in the proof of Corollary 3.7 (a) and using the fact that M is abelian we see that for $h \in M$, $v \in V$ we have

$$\begin{aligned}(hv)^{MV} &= \{h^w v^x \mid x \in M,\ w \in V\} = \{h[h, w]v^x \mid x \in M,\ w \in V\} \\ &= \bigcup_{x \in M} h[\langle h\rangle, V]v^x = h \bigcup_{x \in M} ([\langle h\rangle, V]v)^x,\end{aligned}$$

where $[\langle h\rangle, V]v \in V/[\langle h\rangle, V] \cong C_V(h)$ (as M-modules). Thus $(hv)^{MV} = (hv_0)^{MV}$ for some $v_0 \in C_V(h)$ and

$$(hv)^{MV} = h \bigcup_{x \in M} [\langle h\rangle, V]v_0^x.$$

Hence if for any M-module W we write $N(M, W) = \{x^M \mid x \in W\}$ for the orbits of M on W, then we conclude that

$$\Omega_1 = \{h[\langle h \rangle, V]X \mid h \in M,\ X \in N(M, C_V(h))\}.$$

So if $\omega = h[\langle h \rangle, V]X \in \Omega_1$ for some $h \in M$, $X \in N(M, C_V(h))$, then $\omega^g = \omega$ if and only if $h^g = h$ and $X^g = X$. Hence

$$(3) \qquad C_{\Omega_1}(g) = \{h[\langle h \rangle, V]X \mid h \in C_M(g),\ X \in C_{N(M, C_V(h))}(g)\}.$$

Now for $h \in M$ define $V(h) := \{V_i \mid h$ acts fixed point freely on $V_i\}$. Clearly if $h \in C_M(g)$, then $V(h)$ is a union of some the the V_i, $i = 1, \dots, l$, and some of the $\mathcal{O}_j$, $j = 1, \dots, m$. For any subset $B \subseteq \{V_1, \dots, V_n\}$ we define $M_B \subseteq M$ by $M_B = \{h \in C_M(g) \mid V(h) = B\}$. So $M_B \neq \emptyset$ is only possible if B is a union of some of the V_i ($i = 1, \dots, l$) and some of the $\mathcal{O}_j$ ($j = 1, \dots, m$). More precisely, if

$$f(B) = |\{j \in \{1, \dots, m\} \mid \mathcal{O}_j \subseteq B\}|$$

and

$$g(B) = |\{i \in \{1, \dots, n\} \mid V_i \in \mathcal{O}_j \text{ for some } j \text{ with } \mathcal{O}_j \subseteq B\}|,$$

then by (b) it is clear that

$$(4) \qquad |M_B| \leq (q-2)^{|B| - g(B) + f(B)}$$

and as $|\mathcal{O}_j| \geq 2$ for $j = 1, \dots, m$, we have $g(B) \geq 2f(B)$, so in particular

$$(5) \qquad |M_B| \leq (q-2)^{|B| - f(B)}.$$

For the moment, fix B and $h \in M_B$. Then $|C_V(h)| = q^{n-|B|}$. Let $r \in \mathbb{R}$ such that $(q-1)^r = |C_M(C_V(h))|$ and $s \in \mathbb{R}$ such that $(q-1)^s = |M|$. Then $|M/C_M(C_V(h))| = (q-1)^{s-r}$. Hence by Corollary 4.6 we see that in this case

$$(6) \qquad \begin{aligned} n(M, C_V(h)) &= n(M/C_M(C_V(h)), C_V(h)) \\ &\leq \left(\frac{2}{q}\right)^{\lfloor s-r \rfloor} q^{n-|B|} \leq 2^n q^{r-s+1} q^{n-|B|} = 2^n q^{n+r-s+1-|B|}. \end{aligned}$$

Now consider the action of g on $C_V(h)$. There are exactly $m - f(B)$ indices j such that $W_j \leq C_V(h)$. For any such j and any $x \in M$ it is immediate that $|C_{W_j}(gx)| \leq q$. Also there are exactly $n - l - g(B)$ indices $i \in \{1, \dots, n\}$ such that $V_i \leq W_j \leq C_V(h)$ for some $j \in \{1, \dots, m\}$. Altogether we see that

$$|C_{C_V(h)}(gx)| \leq q^{n-|B|-(n-l-g(B))+m-f(B)} = q^{m+l+g(B)-|B|-f(B)}.$$

Moreover, if $v \in C_V(h)$, then $(v^M)^g = v^M$ if and only if there is an $x \in M$ such that $v^g = v^{x^{-1}}$, that is, $v \in C_{C_V(h)}(gx)$. This shows that

$$|C_{N(M,C_V(h))}(g)| \leq \left|\bigcup_{x \in M} C_{C_V(h)}(gx)\right|.$$

As clearly $C_{C_V(h)}(gxy) = C_{C_V(h)}(gx)$ for all $x \in M$ and $y \in C_M(C_V(h))$, we conclude that if x_i $(i = 1, \ldots, |M/C_M(C_V(h))|)$ are representatives of the cosets of $C_M(C_V(h))$ in M, then $\bigcup_{x \in M} C_{C_V(h)}(gx) = \bigcup_{i=1}^{|M/C_M(C_V(h))|} C_{C_V(h)}(gx_i)$. Hence

$$(7) \qquad \begin{aligned} |C_{N(M,C_V(h))}(g)| &\leq |M/C_M(C_V(h))| q^{m+l+g(B)-|B|-f(B)} \\ &\leq q^{s-r+m+l+g(B)-|B|-f(B)} \end{aligned}$$

Next we claim that

$$(8) \qquad \alpha_{B,h} := |M_B|\,|C_{N(M,C_V(h))}(g)| \leq 2^n q^{7n/8}.$$

To see this we consider two cases:

Case 1: $s - r \leq n/8$: First observe that $m \leq (n-l)/2$ and so $l + m \leq (n+l)/2$. Then by (4) and (7) we have $\alpha_{B,h} \leq q^{s-r+m+l} \leq q^{n/8+(n+l)/2} = q^{5n/8+l/2}$ which together with our hypothesis that $l \leq n/2$ implies (8) in this case.

Case 2: $s - r > n/8$: Then $r - s < -n/8$, and with (5) and (6)

$$\begin{aligned} \alpha_{B,h} &\leq |M_B|\,|N(M, C_V(h))| = |M_B|\, n(M, C_V(h)) \\ &\leq 2^n q^{n+r-s+1-|B|} q^{|B|-f(B)} \leq 2^n q^{n+r-s} \leq 2^n q^{n-n/8} = 2^n q^{7n/8}, \end{aligned}$$

as wanted. So (8) is established.

By (3) and (8) we finally obtain

$$\begin{aligned} |C_{\Omega_1}(g)| &= \sum_{h \in C_M(g)} |C_{N(M,C_V(h))}(g)| = \sum_{B \subseteq \{V_1,\ldots,V_n\}} \sum_{h \in M_B} |C_{N(M,C_V(h))}(g)| \\ &= \sum_{B \subseteq \{V_1,\ldots,V_n\}} |M_B| \max_{h \in M_B} |C_{N(M,C_V(h))}(g)| = \sum_{B \subseteq \{V_1,\ldots,V_n\}} \max_{h \in M_B} \alpha_{B,h} \\ &\leq \sum_{B \subseteq \{V_1,\ldots,V_n\}} 2^n q^{7n/8} \leq 4^n q^{7n/8} \end{aligned}$$

which was to be shown. So the proof of the lemma is complete. □

Finally, we can prove the main theorem of this section. For this we will use the concept of an imprimitivity chain, which was introduced in [12, Definition 1.12]. We will use the notation introduced there.

https://doi.org/10.1017/S1446788700003724 Published online by Cambridge University Press

THEOREM 4.8. *Let G be a solvable group and let V be a finite faithful G-module over $GF(p)$ (where p is a prime). Suppose that $(|G|, p) = 1$ and that $p > 2^{4620} \cdot 3^{20}$. Then $k(GV) \leq |V|$.*

PROOF. Let G be a counterexample with $|G||V|$ minimal. Write $H = GV$ for the semidirect product of G and V with respect to the action of G on V. First we prove that V is irreducible. If not, then $V = V_1 \oplus V_2$ for G-modules V_1, V_2 (note that V is completely reducible by Maschke as $(|G|, |V|) = 1$). So if $C = C_G(V_1)$, then $CV_2 \trianglelefteq H$ and $H/CV_2 \cong (G/C)V_1$. By induction, $k((G/C)V_1) \leq |V_1|$ and $k(CV_2) \leq |V_2|$ and thus $k(H) \leq k(H/CV_2) \cdot k(CV_2) \leq |V_1||V_2| \leq |V|$ contradicting H being a counterexample to the theorem. Thus V is irreducible.

Next suppose that G acts quasiprimitively on V. As by our hypothesis $p > 2^{112}$, we are done by Lemma 4.1 (c). Thus we may assume that G does not act quasiprimitively on V.

Now let $G = H_0 > H_1 > \cdots > H_l$ with $V = V_0 > V_1 > \cdots > V_l$ be an imprimitivity chain of G with respect to 1 and V. As V is not quasiprimitive, $l \geq 1$. Obviously for all $i \in \{0, \ldots, l\}$ we have that V_i is an irreducible H_i-module with $V_i^G = V$.

In particular, $V_l^G = V$, and therefore we can write $V = \bigoplus_{i=1}^m X_i$ for $m = |G : H_l|$ and subspaces X_i $(i = 1, \ldots, m)$ that are transitively permuted by G and where $X_1 = V_l$. The kernel of this permutation action is $M := \bigcap_{g \in G} H_l^g = \mathrm{core}_G(H_l) \trianglelefteq G$, and we have $M/C_M(X_i) \lesssim H_l/C_{H_l}(V_l)$ for all i, and $\overline{H_l} := H_l/C_{H_l}(V_l)$ acts faithfully, irreducibly and quasiprimitively on V_l. In particular, every abelian normal subgroup of $\overline{H_l}$ is cyclic and we adopt the notation of [17, Corollary 1.10] and write $e^2 = |E/Z|$ in that corollary. Furthermore, by Dixon's bound [1] for the order of solvable permutation groups we know that $|G/M| \leq 3^{m-1}$.

Next observe that as $V_1^G = V$, we also can write $V = \bigoplus_{i=1}^n W_i$ for $n = |G : H_1|$ and subspaces W_i $(i = 1, \ldots, n)$ that are transitively permuted by G and where $W_1 = V_1$. If $N := \bigcap_{g \in G} H_1^g = \mathrm{core}_G(H_1) \trianglelefteq G$ is the kernel of this permutation action, then we even know from the construction of an imprimitivity chain that G/N permutes the W_i primitively and faithfully. Note that by Lemma 4.3 we have $|C_V(g)| \leq |V|^{3/4}$ for all $g \in G - N$.

We claim that

$$(\star) \qquad |G| > |V|^{1/8}/3.$$

To see this, assume that $|G| \leq |V|^{1/8}/3$. Observe that by induction and Corollary 3.7 we know that

$$|V| \geq k(NV) = \sum_{v \in V} \frac{|C_N(v)|\, k(C_N(v))}{|N|} = \alpha_P(N, V),$$

where P is the goodness property described in Example 3.4 (a). Hence we can apply Lemma 3.8 with $\Omega = V$, $b = |V|$, $\epsilon = 3/4$ which yields $k(GV) = \alpha_P(G, V) \leq |V|$ contradicting (G, V) being a counterexample. This establishes our claim.

Now we show that $e \leq 8$. For this assume that $e \geq 9$. As $p \geq 3^{112}$, Lemma 4.1 (b) yields that $|\overline{H_l}| \leq |V_l|^{1/8}/3$, but then Lemma 4.2 implies that $|G| \leq |V|^{1/8}/3$ contradicting $(\star)$. So indeed $e \leq 8$, and the rest of the proof splits into two parts:

Case 1: $2 \leq e \leq 8$. Here we first recall that $|G/M| \leq 3^{m-1}$, as seen above. Next we consider the action of M on V. Clearly the $M/C_M(X_i)$ $(i = 1, \dots, m)$ are mutually isomorphic. Furthermore, $M/C_M(X_1) \lesssim \overline{H_l}$. Now let $\overline{U} \leq \overline{H_l}$ be a normal cyclic subgroup of $\overline{H_l}$ corresponding to the U in [17, Corollary 1.10], so that $\overline{U}$ acts fixed point freely on $X_1 = V_l$. Let $\overline{U_1} = \overline{U} \cap M C_{H_l}(V_l)/C_{H_l}(V_l) \lesssim M/C_M(X_1)$ and observe that the action of M on V satisfies the hypotheses of Lemma 4.4 with the image $U_1/C_M(X_1)$ (for some $C_M(X_1) \leq U_1 \leq M$) of $\overline{U_1}$ in $M/C_M(X_1)$ playing the role of $\overline{Z_1}$ in Lemma 4.4. Also let $U_i/C_M(X_i)$ be the corresponding subgroups of $M/C_M(X_i)$ for all i, and let $Z_0 = \bigcap_{i=1}^m U_i$ so that Z_0 plays the role of Z in Lemma 4.4. Observe that by Lemma 4.1 (a) we have $|M/C_M(X_1)| \leq |\overline{H_l}| \leq d\,|\overline{U}|e^{13/2}$ where $d := \dim V_1$, and thus

$$
\begin{aligned}
(9) \qquad |M/U_1| &\leq |(M/C_M(X_1))/(U_1/C_M(X_1))| \leq |\overline{H_l}/\overline{U}| \\
&\leq e^{13/2}d \leq 8^{13/2}d \leq 2^{20}d.
\end{aligned}
$$

With $(\star)$ and (9) and the fact that $M/Z_0 \lesssim \times_{i=1}^m M/U_i$ we obtain

$$\frac{1}{3}|V|^{1/8} < |G| = |G/M|\,|M/Z_0|\,|Z_0| \leq 3^{m-1}|M/U_1|^m|Z_0| \leq 3^{m-1}2^{20m}d^m|Z_0|$$

which, using $|V| = |V_1|^m = p^{dm}$, leads to

$$|Z_0| > \frac{1}{3^m\,2^{20m}}\left(\frac{p^{d/8}}{d}\right)^m.$$

Now as by hypothesis $p > 2^{40}$, we have $p^{d/40} \geq d$ for all possible d, and thus $p^{d/8}/d = (p^{d/40}/d)p^{d/10} \geq p^{d/10}$. Thus we conclude that

$$(10) \qquad |Z_0| > \frac{p^{dm/10}}{3^m \cdot 2^{20m}} = \frac{|V|^{1/10}}{(3 \cdot 2^{20})^m}.$$

As $e \geq 2$, from the structure of $\overline{H_l}$ (described in [17, Corollary 1.10]) it is clear that $V_l = X_1$ is the direct sum of at least two irreducible $\overline{U}$-modules; in particular, X_1 is the direct sum of at least two irreducible $\overline{U_1}$-modules. This together with (9) and (10) allows us to apply Lemma 4.4 (c) with $\epsilon = 1/10$, $k = 2^{20}$, $l = 3 \cdot 2^{20}$; note that by our hypothesis

$$p > \left(2^{11/10} \cdot 3^{1/10} \cdot 4 \cdot 2^{20}\right)^{200} = 2^{220} \cdot 3^{20} \cdot 2^{400} \cdot 2^{4000} = 2^{4620} \cdot 3^{20}.$$

Thus Lemma 4.4 (c) yields $k(MV) \leq |V|/2^m$. As G/M is a solvable subgroup of S_m, by [15, Theorem 2.2] we have $k(G/M) \leq 3^{(m-1)/2}$. Hence altogether we find that

$$k(GV) \leq k(G/M)\,k(MV) \leq 3^{m/2} \cdot \frac{|V|}{2^m} \leq |V|$$

and we are done in this case.

Case 2: $e = 1$. In this case, by [17, Corollary 2.3 (b)] we have that $\overline{H_l} \leq \Gamma(V_l)$ and so $M/C_M(X_i) \lesssim \Gamma(X_i)$ for $i = 1\dots, m$. Now let $g \in G - N$ and put $G_g = \langle g, M\rangle \leq G$. By [17, Lemma 5.1] we know that g fixes at most $n/2$ of the W_i in its permutation action on $\{W_1, \dots, W_n\}$. Consequently, it fixes at most $m/2$ of the X_i in its permutation action on $\{X_1, \dots, X_m\}$. Altogether we see that G_g satisfies the hypothesis of Lemma 4.7, and by Lemma 4.7 (a) $M \lesssim \bigtimes_{i=1}^m \Gamma(X_i)$. Identify M with its isomorphic subgroup in $\bigtimes_{i=1}^m \Gamma(X_i)$ and put $M_0 = M \cap \bigtimes_{i=1}^m \Gamma_0(X_i) \trianglelefteq G$. Also put $\Omega_1 = \mathrm{cl}(M_0 V)$. Then by Lemma 4.7 (c) we know that $|C_{\Omega_1}(g)| \leq 4^m q^{7m/8}$, where we write $q := |V_l| = |X_1|$. Since $g \in G - N$ was arbitrary and as $4 < p^{1/16} \leq q^{1/16}$, we conclude that $|C_{\Omega_1}(g)| \leq q^{15m/16}$ for all $g \in G - N$.

Put $\Omega_0 = \mathrm{Irr}(M_0 V)$. Clearly G acts on Ω_1 as well as Ω_0 by conjugation, and clearly $M_0 \trianglelefteq G$ is contained in the kernel of those actions. By Brauer's permutation lemma (see for example [10, Theorem 18.5 (b)]) we obtain $|C_{\Omega_0}(g)| = |C_{\Omega_1}(g)|$ for $g \in G$; in particular,

$$|C_{\Omega_0}(g)| \leq q^{15m/16} = |V|^{15/16} \quad \text{for all } g \in G - N. \tag{11}$$

Now put $\overline{R} = R/M_0$ for any $M_0 \leq R \leq G$ and observe that $\overline{R} \cong RV/M_0V \leq GV/M_0V \cong \overline{G}$. Then $\overline{G}$ acts (not necessarily faithfully) on Ω_0, and we have $|\overline{G}| = |G/M|\,|M/M_0|$. As observed earlier, $|G/M| \leq 3^{m-1}$. Now

$$|M/M_0| \leq \left| \bigtimes_{i=1}^{m} \Gamma(X_i)/\Gamma_0(X_i) \right| \leq (\log_p q)^m \leq (\log_2 q)^m.$$

Furthermore, as $q \geq p > 2^{2^{10}}$, we see that $\left(q^{1/32}/\log_2 q\right)^m \geq 3^m \geq 3^{m-1}\sqrt{2}$. Thus altogether we obtain

$$|\overline{G}| \leq 3^{m-1}(\log_2 q)^m \leq q^{m/32}/\sqrt{2} = |V|^{1/32}/\sqrt{2}. \tag{12}$$

Next let P be Gallagher's goodness property and remember that by Example 3.4 (b) we have $k(RV) = \alpha_P(RV/(M_0V), \Omega_0)$ for any $M_0 \leq R \leq G$. In particular, $k(GV) = \alpha_P(GV/(M_0V), \Omega_0)$ and also by induction

$$\alpha_P(NV/(M_0V), \Omega_0) = k(NV) \leq |V|. \tag{13}$$

We now apply Lemma 3.8 to the action of $GV/(M_0V)$ on Ω_0 with $b = |V|$ and $\epsilon = 15/16$. Observe that (11)–(13) imply that $\alpha_P(NV/(M_0V), \Omega_0) \leq |V|$,

$|C_{\Omega_0}(gM_0V)| \leq |V|^{\epsilon}$ for all $gM_0V \in GV/(M_0V) - NV/(M_0V)$, and $|GV/(M_0V)| = |\overline{G}| \leq |V|^{(1-\epsilon)/2}/\sqrt{2}$. Hence Lemma 3.8 yields

$$k(GV) = \alpha_P(GV/(M_0V), \Omega_0) \leq |V|,$$

and the proof of the theorem is complete. □

5. Outlook

While the proof of Theorem 4.8 in many instances makes use of the solvability hypothesis, it is likely that with some effort the methods used can be expanded to work for arbitrary groups. Notice that Hypothesis (iii) in Lemma 3.8 typically will not be satisfied in nonsolvable groups, but by Remark 3.9 we can weaken it in the crucial situation to a condition involving class numbers only—and by results of Liebeck and Pyber [16] we know that $k(U) \leq 2^{n-1}$ for any $U \leq S_n$ (where S_n is the symmetric group on n letters); so this weakened hypothesis will be satisfied in arbitrary permutation groups.

Thus Hypothesis (ii) of Lemma 3.8 remains the critical one. A key point in verifying this condition in the proof of Theorem 4.8 was the well-known fact that a nontrivial element of a solvable primitive permutation group on a set Ω fixes at most half of the elements (see [17, Lemma 5.1]). But there are strong (slightly weaker) generalizations of this result to arbitrary primitive permutation groups available today, thanks to results of Guralnick and Magaard (see [8, Corollary 1]). Dealing with the exceptional cases in this result will be one of the problems one faces in generalizing our approach to arbitrary groups.

It is also interesting to compare the approach via Knörr to the approach presented here. The most difficult case in the proof in Theorem 4.8 occurs when the module V is induced from a module of a semilinear group. This case, however, does not provide any difficulty in the solution of the $k(GV)$-problem for solvable groups using Knörr's approach (see for example [25], or [3] for $|G|$ odd). Using this approach the case of primitive V is the most difficult whereas in our approach imprimitive modules are the hardest to come by.

Another interesting question is the following: One of the marvels of Knörr's paper [13] is the theorem that if $C_G(v)$ is abelian for some $v \in V$, then $k(GV) \leq |V|$, in particular this is the case if G has a regular orbit on V. Here a small piece of information that can often be verified yields the wanted conclusion which makes the result very powerful. Is this result somehow hidden in the approach here? Or is there a more elementary proof for it?

Finally, we point out that the proof of Theorem 4.8 involves a little bit of character theory only to deal with the above-mentioned most difficult case where V is induced from the module of a semilinear group. Here we invoked Gallagher's goodness property which is based on characters. It would be nice if we could replace it by our goodness property developed in Definition 3.5 and Lemma 3.6, so that the proof would be entirely group theoretical.

Acknowledgements

This work was initiated while I was a Research Fellow at the University of Leicester (UK) in 1998. I thank G. R. Robinson for inspiring conversations on the subject, and I am indebted to the Deutsche Forschungsgemeinschaft, the University of Leicester and Texas State University for financial support.

I also thank Robert Howlett for providing a shorter proof of Lemma 4.5.

References

[1] J. D. Dixon, 'The fitting subgroup of a linear solvable group', *J. Austral. Math. Soc.* **7** (1967), 417–424.
[2] P. X. Gallagher, 'The number of conjugacy classes in a finite group', *Math Z.* **118** (1970), 175–179.
[3] D. Gluck, 'On the $k(GV)$-problem', *J. Algebra* **89** (1984), 46–55.
[4] D. Gluck and K. Magaard, 'The extraspecial case of the $k(GV)$-problem', *Trans. Amer. Math. Soc.* **354** (2002), 287–333.
[5] ———, 'The $k(GV)$-conjecture for modules in characteristic 31', *J. Algebra* **250** (2002), 252–270.
[6] D. Goodwin, 'Regular orbits of linear groups with an application to the $k(GV)$-problem I', *J. Algebra* **227** (2000), 395–432.
[7] ———, 'Regular orbits of linear groups with an application to the $k(GV)$-problem II', *J. Algebra* **227** (2000), 433–473.
[8] R. Guralnick and K. Magaard, 'On the minimal degree of a primitive permutation group', *J. Algebra* **207** (1998), 127–145.
[9] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).
[10] ———, *Character theory of finite groups* (de Gruyter, Berlin, 1998).
[11] I. M. Isaacs, *Character theory of finite groups* (Academic Press, New York, 1976).
[12] T. M. Keller, 'Orbit sizes and character degrees, II', *J. Reine Angew. Math.* **516** (1999), 27–114.
[13] R. Knörr, 'On the number of characters in a p-block of a p-solvable group', *Illinois J. Math.* **28** (1984), 181–210.
[14] C. Koehler and H. Pahlings, 'Regular orbits and the $k(gv)$-problem', in: *Groups and computation, III*, Ohio State Univ. Math. Res. Inst. Publ. 8 (de Gruyter, Berlin, 2001).
[15] L. G. Kovács and G. R. Robinson, 'On the number of conjugacy classes of a finite group', *J. Algebra* **160** (1993), 441–460.
[16] M. W. Liebeck and L. Pyber, 'Upper bounds for the number of conjugacy classes of a finite group', *J. Algebra* **198** (1997), 538–562.
[17] O. Manz and T. R. Wolf, *Representations of solvable groups*, London Math. Soc. Lecture Notes Series 185 (Cambridge University Press, 1993).
[18] M. Murai, 'A note on the number of irreducible characters in a p-block with normal defect group', *Proc. Japan Acad. Ser. A* **59** (1983), 488–489.

[19] ———, 'A note on the number of irreducible characters in a p-block of a finite group', *Osaka J. Math.* **21** (1984), 387–398.

[20] H. Nagao, 'On a conjecture of Brauer for p-solvable groups', *J. Math. Osaka City Univ.* **13** (1962), 35–38.

[21] U. Riese, 'The quasisimple case of the $k(gv)$-conjecture', *J. Algebra* **235** (2001), 45–65.

[22] U. Riese and P. Schmid, 'Self-dual modules and real vectors for solvable groups', *J. Algebra* **227** (2000), 159–171.

[23] ———, 'Real vectors for linear groups and the $k(GV)$-problem', Preprint, 2001.

[24] G. R. Robinson, 'Further reductions for the $k(GV)$-problem', *J. Algebra* **195** (1997), 141–150.

[25] G. R. Robinson and J. G. Thompson, 'On Brauer's $k(B)$-problem', *J. Algebra* **184** (1996), 1143–1160.

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