# Derived length and conjugacy class sizes 

Thomas Michael Keller<br>Department of Mathematics, Texas State University, 601 University Drive, San Marcos, TX 78666, USA

Received 15 December 2003; accepted 16 November 2004
Communicated by D.J. Benson
Available online 29 December 2004


#### Abstract

Let $G$ be a finite solvable group, and let $F(G)$ be its Fitting subgroup. We prove that there is a universal bound for the derived length of $G / F(G)$ in terms of the number of distinct conjugacy class sizes of $G$. This result is asymptotically best possible. It is based on the following result on orbit sizes in finite linear group actions: If $G$ is a finite solvable group and $V$ a finite faithful irreducible $G$-module of characteristic $r$, then there is a universal logarithmic bound for the derived length of $G$ in terms of the number of distinct $r^{\prime}$-parts of the orbit sizes of $G$ on $V$. This is a refinement of the author's previous work on orbit sizes. © 2004 Elsevier Inc. All rights reserved.


MSC: 20E45; 20D60
Keywords: Solvable group; Derived length; Conjugacy classes

## 1. Introduction

A well-established area in the character theory of finite groups is the question which structural information on the group can be obtained from information on its irreducible complex characters. Early on it has been observed that results on conjugacy class sizes often share some similarity with results on character degrees, and so a question formulated for character degrees often can also be studied for conjugacy class sizes, and such questions have led to interesting results in the past, see e.g. [2, §33].

[^0]In this paper we are concerned with the Taketa problem for conjugacy classes. The original Taketa problem asks for bounds for the derived length $\mathrm{dl}(G)$ of a finite solvable group $G$ in terms of the number $|\operatorname{cd}(G)|$ of its irreducible complex character degrees. (See [6] for a survey of recent results on that problem.) Thus the Taketa problem for conjugacy classes asks for bounds for $\mathrm{dl}(G)$ in terms of $|\operatorname{cs}(G)|$, the number of distinct conjugacy class sizes of $G$. (Here $\operatorname{cs}(G)=\left\{\left|g^{G}\right| \mid g \in G\right\}$ is the set of conjugacy class sizes of $G$.) For $p$-groups, it has already been raised by Mann [10, Question 28]. It turns out that the Taketa problem for conjugacy classes is even more difficult than the original Taketa problem, at least for $p$-groups. It has long been known that $\mathrm{dl}(G) \leqslant|\operatorname{cd}(G)|$ for $p$-groups, so at least there is a linear bound (even though it is conjectured that the true bound is logarithmic). On the other hand, it has been shown only recently by Ishikawa [5] that $p$-groups with $|\operatorname{cs}(G)|=2$ have derived length 2 (and nilpotency class at most 3 ), and it is not known whether there is a bound for the derived length of $p$-groups $G$ with $|\operatorname{cs}(G)|=3$.

While there may not be any deeper general relationship between character degrees and conjugacy class sizes, there is at least one reason for the many similarities between results on the two invariants, namely the fact that the orbit sizes in the action of a group $G$ on a $G$-module $V$ are conjugacy class sizes of the semidirect product $G V$, whereas the orbit sizes of $G$ on $\operatorname{Irr}(V)$ are character degrees of $G V$. It seems as if whenever a result on $\operatorname{cd}(G)$ can be obtained via studying orbit sizes, a corresponding result can be proved for conjugacy classes. For $p$-groups, the orbit size approach breaks down, which might in part account for the fact that for $p$-groups there is no relationship between $|\operatorname{cd}(G)|$ and $|\operatorname{cs}(G)|$, as was shown by Moretó and Fernández-Alcober [1].

Since the author's recent results on the Taketa problem in [7-9] were based entirely on results on orbit sizes, Moretó asked whether those results would also yield results for the Taketa problem for conjugacy classes. The answer is yes, almost. We have to do some extra work. With this we obtain our main result:

Theorem A. There exist universal constants $C_{1}, C_{2}$ such that the following holds. If $G$ is a finite solvable group with Fitting subgroup $F(G)$, then

$$
\mathrm{dl}(G / F(G)) \leqslant C_{1} \log _{2}|\operatorname{cs}(G)|+C_{2}
$$

in particular, for the Fitting height $h(G)$ we have

$$
h(G) \leqslant C_{1} \log _{2}|\operatorname{cs}(G)|+C_{2}+1
$$

Of course, the result on $h(G)$ follows immediately from the bound on $\mathrm{dl}(G / F(G))$. We will prove Theorem A below with $C_{1}=24$ and $C_{2}=364$ (see Corollary 3.2 below). Certainly these constants (which come straight from [7, Theorem 2.1]) are not the best possible ones; however, asymptotically a logarithmic bound in Theorem A is the best that one can hope for, as is evidenced in Example 3.3 below.

The decisive link between conjugacy class sizes and orbit sizes is provided by Lemma 2.1 below and is essentially an old argument due to Glauberman. To use
that result, unlike for the Taketa problem it is not sufficient to bound $\mathrm{dl}(G)$ in terms of the number of different orbit sizes of $G$ on a $G$-module $V$, but rather we need to bound $\mathrm{dl}(G)$ in terms of the $r^{\prime}$-parts of the number of different orbit sizes of $G$ on $V$, where $r$ is the characteristic of $V$. So write

$$
m_{r^{\prime}}(G, V)=\left|\left\{\left|v^{G}\right|_{r^{\prime}} \mid v \in V\right\}\right|
$$

for the number of $r^{\prime}$-parts of the orbit sizes of $G$ on $V$. Inspection of the proofs in $[7,8]$ shows that they yield bounds for $\mathrm{dl}(G)$ in terms of $m_{r^{\prime}}(G, V)$ in many situations, in particular, when $|G|$ is odd. So for odd-order groups Theorem A follows right away from [7, Theorem 2.1] and Lemma 2.1 below. In the general case, however, there is one special situation where the proofs in [8] just do not yield a result on $m_{r^{\prime}}(G, V)$. This situation is dealt with in Section 2 of this paper. Together with the previous work this yields our second main result, from which Theorem A will follow readily.

Theorem B. Let $C_{1}$ and $C_{2}$ be as in Theorem A. If $G$ is a finite solvable group and $V$ a finite faithful irreducible $G$-module of characteristic $r$, then

$$
\mathrm{dl}(G) \leqslant C_{1} \log m_{r^{\prime}}(G, V)+C_{2}
$$

Obviously this is a refinement of the theorem in the introduction of [7], and we will prove it with the same constants $C_{1}, C_{2}$ as the ones in [7, Theorem 2.1] (see Theorem 3.1. below).

We finally note that the general conjecture that $\mathrm{dl}(G)$ is bounded in terms of $|\operatorname{cs}(G)|$ clearly by Theorem A is now reduced to the following

Conjecture C. There exists a function $f: \mathbb{N} \rightarrow \mathbb{R}$ such that if $G$ is a finite solvable group, then

$$
\mathrm{dl}(F(G)) \leqslant f(|\operatorname{cs}(G)|)
$$

This, of course, still includes the highly difficult case of $p$-groups.
Notation: Our notation is mostly standard. As in [11], we write, if $V=G F\left(q^{m}\right)$ for some prime $q$, the semi-linear group $\Gamma\left(q^{m}\right)=\Gamma(V)=\left\{x \mapsto a x^{\sigma} \mid a \in \mathrm{GF}\left(q^{m}\right)^{\#}, \sigma \in\right.$ $\left.\operatorname{Gal}\left(\mathrm{GF}\left(q^{m}\right) / \mathrm{GF}(q)\right)\right\}$. If $n \in \mathbb{N}$ and $p$ is a prime, then $n_{p}$ is the $p$-part and $n_{p^{\prime}}$ is the $p^{\prime}$-part of $n$. If $G$ is a group, then $O_{p}(G)$ denotes the largest normal $p$-subgroup of $G$, and a $p$-element of $G$ is an element of order a power of $p$. The minimal number of generators of a group $G$ is written as $d(G)$.

For groups $A, B$ we say that $A$ acts fixed point freely on $B$ if $A$ acts on $B$ (via automorphisms) and the semidirect product $A B$ is a Frobenius group with kernel $B$. We also say that $a \in A$ acts fixed point freely on $B$ if $\langle a\rangle$ acts fixed point freely on $B$.

Moreover, for a real number $x$ by $\lceil x\rceil$ and $\lfloor x\rfloor$ we mean the upper and lower integer part of $x$ (respectively).

## 2. $p^{\prime}$-parts of orbit sizes

In this section we collect all the results that we need to prove our main results.
2.1. Lemma. Let $G$ be a finite solvable group and $p$ be a prime. Write $P=O_{p}(G)$ and $V=P / \Phi(P)$. Suppose that $G$ has $r$ orbits in its action on $V$ whose sizes have mutually distinct $p^{\prime}$-parts. Then $G$ has $r$ conjugacy classes whose sizes have mutually distinct $p^{\prime}$-parts. In particular, $|\operatorname{cs}(G)| \geqslant r$.

Proof. Let $v_{i} \in P(i=1, \ldots, r)$ such that the $\overline{v_{i}}:=v_{i} \Phi(P)$ are representatives of orbits of $G$ on $V$ whose sizes have mutually distinct $p^{\prime}$-parts. Fix $j \in\{1, \ldots, r\}$. If $x \in \overline{v_{j}}$, then clearly $C_{G}(x) \Phi(P) / \Phi(P) \leqslant C_{G / \Phi(P)}\left(\overline{v_{j}}\right)$, and thus we see that $(*)$ $\left|C_{G}(x)\right|_{p^{\prime}} \leqslant\left|C_{G / \Phi(P)}\left(\overline{v_{j}}\right)\right|_{p^{\prime}}$, the latter being the $p^{\prime}$-part of the stabilizers of $\overline{v_{j}}$ in the action of $G$ on $V$. Now let $H$ be a Hall- $p^{\prime}$-subgroup of that stabilizer. Then $H$ acts on $P$ and fixes the set $\overline{v_{j}}$ (as a set). By an argument of Glauberman [3, I, Satz 18.6] we see that there exists a $w_{j} \in \overline{v_{j}}$ such that $H \leqslant C_{G}\left(w_{j}\right)$. With $(*)$ we conclude that $H$ is a Hall- $p^{\prime}$-subgroup of $C_{G}\left(w_{j}\right)$. Since $j$ was arbitrary, it follows that the $w_{j}$ $(j=1, \ldots, r)$ are representatives of conjugacy classes of $G$ whose sizes have mutually distinct $p^{\prime}$-parts, as wanted.
2.2. Hypothesis. Let $G$ be a finite group and $V$ be a finite faithful $F G$-module, where $F$ is a field. Suppose that there is an $S \unlhd G$ which is elementary abelian of order $q^{l}$ for a prime $q$, and suppose further that $V_{S}=W_{1} \oplus \cdots \oplus W_{t}$ for $S$-submodules $W_{i}$ of $V$ such that if $j \in\{1, \ldots, t\}$ and $x \in S$, then $x$ acts either fixed point freely or trivially on $W_{j}$. Assume also that each $g \in G$ (possibly trivially) permutes the $W_{i}(i=1, \ldots, t)$.
2.3. Lemma. Assume Hypothesis 2.2 and that $l \geqslant 2$.
(a) There is an $x \in S$ such that $x$ acts trivially on at least $\left\lceil\frac{t}{q+1}\right\rceil$ of the $W_{i}$.
(b) Let $x \in S$ such that the number $r$ of $W_{i}$ on which $x$ acts trivially is maximal. Let $y \in S$ with $y \notin\langle x\rangle$. Then $y$ acts trivially on at most $r-\left\lceil\frac{t-r}{q}\right\rceil$ of the $W_{i}$ with $W_{i} \leqslant C_{V}(x)$.
In particular, if $r \leqslant \frac{s-1}{s} t$ for some $s \in \mathbb{N}$ then $r-\left\lceil\frac{t-r}{q}\right\rceil \leqslant \frac{q(s-1)-1}{q(s-1)} r \leqslant \frac{q s-1}{q s} r$.
Proof. (a) Let $1 \neq x_{1} \in S$ and $x_{2} \in S-\left\langle x_{1}\right\rangle$ and put $U=\left\langle x_{1}, x_{2}\right\rangle \leqslant S$. Then $U$ has $q+1$ nontrivial cyclic subgroups. Moreover the $C_{U}\left(W_{i}\right), i=1, \ldots, t$, are nontrivial subgroups of $U$. Hence there must be an $1 \neq x \in U$ such that $\langle x\rangle$ is a subgroup of at least $\left\lceil\frac{t}{q+1}\right\rceil$ of the $C_{U}\left(W_{i}\right)$. So (a) follows.
(b) Let $X$ be the sum of those $W_{i}$ on which $x$ acts trivially, and let $Y$ be the sum of the $W_{i}$ on which $x$ acts nontrivially. Hence $V=X \bigoplus Y$ and $X$ is the sum of $r$ of the $W_{i}$, and $Y$ is the sum of $t-r$ of the $W_{i}$. Consider the action of $U=$ $\langle x, y\rangle$ on $Y$. As $x$ acts fixed point freely on $Y$, note that for all $W_{i} \leqslant Y$ we know that $C_{U}\left(W_{i}\right)$ is a nontrivial cyclic subgroup of $U$, and altogether there are $q$ nontrivial cyclic subgroups of $U$ different from $\langle x\rangle$. Hence there is a $z \in U$ that acts trivially on at least $\left\lceil\frac{t-r}{q}\right\rceil$ of the $W_{i} \leqslant Y$, and clearly we may assume that $z=x^{i} y$ for some
$i \in \mathbb{N}$. Now by the definition of $r$ clearly $z$ can act trivially on at most $r-\left\lceil\frac{t-r}{q}\right\rceil$ of the $W_{i} \leqslant X$, and as $x$ acts trivially on $X$, this means that also $y$ can act trivially on at most $r-\left\lceil\frac{t-r}{q}\right\rceil$ of the $W_{i} \leqslant X$ which is the first statement of (b). The second follows by simple arithmetic.
2.4. Lemma. Assume Hypothesis 2.2 and that the $C_{S}\left(W_{i}\right)(i=1, \ldots, t)$ are mutually distinct. Then the following hold:
(a) $C_{G}(S) \leqslant \bigcap_{i=1}^{t} N_{G}\left(W_{i}\right)$.
(b) Suppose that there is an $l \in \mathbb{R}$ such that $\left|C_{V}(g)\right| \leqslant|V|^{\frac{8 l-1}{8 l}}$ for all q-elements $g \in$ $C_{G}(S)$ and $\left|C_{V}(g)\right| \leqslant|V|^{\frac{l-1}{l}}$ for all $g \in S$. If $|G| \leqslant|V|^{\frac{1}{8 l}}$, then $G$ has a $q$-regular orbit on $V$ (i.e., an orbit whose size contains the full q-part of $|G|$ ).

Proof. (a) Let $j \in\{1, \ldots, t\}$ and $g \in C_{G}(S)$. Then $C_{S}\left(W_{j}\right)=C_{S}\left(W_{j}\right)^{g}=C_{S}\left(W_{j}^{g}\right)$, and so by hypothesis $W_{j}=W_{j}^{g}$. This proves (a).
(b) First we observe that by a routine argument (see e.g. [9, Lemma 1.2]) it follows that $\left|C_{V}(g)\right| \leqslant|V|^{\frac{2 l-1}{2 l}}$ for all $g \in G-C_{G}(S)$, and so by our hypothesis we conclude that

$$
\left|C_{V}(g)\right| \leqslant|V|^{\frac{8 l-1}{8 l}} \quad \text { for all } q \text {-elements } g \in G
$$

 and thus $|V| \leqslant \sum_{g \in G-\{1\}, g \text { a } ~}^{q \text {-element }}\left|C_{V}(g)\right|<|G||V|^{\frac{8 l-1}{8 l}}$. Hence $|G|>|V|^{\frac{1}{8 l}}$, a contradiction. This proves the lemma.

We are now ready to prove the crucial result we need. For the proof, we need the notion of a special pair as introduced in [8, Definition 3.2]. For the convenience of the reader we reproduce this definition here.
2.5. Definition. Let $p$ be a prime and $E$ be a group with a normal subgroup $N \leqslant E$ such that $E / N$ is elementary abelian of order $p^{m}$ for an integer $m$. Suppose that $E$ acts on a vector space $V$ over a finite field such that $V$ is a faithful $E$-module which is induced from a completely reducible $N$-module $W_{1}$. Consequently we can write

$$
V_{N}=W_{1} \oplus \cdots \oplus W_{p^{m}}
$$

with $W_{j}=W_{1}^{\overline{x_{j}}}$ for a suitable $\overline{x_{j}} \in E / N\left(j=1, \ldots, p^{m}\right)$. Furthermore, suppose that $N / C_{N}\left(W_{j}\right) \lesssim L$ (as a linear group on $W_{j}$ ) for all $j$, where $L$ is a solvable group acting faithfully and irreducibly on $W_{j}$ and having exactly one nontrivial orbit in its action on $W_{j}$. We also assume that $Z\left(F\left(N / C_{N}\left(W_{j}\right)\right)\right)>1$ and that this group acts fixed point freely on $W_{j}$.

Note that by Huppert's classification of solvable doubly transitive permutation groups (see [11, Theorem 6.8]) we know all the possible isomorphism types of $L$. Next we put $M=Z(F(N))$. So we have $1<M, M$ is abelian and $M / C_{M}\left(W_{j}\right)>1$ acts fixed point freely on $W_{j}$ (for all $j$ ). We assume that for any prime $q$ dividing $|M|$ for $Q \in \operatorname{Syl}_{q} M$ we have one of the following:

$$
\begin{aligned}
& C_{Q}\left(W_{j}\right)=1 \text { for } j=1, \ldots, p^{m} \text { (so that in this case } Q \text { is cyclic) } \\
& \text { or }(*) \text { the } C_{Q}\left(W_{j}\right), j=1, \ldots, p^{m} \text {, are mutually distinct. }
\end{aligned}
$$

Observe that the latter condition is equivalent to demanding that even the $C_{\Omega_{1}(Q)}\left(W_{j}\right)$, $j=1, \ldots, p^{m}$ are mutually distinct, as $Q$ acts faithfully on $V$ and $d\left(C_{Q}\left(W_{j}\right)\right)=$ $d(Q)-1$ for all $j$.

If we have this setting, then we say that $(E, V)$ is a special pair and also write $(E, V)=\left(E, V, N, M, p^{m}\right)$.
2.6. Theorem. Let p be a prime. Suppose that $G$ is a finite solvable group which acts faithfully and irreducibly on a $G$-module $V$ over $G F\left(p^{f}\right)$ for some $f \in \mathbb{N}$. Also suppose that for some $N \unlhd G$ we have the Clifford decomposition $V_{N}=W_{1} \oplus \cdots \oplus W_{n}$ (where $n=p^{m}$ for some $\left.m \in \mathbb{N}\right)$ into homogeneous components $W_{i}(i=1, \ldots, n)$ which are faithfully and primitively permuted by $G / N$. Suppose further that $H:=N_{G}\left(W_{1}\right)$ has exactly one nontrivial orbit on $W_{1}$. Put $M=Z(F(N)) \unlhd G$ and $k=d(M)$. Assume that $k \leqslant \frac{m^{2}}{4} \log _{2} p$. Then

$$
m_{p^{\prime}}(G, V) \geqslant\left\lfloor\frac{\sqrt{m}}{8}\right\rfloor .
$$

Proof. Clearly we may assume that $m \geqslant 100$. Let $N<E \unlhd G$ such that $E / N$ is the unique minimal normal subgroup of $G / N$. As in the beginning of the proof of [8, Theorem 3.20] we see that $(E, V)$ is a special pair. We proceed in several steps.

Step 1: $M$ (and thus $F(N)$ ) is a $p^{\prime}$-group and $k \geqslant \frac{2}{3} m$. For any noncyclic Sylow subgroup $T$ of $M$ we have $d(T) \geqslant \frac{2}{3} m$.

As $\operatorname{char}(V)=p$, it is clear that $p$ does not divide $|M|$. Next note that $C_{E}(N) \leqslant N$, because otherwise there would be an $x \in C_{E}(N)-N$ so that $W_{1}$ and $W_{1}^{x}\left(\neq W_{1}\right)$ would be isomorphic $N$-modules contradicting the fact that $W_{1}$ and $W_{1}^{x}$ are different homogeneous components of $V_{N}$. Thus $E / N$ is isomorphic to a chief factor of $G / C_{G}(N) \leqq$ Aut $N$.

Clearly the structure of $N$ is well known (see [11, Theorem 6.8]). We next show that $M$ is not cyclic by using an argument already employed in [8, p. 91]. First recall that $C_{E}(N) \leqslant N$. Assume that $M$ is cyclic. Then $M$ acts faithfully on each $W_{i}$, so $E / N$ is isomorphic to a chief factor of $G / C_{G}(N) \leqq$ Aut $(N)$. But as $m \geqslant 100$ and $N$ is isomorphic to a subgroup of $H / C_{H}\left(W_{1}\right)$ which has only one nontrivial orbit on $W_{1}$, it is clear that $\operatorname{Aut}(N)$ does not have such a large composition factor. This contradiction shows that $M$ is not cyclic and thus $k \geqslant 2$.

Remember that as $(E, V)$ is a special pair, any noncyclic Sylow subgroup $T$ of $M$ satisfies Definition $2.5(*)$, and hence if $S \in \operatorname{Syl}_{p}(E)$, then $d\left(S / C_{S}(T)\right) \geqslant m$. As $p$ does not divide $|T|$, a result of Isaacs [4, Theorem A] readily implies that $m \leqslant \frac{3}{2} d(T)$ and thus $d(T) \geqslant \frac{2}{3} m$.

Step 2: We have that

$$
|G| \leqslant p^{\frac{13}{4} m}\left|W_{1}\right|^{\frac{m^{2}}{2} \log _{2} p}
$$

Observe that $|G| \leqslant|G / E| \cdot|E / N| \cdot|N|$, and as $E / N$ is an irreducible and faithful $G / E-$ module, by [11, Theorem 3.5] we have $|G / E| \leqslant p^{\frac{9}{4} m}$ and thus $|G| \leqslant p^{\frac{9}{4} m} \cdot p^{m} \cdot|N|=$ $p^{\frac{13}{4} m} \cdot|N|$. Next note that by the proof of [8, Lemma 3.5] we may assume (by possibly renumbering the $W_{i}$ ) that

$$
\bigcap_{i=1}^{k} C_{N}\left(W_{i}\right)=C_{N}\left(\bigoplus_{i=1}^{k} W_{i}\right)=1
$$

and thus

$$
|N| \leqslant\left|N / C_{N}\left(W_{1}\right)\right|^{k}
$$

Now from [11, Theorem 6.8] it is clear that $\left|H / C_{G}\left(W_{1}\right)\right| \leqslant\left|W_{1}\right|^{2}$, and hence $\mid N / C_{N}$ $\left(W_{1}\right)\left|\leqslant\left|H / C_{G}\left(W_{1}\right)\right| \leqslant\left|W_{1}\right|^{2}\right.$. So altogether

$$
|G| \leqslant p^{\frac{13}{4} m}|N| \leqslant p^{\frac{13}{4} m}\left|N / C_{N}\left(W_{1}\right)\right|^{k} \leqslant p^{\frac{13}{4} m} \cdot\left|W_{1}\right|^{2 k} \leqslant p^{\frac{13}{4} m} \cdot\left|W_{1}\right|^{\frac{m^{2}}{2} \log _{2} p}
$$

as wanted.
Step 3: We may assume that $q \leqslant p^{\sqrt{m}}$ for any prime $q$ dividing $|M|$ with noncyclic Sylow $q$-subgroup of $M$.

Suppose that there is a prime $q$ dividing $|M|$ such that the Sylow $q$-subgroup of $M$ is not cyclic and such that $q>p^{\sqrt{m}}$. Let $0 \neq w_{i} \in W_{i}$ for all $i$ and define $v_{j}=\sum_{i=1}^{j} w_{i}$ for $j=1, \ldots, n$, so that $C_{N}\left(v_{i}\right) \geqslant C_{N}\left(v_{j}\right)$ for all $i \leqslant j$. Now by Step 1 , if $Q \in \operatorname{Syl}_{q} M$, then $Q$ is abelian and $d(Q) \geqslant \frac{2}{3} m$. So if we put $s=\left\lfloor\frac{2}{3} m\right\rfloor$, then it is clear that there are $x_{1}, \ldots, x_{s} \in\left\{v_{i} \mid i=1, \ldots, n\right\}$ such that $C_{Q}\left(x_{i}\right)>C_{Q}\left(x_{i+1}\right)$ for $i=1, \ldots, s-1$, which implies that $\frac{\left|C_{N}\left(x_{i}\right)\right|}{\left|C_{N}\left(x_{i+1}\right)\right|} \geqslant q>p^{\sqrt{m}}$. Moreover, as in Step 2 by [11, Theorem 3.5] we see that $|G / E| \leqslant p^{\frac{9}{4} m}$ and thus $|G / N|_{q} \leqslant p^{\frac{9}{4} m} \leqslant q^{\frac{9}{4} \sqrt{m}}$ (as $q \neq p$ ). Therefore it is easy to see that

$$
\left|C_{G}\left(x_{\left\lceil k \frac{9}{4} \sqrt{m}+1\right\rceil}\right)\right|_{q}>\left|C_{G}\left(x_{\left\lceil(k+1) \frac{9}{4} \sqrt{m}+1\right\rceil}\right)\right| \quad \text { for } k=1, \ldots,\left\lfloor\frac{s-2}{\frac{9}{4} \sqrt{m}}\right\rfloor-1
$$

and consequently

$$
m_{p^{\prime}}(G, V) \geqslant \frac{s-2}{\frac{9}{4} \sqrt{m}} \geqslant \frac{4}{9} \frac{\frac{2}{3} m-3}{\sqrt{m}} \geqslant \frac{2}{9} \sqrt{m}
$$

so that we are done. Hence Step 3 is proved.
Step 4: Let $1 \neq x \in M$. Then $x$ acts fixed point freely on at least $\frac{4 p^{m}}{m^{2} \log _{2} p}$ of the $W_{i}$.
To prove this, we may assume that the order of $x$ is a prime $p_{1}$, so $x \in \Omega_{1}\left(P_{1}\right)$, where $P_{1} \in \operatorname{Syl}_{p_{1}} M$. Now let $P_{2}=\left\langle x^{g} \mid g \in G\right\rangle$, so $P_{2}$ is an elementary abelian normal subgroup of $G$ and thus, as $V$ is an irreducible and faithful $G$-module, $C_{V}\left(P_{2}\right)=0$. Now choose $g_{i} \in G$ such that the $x_{i}=x^{g_{i}}, i=1, \ldots, d=d\left(P_{2}\right)$, form a minimal set of generators of $P_{2}$. Then if $x$ acts fixed point freely on exactly $t_{0}$ of the $W_{i}$, so does each $x_{i}$. In particular we see by an easy induction that $C_{V}\left(\left\langle x_{1}, \ldots, x_{i}\right\rangle\right)$ is the sum of at least $p^{m}-i t_{0}$ of the $W_{i}$. As $0=C_{V}\left(P_{2}\right)=C_{V}\left(\left\langle x_{1}, \ldots, x_{d}\right\rangle\right)$, this means that $p^{m}-d t_{0} \leqslant 0$ and thus $t_{0} \geqslant \frac{p^{m}}{d}$. Now by hypothesis we have $d \leqslant \frac{m^{2}}{4} \log _{2} p$, and so the assertion of Step 4 follows.

Step 5: Conclusion.
We begin by choosing a prime $q$ dividing $|M|$ in the following way. Remember that $V$ is a $G F\left(p^{f}\right)$-vector space; let $p_{0}=p^{f}$ and $s=\operatorname{dim} W_{1}$. By Huppert's result [11, Theorem 6.8] (which is also restated in [8, Theorem 3.1]) we know the structure of $L:=N_{G}\left(W_{1}\right) / C_{G}\left(W_{1}\right)$, and using that result we choose $q$ as follows:

Case A: Suppose that $L \leqslant \Gamma\left(p_{0}^{s}\right)$. Then as $L$ has exactly one nontrivial orbit on $W_{1}$, clearly $\left(p_{0}^{s}-1\right)||L|$, and so $| L \mid$ is divisible by all Zsigmondy prime divisors of $p_{0}^{s}-1$.
(i) If there is a Zsigmondy prime divisor $r$ of $p_{0}^{s}-1$ (i.e., a prime $r$ dividing $p_{0}^{s}-1$, but not dividing $p_{0}^{i}-1$ for any $1 \leqslant i \leqslant s-1$ ) such that the Sylow $r$-subgroup of $M$ is not cyclic, then let $q=r$.
(ii) If there is a Zsigmondy prime divisor $r$ of $p_{0}^{S}-1$, but none for which the Sylow $r$-subgroup of $M$ is not cyclic, then let $q$ be any prime divisor of $M$ for which the Sylow $q$-subgroup of $M$ is not cyclic (such a prime exists by Step 1). Next suppose that there is no Zsigmondy prime divisor of $p_{0}^{s}-1$. By [11, Theorem 6.2 and Proposition 3.1] we have either $s=2$ and $p_{0}=p$ is a Mersenne prime, or $n=6$ and $p_{0}=2$.
(iii) In the first case, if there is an odd prime divisor $r$ of $p^{2}-1$ such that the Sylow $r$-subgroup of $M$ is not cyclic, let $q=r$.
(iv) Otherwise let $q=2$.
(v) If $n=6$ and $p=2$, then if the Sylow 7 -subgroup of $M$ is not cyclic, let $q=7$.
(vi) Otherwise let $q=3$.

Case B: Suppose that $L$ is one of the exceptional groups in [11, Theorem 6.8].
(i) In the situation of [11, Theorem 6.8(a)], choose $q=2$.
(ii) In the situation of [11, Theorem 6.8(b)], if there is an odd prime $r$ of $|F(L)|$ such that the Sylow $r$-subgroup of $M$ is not cyclic, let $q=r$, unless $\left|W_{1}\right|=7^{2}$ and $|F(L)|=2^{3} \cdot 3$ and the Sylow 2-subgroup of $M$ is not cyclic, in which case we let $q=2$.
(iii) Otherwise let $q=2$.

Observe that in any case $Q_{0} \in \operatorname{Syl}_{q} M$ is not cyclic, and put $E_{0}=\Omega_{1}\left(Q_{0}\right) \unlhd G$. Then (by Step 1) $d=d\left(E_{0}\right) \geqslant \frac{2}{3} m$. Now define $1=A_{0}<A_{1}<\cdots<A_{d}=E_{0}$ as follows: $A_{0}=1$, and if $A_{i}$ has already been defined for some $i \geqslant 0$ then observe that $C_{V}\left(A_{i}\right)$ is a sum of some of the $W_{j}$, and let $a_{i+1} \in E$ be such that $\mid\left\{j \mid W_{j} \leqslant C_{V}\left(A_{i}\right)\right.$ and $a_{i+1}$ acts trivially on $\left.W_{j}\right\} \mid$ is maximal. Then put $A_{i+1}=$ $\left\langle A_{i}, a_{i+1}\right\rangle$. Observe that with this definition of the $A_{i}$ by Lemma 2.3(a) (applied to $E / A_{i}$ acting on $\left.C_{V}\left(A_{i}\right)\right)$ and an easy induction we have that $C_{V}\left(A_{i}\right)$ is the sum of at least $\frac{p^{m}}{(q+1)^{i}}$ of the $W_{i}$. Moreover, by Step 4 each $y \in E$ acts trivially on at most $p^{m}-\frac{4 p^{m}}{m^{2} \log _{2} p}=\frac{s_{0}-1}{s_{0}} p^{m}$ of the $W_{i}$, where $s_{0}=\frac{m^{2}}{4} \log _{2} p$. Hence by Lemma 2.3(b) and an easy induction we observe that each $y \in E_{0}-A_{i}$ acts trivially on at most $\frac{q^{i} s_{0}-1}{q^{i} s_{0}} r_{i}$ of the $W_{i}$ with $W_{i} \leqslant C_{V}\left(A_{i}\right)$, where $r_{i}$ denotes the number of $W_{i}$ with $W_{i} \leqslant C_{V}\left(A_{i}\right)$. In particular, we have $\left|C_{V}\left(A_{i}\right)\right|=\left|W_{1}\right|^{r_{i}}$ and thus

$$
\left|C_{C_{V}\left(A_{i}\right)}(\bar{y})\right| \leqslant\left|C_{V}\left(A_{i}\right)\right|^{\frac{q^{i} s_{0}-1}{q^{i} s_{0}}} \quad \text { for all } \bar{y} \in E_{0} / A_{i}(i=1, \ldots, d)
$$

Now fix $i \in\{1, \ldots, d\}$ and put $M_{i}=N_{G}\left(A_{i}\right)$ and $V_{i}=C_{V}\left(A_{i}\right)$. If $v \in V_{i}$ lies in a regular orbit of $E_{0} / A_{i}$ on $V_{i}$, then $A_{i}=E_{0} \cap C_{G}(v) \unlhd C_{G}(v)$ which implies that $C_{G}(v) \leqslant M_{i}$. Also note that by our construction of the $A_{i}$ it is clear that $E_{0} / A_{i}$ acts faithfully on $V_{i}$, and therefore we have $N_{G}\left(V_{i}\right)=M_{i}$, because clearly $N_{G}\left(A_{i}\right) \leqslant N_{G}\left(V_{i}\right)$, and if there were a $g \in N_{G}\left(V_{i}\right)-N_{G}\left(A_{i}\right)$, then we would have $C_{V}\left(A_{i}\right)=C_{V}\left(A_{i}\right)^{g}=C_{V}\left(A_{i}^{g}\right)$ and $A_{i}<\left\langle A_{i}, A_{i}^{g}\right\rangle \leqslant E_{0}$ and $C_{V}\left(A_{i}\right)=C_{V}\left(\left\langle A_{i}, A_{i}^{g}\right\rangle\right)$ so that there would be a $h \in$ $\left\langle A_{i}, A_{i}^{g}\right\rangle-A_{i}$ acting trivially on $V_{i}$, against the faithful action of $E_{0} / A_{i}$ on $V_{i}$.

Now consider the action of $\overline{M_{i}}=M_{i} / C_{M_{i}}\left(V_{i}\right)$ on $V_{i}$. Using Lemma 2.4 we want to identify values of $i$ for which $\overline{M_{i}}$ has a $q$-regular orbit on $V_{i}$. Note that if $v_{i} \in V_{i}$ is in such an orbit, then $v_{i}$ is in a regular orbit of $E_{0} / A_{i}$ on $V_{i}$ and thus $C_{G}\left(v_{i}\right)=C_{M_{i}}\left(v_{i}\right)$ and

$$
\begin{equation*}
\left|C_{G}\left(v_{i}\right)\right|_{q}=\left|C_{M_{i}}\left(V_{i}\right)\right|_{q}=\left|C_{G}\left(V_{i}\right)\right|_{q}, \tag{0}
\end{equation*}
$$

the latter equality following as $M_{i}=N_{G}\left(V_{i}\right)$.
Observe that the action of $\overline{M_{i}}$ satisfies the general hypothesis of Lemma 2.4, where $\overline{E_{0}}:=E_{0} / A_{i} \cong E_{0} C_{M_{i}}\left(V_{i}\right) / C_{M_{i}}\left(V_{i}\right)$ plays the role of $S$; in particular, the $C_{\overline{E_{0}}}\left(W_{j}\right)$ (for all $W_{j} \leqslant V_{i}$ ) are mutually distinct just because the $C_{E_{0}}\left(W_{j}\right)$ are different, as $(E, V)$
is a special pair. By Lemma 2.4(a) we have

$$
\begin{equation*}
C_{\overline{M_{i}}}\left(\overline{E_{0}}\right) \leqslant \bigcap_{j \text { with } W_{j} \leqslant V_{i}} N_{\overline{M_{i}}}\left(W_{j}\right) \leqq X_{j \text { with } W_{j} \leqslant V_{i}} \Gamma\left(W_{j}\right) . \tag{1}
\end{equation*}
$$

We now have to verify the hypothesis of Lemma 2.4(b), which is a little more troublesome. As seen above, we have $(*)\left|C_{V_{i}}(\bar{y})\right| \leqslant\left|V_{i}\right|^{\frac{q^{i} s_{0}-1}{q^{i} s_{0}}}$ for all $\bar{y} \in \overline{E_{0}}$. Next we put $l_{i}=q^{i} s_{0}$ and want to show that

$$
\begin{equation*}
\left|C_{V_{i}}(\bar{y})\right| \leqslant\left|V_{i}\right|^{\frac{8 l_{i}-1}{8 l_{i}}} \text { for all } q \text {-elements } \bar{y} \in C_{\overline{M_{i}}}\left(\overline{E_{0}}\right) . \tag{2}
\end{equation*}
$$

To see this, we have to consider all situations $\mathrm{A}(\mathrm{i})-(\mathrm{vi})$ and $\mathrm{B}(\mathrm{i})-(\mathrm{iii})$ outlined above.
In Case $\mathrm{A}(\mathrm{i})$, let $\bar{Q} \in \operatorname{Syl}_{q}\left(C_{\overline{M_{i}}}\left(\overline{E_{0}}\right)\right)$. Then by (1) and [11, Lemma 6.5(c)] it follows that $\bar{Q} \leqslant F\left(C_{\overline{M_{i}}}\left(\overline{E_{0}}\right)\right) \leqq X_{j}$ with $W_{j} \leqslant V_{i} \Gamma_{0}\left(W_{i}\right)$, and so $\bar{Q} \unlhd \overline{M_{i}}$ is abelian and $\bar{Q} \leqslant \bar{M}$. Therefore we have $\bar{Q}=Q_{0} C_{M_{i}}\left(V_{i}\right) / C_{M_{i}}\left(V_{i}\right)=: \overline{Q_{0}}$. Now if $x \in Q_{0}$ with $x^{q} \in C_{M_{i}}\left(V_{i}\right)$, then $x^{q}$ acts trivially on all $W_{j}$ with $W_{j} \leqslant V_{i}$, and as for each $z \in M$ and $l \in\{1, \ldots, n\} z$ acts either fixed point freely or trivially on $W_{l}$, we further see that $x \in C_{M_{i}}\left(V_{i}\right)$.

This shows that $\Omega_{1}\left(\overline{Q_{0}}\right) \leqslant \Omega_{1}\left(Q_{0}\right) C_{M_{i}}\left(V_{i}\right) / C_{M_{i}}\left(V_{i}\right)=\overline{\Omega_{1}\left(Q_{0}\right)}$, and as trivially $\overline{\Omega_{1}\left(Q_{0}\right)} \leqslant \Omega_{1}\left(\overline{Q_{0}}\right)$, we have that $\Omega_{1}(\bar{Q})=\Omega_{1}\left(\overline{Q_{0}}\right)=\overline{\Omega_{1}\left(Q_{0}\right)}$ and so $\Omega_{1}(\bar{Q})=\overline{E_{0}}$. Thus all $q$-elements of $C_{\overline{M_{i}}}\left(\overline{E_{0}}\right)$ are in $\bar{Q}$. The same is true (for similar reasons) in Cases $\mathrm{A}(\mathrm{iii})$ and $\mathrm{A}(\mathrm{v})$ (as is clear by (1) and [11, Lemma 6.5]), and $\mathrm{B}(\mathrm{ii})$ when $q \notin\{2,3\}$. So in all these cases it follows immediately by $(*)$ that $\left|C_{V_{i}}(\bar{y})\right| \leqslant\left|V_{i}\right|^{\frac{l_{i}-1}{l_{i}}}$ for all $\bar{y} \in \bar{Q}$ so that (2) follows.

In Case $\mathrm{A}(i i)$ let $r$ be a Zsigmondy prime divisor of $p_{0}^{s}-1$, and so $r||L|$. Let $x \in L$ be of order $r$. By [11, Lemma 6.4 and Lemma 6.5(c)] we have $C_{L}(x)=F(L)$ and $r$ does not divide $|L / F(L)|$.

Now consider the case that $x \notin N_{0}:=N C_{G}\left(W_{1}\right) / C_{G}\left(W_{1}\right)$. We want to show that $N_{0}$ is cyclic. Clearly $N_{0} \unlhd L$ and $\langle x\rangle \unlhd L$, hence [ $\left.N_{0},\langle x\rangle\right] \leqslant N_{0} \cap\langle x\rangle=1$, so $N_{0} \leqslant C_{L}(x)$, and $C_{L}(x)$ is cyclic by [11, Lemma 6.5(c)]. Thus indeed $N_{0}$ is cyclic, and thus $N$ is abelian. Next consider the case that $x \in N C_{G}\left(W_{1}\right) / C_{G}\left(W_{1}\right)$. Then even $x \in M C_{G}\left(W_{1}\right) / C_{G}\left(W_{1}\right)$, and since in Case A(ii) we know that $\left\langle x^{g} \mid g \in G\right\rangle=\langle x\rangle$ is cyclic, we see that

$$
\begin{aligned}
C_{N}(\langle x\rangle) C_{N}\left(W_{i}\right) / C_{N}\left(W_{i}\right) & \leqslant C_{N / C_{N}\left(W_{i}\right)}\left(\langle x\rangle C_{N}\left(W_{i}\right) / C_{N}\left(W_{i}\right)\right) \\
& \leqslant F\left(N / C_{N}\left(W_{i}\right)\right)=: F_{i} / C_{N}\left(W_{i}\right)
\end{aligned}
$$

for all $i$, whence $C_{N}(\langle x\rangle) \leqslant \bigcap_{i=1}^{n} F_{i}=F(N)$ (by [11, Proposition 9.5]). Hence $C_{N}(\langle x\rangle)=F(N)$, and so $N / F(N)=N / C_{N}(\langle x\rangle) \leqq$ Aut $(\langle x\rangle)$ which is cyclic. Therefore in Case A(ii) we always know that $N / F(N)$ is cyclic and thus any $g \in N-F(N)$ acts nontrivially on each $W_{i}$. In Case $\mathrm{A}(\mathrm{vi})$, by [11, Lemma 6.5] every 3-element
$g \in N-F(N)$ acts nontrivially on each $W_{i}$, and the same is true in Case $\mathrm{B}(\mathrm{ii})$ when $q=3$. Hence in these cases we see that $\left|C_{W_{i}}(g)\right| \leqslant\left|W_{1}\right|^{\frac{1}{2}}$ for all $q$-elements $g \in N-F(N)$ and thus $\left|C_{V_{i}}(\bar{y})\right| \leqslant\left|V_{i}\right|^{\frac{1}{2}}$ for all $q$-elements $\bar{y} \in C_{\overline{M_{i}}}\left(\overline{E_{0}}\right)$, which implies (2).

Next observe that in Case A(iv), if $\bar{K}$ is the inverse image of a Sylow 2-subgroup of $X_{j}$ with $W_{j} \leqslant V_{i} \Gamma_{0}\left(W_{j}\right)$ in the embedding $C_{\overline{M_{i}}} \overline{\left(E_{0}\right)} \leqq X_{j}$ with $W_{j} \leqslant V_{i} \Gamma\left(W_{j}\right)$, then $\bar{K} \unlhd \overline{M_{i}}$, and similarly as in the Case $\mathrm{A}(\mathrm{i})$ we obtain that $\overline{E_{0}}=\Omega_{1}(\bar{K})$, so that by ( $*$ ) we have $\left|C_{V_{i}}(\bar{y})\right| \leqslant\left|V_{i}\right|^{\frac{l_{i}-1}{l_{i}}}$ for all $\bar{y} \in \bar{K}$. Moreover no 2-element of $C_{\overline{M_{i}}}\left(\overline{E_{0}}\right)$ centralizes $\bar{K}$, and so the usual routine argument already mentioned in the proof of Lemma 2.4 yields $\left|C_{V_{i}}(\bar{y})\right| \leqslant\left|V_{i}\right|^{\frac{2 l_{i}-1}{l_{i}}}$ and thus (2) for all 2-elements of $C_{\overline{M_{i}}}\left(\overline{E_{0}}\right)$, as wanted.

A similar argument yields (2) in the remaining cases as well. In Case B (ii) when $q=$ 2, and in Case B (iii) simply work with $\bar{K}$ being the inverse image of $X_{j}$ with $W_{j} \leqslant V_{i} Q_{8}$ in the embedding $C_{\overline{M_{i}}}\left(\overline{E_{0}}\right) \leqq X_{j}$ with $W_{j} \leqslant V_{i} N_{G}\left(W_{j}\right) / C_{G}\left(W_{j}\right)$ and proceed as in Case A(iv). In Case B(i), work with $\bar{K}$ being the inverse image of $X_{j}$ with $W_{j} \leqslant V_{i} E\left(2^{5}\right)$ (where $E\left(2^{5}\right)$ denotes an extraspecial group of order $2^{5}$ ) and note that for $\bar{y} \in \bar{K}$ by [9, Lemma 1.2] $\left|C_{W_{j}}(\bar{y})\right| \leqslant\left|W_{j}\right|^{3 / 4}$ whenever $\bar{y}$ acts nontrivially on $W_{j}$. Moreover as each $\bar{x} \in \overline{E_{0}}$ acts trivially on at most $\frac{l_{i}-1}{l_{i}}$ of the $W_{j}$ with $W_{j} \leqslant V_{i}$, we see that each $\bar{y}$ can also act trivially on at most $\frac{l_{i}-1}{l_{i}}$ of the $W_{j} \leqslant V_{i}$, and thus

$$
\left|C_{V_{i}}(\bar{y})\right| \leqslant\left|V_{i}\right|^{\frac{l_{i}-1}{l_{i}}} \cdot\left(\left|V_{i}\right|^{3 / 4}\right)^{\frac{1}{T_{i}}}=\left|V_{i}\right|^{\frac{4 l_{i}-1}{l_{i}}}
$$

for all $\bar{y} \in \bar{K}$. Finally, as no 2-element $\bar{y} \in C_{\overline{M_{i}}}\left(\overline{E_{0}}\right)-\bar{K}$ centralizes $\bar{K}$, the routine argument used before yields (2).

So (2) is proved in all cases. Now Lemma 2.4(b) yields a $v_{i} \in V_{i}$ satisfying (0) provided that $\left|\overline{M_{i}}\right| \leqslant\left|V_{i}\right|^{\frac{1}{\bar{q}_{i}}}$. To make this happen, it suffices that

$$
\left|\overline{M_{i}}\right| \leqslant\left|W_{1}\right|^{\frac{p^{m}}{p_{i}(q+1)^{i}}},
$$

as $\left|V_{i}\right| \geqslant\left|W_{1}\right|^{\frac{p^{m}}{(q+1)^{i}}}$ (as we saw above with Lemma 2.3(a)), and for that as by Step 2

$$
\left|\overline{M_{i}}\right| \leqslant|G| \leqslant p^{\frac{13}{4} m}\left|W_{1}\right|^{\frac{m^{2}}{2} \log _{2} p},
$$

it suffices that

$$
p^{\frac{13}{4} m}\left|W_{1}\right|^{\frac{m^{2}}{2} \log _{2} p} \leqslant\left|W_{1}\right|^{\frac{p^{m}}{8_{i}(q+1)^{i}}}
$$

or

$$
p^{\frac{13}{4} m} \leqslant\left|W_{1}\right|^{\frac{p^{m}}{8_{i}(q+1)^{i}} i} \frac{m^{2}}{2} \log _{2} p .
$$

As $l_{i}=q^{i} s_{0}=q^{i} \frac{m^{2}}{4} \log _{2} p$ and, by Step $3, q \leqslant p^{\sqrt{m}}$, we see that

$$
8 l_{i}(q+1)^{i} \leqslant 8 p^{i \sqrt{m}} \frac{m^{2}}{4}\left(\log _{2} p\right)\left(p^{\sqrt{m}}+1\right)^{i} \leqslant 2^{i+1} m^{2} p^{2 i \sqrt{m}} \log _{2} p
$$

and so it suffices that

$$
p^{\frac{13}{4} m} \leqslant\left|W_{1}\right|^{\frac{p^{m}}{2^{i+1} m^{2} p^{2 i \sqrt{m}} \log _{2} p}}-\frac{m^{2}}{2} \log _{2} p .
$$

From now on consider only $i$ with $i \leqslant \frac{1}{8} \sqrt{m}$. Then the exponent of $\left|W_{1}\right|$ in the previous inequality is positive, and as clearly $\left|W_{1}\right| \geqslant p$, it suffices to have

$$
\frac{13}{4} m \leqslant \frac{p^{m}}{2^{i+1} m^{2} p^{2 i \sqrt{m}} \log _{2} p}-\frac{m^{2}}{2} \log _{2} p
$$

and as $\frac{m^{2}}{2} \log _{2} p \geqslant \frac{13}{4} m$, for that it suffices that

$$
m^{2} \log _{2} p \leqslant \frac{p^{m-2 i \sqrt{m}}}{2^{i+1} m^{2} \log _{2} p}
$$

which is equivalent to

$$
2^{i+1} m^{4}\left(\log _{2} p\right)^{2} \leqslant p^{m-2 i \sqrt{m}}
$$

For this, as $p \geqslant 2$, it suffices that

$$
m^{4}\left(\log _{2} p\right)^{2} \leqslant p^{m-2 i \sqrt{m}-i-1}
$$

and this is implied by

$$
m^{4}\left(\log _{2} p\right)^{2} \leqslant p^{m-4 i \sqrt{m}}
$$

Now as $i \leqslant \frac{1}{8} \sqrt{m}$, then $i \leqslant \frac{\sqrt{m}}{4}-\frac{1}{\sqrt{m}}=\frac{m-4}{4 \sqrt{m}}$ and $m-4 i \sqrt{m} \geqslant 4$, and hence it suffices that

$$
m^{4} \leqslant\left(\frac{p}{\sqrt{\log _{2} p}}\right)^{m-4 i \sqrt{m}}
$$

and as $\frac{p}{\sqrt{\log _{2} p}} \geqslant 2$, we conclude that to apply Lemma 2.4(b), it suffices to have an $i \leqslant \frac{1}{8} \sqrt{m}$ with

$$
\begin{equation*}
m^{4} \leqslant 2^{m-4 i \sqrt{m}}=2^{\sqrt{m}(\sqrt{m}-4 i)} \tag{3}
\end{equation*}
$$

Now as $i \leqslant \frac{1}{8} \sqrt{m}$, then (3) holds if $m^{4} \leqslant 2^{\frac{m}{2}}$ which is the case as $m \geqslant 100$. Hence by Lemma 2.4 for $i=1, \ldots,\left\lfloor\frac{1}{8} \sqrt{m}\right\rfloor$ there are $v_{i} \in V_{i}$ such that $\left|C_{G}\left(v_{i}\right)\right|_{q}=\left|C_{G}\left(V_{i}\right)\right|_{q}$, and thus as $V_{1}>V_{2}>\cdots>V_{d}$ and $C_{E_{0}}\left(V_{1}\right)<C_{E_{0}}\left(V_{2}\right)<\cdots<C_{E_{0}}\left(V_{d}\right)$, we have

$$
\left|C_{G}\left(v_{1}\right)\right|_{q}<\left|C_{G}\left(v_{2}\right)\right|_{q}<\cdots<\left|C_{G}\left(v_{\left\lfloor\frac{1}{8} \sqrt{m}\right\rfloor}\right)\right|_{q}
$$

so that $m_{p^{\prime}}(G, V) \geqslant\left\lfloor\frac{1}{8} \sqrt{m}\right\rfloor$ which is the assertion of the theorem. So the proof of the theorem is complete.

We now can strengthen [8, Theorem 3.20].
2.7. Theorem. Suppose that $G$ is a finite solvable group which acts faithfully and irreducibly on a G-module $V$ over a finite field of characteristic $r$. Suppose that for some $N \unlhd G$ we have the Clifford decomposition $V_{N}=W_{1} \oplus \cdots \oplus W_{n}$ (for an $n>1$ ) into homogeneous components $W_{i}(i=1, \ldots, n)$ which are faithfully and primitively permuted by $G / N$. Suppose further that $H:=N_{G}\left(W_{1}\right)$ has exactly one nontrivial orbit on $W_{1}$. Surely $n=p^{m}$ for some prime $p$ and an integer $n$. Then

$$
m_{r^{\prime}}(G, V) \geqslant\left\lceil\frac{\sqrt{m}}{224}\right\rceil
$$

Proof. The idea is to proceed exactly as in the proof of [8, Theorem 3.20] and adjust it whenever it does not yield the wanted conclusion. We will see that there is only one situation where such an adjustment is needed. The first part of the proof of [8, Theorem 3.20] shows that we may assume that ( $E, V, N, M, p^{m}$ ) is a special pair, where $M=Z(F(N))$. Put $k=d(M)$.

Assume that $k>\frac{m^{2}}{4} \log _{2} p$. In this case in [8] we show that there are at least $\frac{m}{20}$ orbits whose sizes have different $q$-parts for some $q||M|$. Hence $q \neq r$ and we are done in this case.

So we may assume that $k \leqslant \frac{m^{2}}{4} \log _{2} p$. This situation is subdivided into two cases:
Case 1: $p \times|M|$.
If each $v \in W_{1}$ is centralized by some Sylow $p$-subgroup of $H$, then [8, Lemma 3.14] yields $m-8$ orbits of $G$ on $V$ whose sizes have mutually distinct $p$-parts. So if $p \neq r$, we are done here. Therefore let $p=r$. This is exactly the situation where Theorem 2.6. is needed, and it yields the conclusion here.

So we may assume that not every $v \in W_{1}$ is centralized by some Sylow $p$-subgroup of $H$. Here we first consider the case that there are $p$-elements $\bar{x} \in H / C_{H}\left(W_{1}\right)-$ $N C_{H}\left(W_{1}\right) / C_{H}\left(W_{1}\right)$ that act fixed point freely on $W_{1}$. Then [8, Lemma 3.19] is involved which yields, with one exception for $p=3,\left\lceil\frac{\sqrt{m}}{224}\right\rceil$ elements of $V$ having mutually distinct $q$-parts for some prime $q||M|$. Thus $q \neq r$ and we are done here.

So now suppose that $N C_{H}\left(W_{1}\right) / C_{H}\left(W_{1}\right)$ contains all $p$-elements of $H / C_{H}\left(W_{1}\right)$ acting fixed point freely on $W_{1}$, or that we are in that one exception for $p=3$. Here in one instance $\frac{m}{2}$ orbits of sizes having mutually distinct $p$-parts are found using [8, Lemma 3.15], but note that by the table on [8, p. 88] we have $r \neq p$, so that we are done. In the remaining cases the orbits found have mutually distinct $q$-parts for some prime $q$ dividing $|M|$, so $q \neq r$ and we are done with Case 1 .

Case 2: $p||M|$.
Case 2a: The Sylow p-subgroup of $M$ satisfies Definition 2.5(*).
Then [8, Lemma 3.15] is used to establish the existence of $\frac{m}{2}$ orbits whose sizes have mutually distinct $p$-parts. But as $p||M|$, clearly $p \neq r$, and so we are done here.

Case 2b: The Sylow $p$-subgroup of $M$ does not satisfy Definition 2.5(*).
Here in one instance the wanted result is obtained by using what has already been established in Case 1, and in the remaining cases [8, Lemma 3.19] is involved, where $\left\lceil\frac{\sqrt{m}}{224}\right\rceil$ orbits are found having mutually distinct $q$-parts for some prime $q$ dividing $|M|$. Hence $q \neq r$, and the proof of the theorem is complete.

## 3. The main results

We now can prove our wanted generalization of the main result in [7].
3.1. Theorem. Let $G$ be a finite solvable group and let $V$ be a faithful and irreducible $G$-module over a finite field of characteristic $r$. Then

$$
\mathrm{dl}(G) \leqslant 24 \log _{2} m_{r^{\prime}}(G, V)+364
$$

Proof. We proceed exactly as in the proof of [7, Theorem 2.1]. Essentially this proof puts two results on orbit sizes together, namely [7, Theorem 1.5; 8, Theorem 4.5]. The first of these results bounds $\mathrm{dl}\left(\mathrm{O}_{q}(G)\right)$ (for some prime $q$ ) logarithmically in terms of the number $b(G, V)$ of $q$-parts of the orbit sizes of $G$ on $V$. So clearly $q \neq r$ and then $b(G, V) \leqslant m_{r^{\prime}}(G, V)$, and it remains to adjust the proof of [8, Theorem 4.5] to yield a bound on $m_{r^{\prime}}(G, V)$. All bounds on orbit sizes in that proof come directly from [8, Theorem 4.1]. Part (a) of that theorem distinguishes orbit sizes by their $q$-parts for a
prime $q$ such that $G$ has a normal $q$-subgroup of class 1 or 2 . Hence $q \neq r$, and we get a statement for $m_{r^{\prime}}(G, V)$ here. As to part (b) of [8, Theorem 4.1], it is proved that $m(G, V) \geqslant s_{1}$ and $m(G, V) \geqslant s_{2}$ for certain parameters $s_{1}$ and $s_{2}$. As to the first bound, this comes from orbit sizes having mutually distinct $q$-parts for some prime $q$ dividing an abelian normal subgroup of $G$, and so $q \neq r$, and we indeed have $m_{r^{\prime}}(G, V) \geqslant s_{1}$. As to the bound $m(G, V) \geqslant s_{2}$, this is obtained by using [8, Theorem 3.20]. So here we instead use our new result Theorem 2.7. and obtain $m_{r^{\prime}}(G, V) \geqslant s_{2}$. We are done.

We finally can prove the wanted result on conjugacy class sizes.
3.2. Corollary. Let $G$ be a finite solvable group. Then

$$
\mathrm{dl}(G / F(G)) \leqslant 24 \log _{2}|\operatorname{cs}(G)|+364
$$

Proof. Put $k=\mathrm{dl}(G / F(G))$ and $\bar{G}=G / F(G)$. It is well known that (additively written) we have $F(G) / \Phi(G)=\bigoplus_{i=1}^{t} V_{i}$ for some irreducible $G F\left(p_{i}\right) \bar{G}$ modules $V_{i}$ with suitable primes $p_{i}(i=1, \ldots, t)$ and that $\bar{G}$ acts faithfully on $F(G) / \Phi(G)$. Thus we may assume that $\bar{G}{ }^{(k-1)}$ acts nontrivially on $V_{1}$, so that with $G_{0}=\bar{G} / C_{\bar{G}}\left(V_{1}\right) \cong G / C_{G}\left(V_{1}\right)$ we have that $\mathrm{dl}\left(G_{0}\right)=k$, and $G_{0}$ acts faithfully and irreducibly on $V_{1}$. Let $r=p_{1}$. Then by Theorem 3.1. we have

$$
k=\mathrm{dl}\left(G_{0}\right) \leqslant 24 \log _{2} m_{r^{\prime}}\left(G_{0}, V_{1}\right)+364
$$

Now clearly $V_{1}$ is isomorphic to a $G_{0}$-submodule of $P / \Phi(P)$, where $P=O_{r}(G)$, and thus $m_{r^{\prime}}\left(G_{0}, V_{1}\right) \leqslant m_{r^{\prime}}\left(G_{0}, P / \Phi(P)\right)$, and as $F(G)$ acts trivially on $P / \Phi(P)$, we also have

$$
m_{r^{\prime}}\left(G_{0}, P / \Phi(P)\right)=m_{r^{\prime}}(G, P / \Phi(P))
$$

Now by Lemma 2.1 we have $m_{r^{\prime}}(G, P / \Phi(P)) \leqslant|\operatorname{cs}(G)|$, and so altogether we obtain

$$
\mathrm{dl}(G / F(G))=k \leqslant 24 \log _{2}|\operatorname{cs}(G)|+364
$$

as wanted.
3.3. Example. We finally show that the logarithmic bounds of Theorem A are asymptotically best possible. To see this, let $C_{3}$ and $C_{5}$ be the cyclic groups of order 3 and 5 (respectively), and for $n \in \mathbb{N}$ let $G_{n}$ be the iterated regular wreath product $C_{5} C_{3} C_{3} C_{5}$ 2 $C_{3} 2 \ldots 2 C_{5}$ 2 $C_{3}$ with $2 n$ factors. Then it is easy to see that $\left|G_{n}\right|_{3} \leqslant 3 \sum_{k=0}^{2 n-1} 5^{k} \leqslant 3^{5^{2 n}}$ and likewise $\left|G_{n}\right| 5 \leqslant 5^{5^{2 n}}$. Thus $\left|G_{n}\right|$ has at most $\left(5^{2 n}+1\right)^{2} \leqslant 5^{4 n+1}$ divisors, so that trivially $\left|\operatorname{cs}\left(G_{n}\right)\right| \leqslant 5^{4 n+1}$.

Furthermore clearly $h\left(G_{n}\right)=\mathrm{dl}\left(G_{n}\right)$, and $\mathrm{dl}\left(G_{n}\right)=2 n$ by [11, Proposition 3.10]. Then

$$
h\left(G_{n}\right)=\mathrm{dl}\left(G_{n}\right)=2 n=\frac{1}{2} \log _{5}\left(5^{4 n+1}\right)-\frac{1}{2} \geqslant \frac{1}{2} \log _{5}\left|\operatorname{cs}\left(G_{n}\right)\right|-\frac{1}{2}
$$

which shows that in general we cannot expect stronger than logarithmic bounds for $\mathrm{dl}(G)$ in terms of $|\operatorname{cs}(G)|$ in Theorem A.

## Acknowledgments

This work was initiated and done in part while I visited the University of the Basque Country (Spain) for three weeks during the summer of 2003. I would like to thank Alex Moretó for inspiring discussions on the subject of this paper, and Alex, Josu Sangróniz and Gustavo Fernández-Alcober as well as the mathematics department for their hospitality.

I also thank an anonymous referee for suggestions that improved the readability of the paper.

## References

[1] G.A. Fernández-Alcober, A. Moretó, On the number of conjugacy class sizes and character degrees in finite p-groups, Proc. Amer. Math. Soc. 129 (2001) 3201-3204.
[2] B. Huppert, Character Theory of Finite Groups, de Gruyter, Berlin, 1998.
[3] B. Huppert, Endliche Gruppen I, Springer, Berlin-Heidelberg-New York, 1967.
[4] I.M. Isaacs, The number of generators of a linear p-group, Canad. J. Math. 24 (1972) 851-858.
[5] K. Ishikawa, On finite p-groups which have only two conjugacy lengths, Israel J. Math. 129 (2002) 119-123.
[6] T.M. Keller, Orbits in finite group actions, Proceedings of Groups St. Andrews 2001 in Oxford, London Mathematical Society Lecture Notes Series, vol. 305, 2003, pp. 306-331.
[7] T.M. Keller, Orbit sizes and character degrees, III, J. Reine Angew. Math. 545 (2002) 1-17.
[8] T.M. Keller, Orbit sizes and character degrees, II, J. Reine Angew. Math. 516 (1999) 27-114.
[9] T.M. Keller, Orbit sizes and character degrees, Pacific J. Math. 187 (1999) 317-332.
[10] A. Mann, Some questions about p-groups, J. Austral. Math. Soc. (Series A) 67 (1999) 356-379.
[11] O. Manz, T.R. Wolf, Representations of solvable groups, London Mathematical Society Lecture Notes Series, vol. 185, Cambridge University Press, Cambridge, 1993.


[^0]:    E-mail address: keller@txstate.edu.

    0001-8708/\$ - see front matter © 2004 Elsevier Inc. All rights reserved.
    doi:10.1016/j.aim.2004.11.002

