Canad. Math. Bull. Vol. **49** (2), 2006 pp. 285–295

Orbits and Stabilizers for Solvable Linear Groups

Jeffrey M. Riedl

Abstract. We extend a result of Noritzsch, which describes the orbit sizes in the action of a Frobenius group G on a finite vector space V under certain conditions, to a more general class of finite solvable groups G. This result has applications in computing irreducible character degrees of finite groups. Another application, proved here, is a result concerning the structure of certain groups with few complex irreducible character degrees.

1 Introduction

In studying connections between the structure of a finite solvable group G and the set $\mathrm{cd}(G)$ consisting of the degrees of its ordinary irreducible characters, it is often useful to be able to describe the set of orbit sizes in the action of some relatively small quotient of G on an elementary abelian p-group. (Typically, this p-group is the group of linear characters of some chief factor of G.) A result of this type that has proved to be valuable is the following [4, Lemma 1.10], due to Noritzsch.

Theorem 1.1 (Noritzsch) *Let G be a Frobenius group with abelian Frobenius kernel G'. Suppose that G acts on an elementary abelian p-group V (for some prime p) and that the action of G' on V is Frobenius. Let $\mathcal{S}$ be the set of sizes of the G-orbits on the nonidentity elements of V. Then $\mathcal{S} \cup \{|G|\}$ is the set of all numbers of the form $|G|/k$, where k runs over the divisors of $|G:G'|$.*

Noritzsch's argument in [4] actually proves more, namely, that if $K > 1$ is any subgroup of G such that $K \cap G' = 1$, then K is the stabilizer in G of some element of V.

The conclusion of Noritzsch's theorem is stated in a way that avoids the question of whether or not $\mathcal{S}$ contains $|G|$. Examples show that both alternatives are possible.

The condition that G is a Frobenius group with abelian kernel G' is, of course, very restrictive, and there are situations where it would be convenient to be able to relax this condition somewhat. We will say that G is a $(*)$-group if G' is abelian and the action of $G/G'\mathbf{Z}(G)$ on G' is Frobenius. In particular, if G is a nontrivial $(*)$-group and $\mathbf{Z}(G) = 1$, then G is a Frobenius group with kernel G', as in Noritzsch's theorem.

Before stating our first theorem, which describes the stabilizer subgroups and orbit sizes for certain actions of $(*)$-groups on elementary abelian p-groups, we need the following lemma:

Received by the editors June 7, 2004.
AMS subject classification: 20B99, 20C15, 20C20.

https://doi.org/10.4153/CMB-2006-030-1 Published online by Cambridge University Press

Lemma 1.2 *Let G be a $(*)$-group and write $F = G'\mathbf{Z}(G)$. Then there is a unique subgroup M that contains F and is maximal with the property that M splits over F.*

Note that in the case of Noritzsch's theorem, where $F = G'$, we have $M = G$.

Theorem 1.3 *Let G be a $(*)$-group and let F and M be as in Lemma* 1.2. *Suppose that G acts on an elementary abelian p-group V and that the action of F on V is Frobenius. Let $\mathcal{S}$ be the set of sizes of the G-orbits on the nonidentity elements of V. Then*

(i) *a nonidentity subgroup K of G is the stabilizer of some nonidentity element of V if and only if $K \cap F = 1$, and*

(ii) *$\mathcal{S} \cup \{|G|\}$ is the set of numbers $|G|/k$, where k runs over the divisors of $|M{:}F|$.*

The conclusion of Theorem 1.3 is the same as that of Theorem 1.1, but for our more general hypothesis. In Theorem 1.3(i), the necessity of the condition $K \cap F = 1$ for K to be a stabilizer subgroup is immediate from the fact that the action of F on V is Frobenius. The fact that this same condition is sufficent, however, is less obvious.

We now present an example that illustrates not only that the generality of Theorem 1.3 is actually needed in certain cases, but also the inherent obstacle to proving Theorem 1.3 by simply applying Theorem 1.1 to some carefully-chosen Frobenius subgroup of G.

Example Let $A = \langle \sigma \rangle$ be the Galois group of the extension $\mathrm{GF}(7) \subseteq \mathrm{GF}(7^{12})$ of finite fields, where $\sigma\colon x \mapsto x^7$ for all $x \in \mathrm{GF}(7^{12})$. The semi-linear group $\mathrm{GF}(7^{12})^\times \rtimes A$ acts on the additive group $V = \mathrm{GF}(7^{12})$. We now construct a subgroup G to act on V.

Fix a generator y for the cyclic subgroup of order 9 in the multiplicative group $\mathrm{GF}(7^3)^\times$. Write $w = \sigma^4 y$ and $S = \langle w \rangle$. By [5, Lemma 6], $w^3 = y^m$, where $m = (7^{12} - 1)/(7^4 - 1)$ has 3-part equal to 3, and so the element w has order 9. Also, $C = \langle y^m \rangle$ is the subgroup of order 3 in $\mathrm{GF}(7)^\times$. The group $B = \langle \sigma^3 \rangle$ of order 4 centralizes S.

Let P and Q be the subgroups of orders 13 and 2, respectively, in $\mathrm{GF}(7^{12})^\times$. As 13 divides neither $7^6 - 1$ nor $7^4 - 1$, the action of SB/C on P is Frobenius. Let $G = PQSB$, and note that $G' = P$ and $\mathbf{Z}(G) = QC$. The action of $F = G'\mathbf{Z}(G)$ on V is Frobenius, since $F \subseteq \mathrm{GF}(7^{12})^\times$. As $F \cap B = 1$, the group FB splits over F. Note that $|G{:}FB| = 3$, while $|FB{:}F| = 4$. Since Sylow 3-subgroups of G are cyclic of order 9, no subgroup of G having order divisible by 9 splits over F. Thus, in the notation of Lemma 1.2, $M = FB$. We may apply Theorem 1.3, with $|M{:}F| = 4$, to deduce $\mathcal{S} \cup \{|G|\} = \{|G|, |G|/2, |G|/4\}$.

Now suppose we want to show that the subgroup $K = \langle \sigma^6 \rangle$ of order 2 in B is the stabilizer in G of some nonidentity element of V. There is a cyclic subgroup L of order 4, distinct from B, such that $K < L \subseteq B \dot{\times} Q$. The distinct groups $G'B$ and $G'L$ are maximal as Frobenius subgroups of G. Applying Theroem 1.1 to the action of $G'B$ on V yields that $K = \mathbf{C}_{G'B}(v)$ for some nonidentity element $v \in V$. But since $K = G'B \cap L$, one cannot rule out the possibility here that $\mathbf{C}_G(v)$ includes the entire subgroup L.

Corollary 1.4 *In the situation of Theorem* 1.3*, the action of G on V is Frobenius if and only if $M = F$.*

Corollary 1.4 follows immediately from Theorem 1.3. For a wealth of examples in which the action of G on V actually is Frobenius, we refer the reader to [5, Theorem 11].

If G is a finite solvable group, we denote its *Fitting subgroup* by $\mathbf{F}(G)$ and its *Fitting series* (see [5] for definition) by $1 = \mathbf{F}_0(G) < \mathbf{F}_1(G) < \cdots < \mathbf{F}_{h-1}(G) < \mathbf{F}_h(G) = G$, where $h = \mathrm{h}(G)$ is the *Fitting height* of G, a number which in some sense measures how far the group G is from being nilpotent. We use Theorem 1.3 to prove the following result, which gives structural information about certain solvable groups with few character degrees.

Theorem 1.5 *Let G be a solvable group and write $F_i = \mathbf{F}_i(G)$ for $i \in \{1, 2\}$. Suppose that $\mathrm{h}(G) = 3$ and $|\mathrm{cd}(G/F_1)| = 2$ and $|\mathrm{cd}(G)| \leq 4$. Then there exists a chief factor F_1/M of G such that $G/\mathbf{C}_G(F_1/M)$ is nonnilpotent while $|F_1 : M|$ is relatively prime to $|F_2 : F_1|$.*

Theorem 1.5 plays a crucial role in the proof of the main result of [6], which says that if G is any solvable group such that $|G : \mathbf{F}(G)|$ is odd and $|\mathrm{cd}(G)| \leq 5$, then $\mathrm{h}(G) \leq 3$.

Finally, to show the hypothesis $|\mathrm{cd}(G)| \leq 4$ in Theorem 1.5 is truly needed, we present examples of a solvable groups G satisfying $\mathrm{h}(G) = 3$, $|\mathrm{cd}(G/F_1)| = 2$, and $|\mathrm{cd}(G)| = 5$, but having no chief factor of the form F_1/M for which $|F_1 : M|$ is relatively prime to $|F_2 : F_1|$.

2 Proofs

Before proving Lemma 1.2, we need the following.

Lemma 2.1 *Let $K \subseteq N$ be normal subgroups of a group G, and suppose that $|K|$ is relatively prime to $|G : N|$. If G/K splits over N/K, then G splits over N.*

Proof Let H/K be a complement for N/K in G/K. By the Schur–Zassenhaus theorem, there is a complement L for K in H. Observe that L is a complement for N in G. ■

Proof of Lemma 1.2 Write π to denote the set of all prime divisors of $|G : F|$. For each prime $p \in \pi$, choose a p-subgroup L_p of G, of maximal order with the property that $L_p \cap F = 1$. Since $G' \subseteq F$, we have $L_p \cap G' = 1$. Let L/G' be the direct product of the subgroups L_pG'/G' (for $p \in \pi$) of G/G'. Let $M = FL$, and note that L/G' is a complement for F/G' in M/G'. As the action of G/F on G' is Frobenius, we see that $|M : F|$ and $|G'|$ are relatively prime. Now Lemma 2.1 implies that M splits over F.

Let H be any subgroup of G that contains F. If $H \subseteq M$, then H clearly splits over F. Now assume instead that H splits over F. Because G/F is cyclic, showing that $|H/F|$ divides $|M/F|$ is sufficient for proving that $H \subseteq M$. For $p \in \pi$, let S_p be a

https://doi.org/10.4153/CMB-2006-030-1 Published online by Cambridge University Press

Sylow p-subgroup of any complement for F in H. Using the maximality of L_p, we deduce that $|H/F|_p = |S_p| \leq |L_p| = |M/F|_p$, and so $H \subseteq M$. ■

Our proof of Theorem 1.3 is a careful adaptation of Noritzsch's proof of Theorem 1.1. For this we need the following elementary number-theoretic lemmas.

Lemma 2.2 *Let $q > 1$ and $p > 1$ and $k > 1$ be integers. Then both qk and q^2 are smaller than $(p^{kq} - 1)/(p^k - 1)$.*

Proof Write $m = 2^k + \cdots + 2^{(q-1)k}$, and note that $(p^{kq} - 1)/(p^k - 1) = 1 + p^k + \cdots + p^{(q-1)k} > m$. We now show that $qk \leq m$ and $q^2 \leq m$. Since $k \geq 2$, we have $2k \leq 2^k$. As $q \geq 2$, we have $q \leq 2(q-1)$. Combining these, $qk \leq (q-1)2k \leq (q-1)2^k \leq m$. Since $k \geq 2$, we have $4^{q-1} \leq 2^{(q-1)k} \leq m$. The reader may verify that $q^2 \leq 4^{q-1}$ for $q \geq 2$. ■

Lemma 2.3 *Let $p > 1$ be an integer and let $q_1 < q_2 < \cdots < q_t$ be primes. Write $f = q_1 \cdots q_t$ and write $f_i = f/q_i$ for $1 \leq i \leq t$. Then*

$$\sum_{i=1}^{t} q_i(p^{f_i} - 1) < p^f - 1.$$

Proof The case $t = 1$ is clear, since $q < 1 + p + \cdots + p^{q-1} = (p^q - 1)/(p - 1)$.

Now suppose $t > 1$. It suffices to show that each of the t summands is smaller than $(p^f - 1)/t$, or equivalently, that $q_i t$ is smaller than $n = (p^{f_i q_i} - 1)/(p^{f_i} - 1)$. Since $t \leq q_t$, it is enough to prove that $q_i q_t < n$. In case $i < t$, then q_t divides f_i, and Lemma 2.2 implies that $n > q_i f_i \geq q_i q_t$, as desired. In case $i = t$, Lemma 2.2 yields $n > {q_i}^2 = q_i q_t$. ■

Proof of Theorem 1.3 (i) Let C be a (cyclic) complement for F in M, and let π be the set of all prime divisors of $|M{:}F|$. Note that $M = G'C \dot{\times} \mathbf{Z}(G)$, while $G'C$ is a Frobenius group. Write $Z_\pi = \mathbf{O}_\pi(\mathbf{Z}(M))$. The Hall π-subgroups of M are all of the form $C^x \dot{\times} Z_\pi$ for $x \in G'$. The intersection of any two distinct Hall π-subgroups of M is Z_π.

Let $K > 1$ be any subgroup of G such that $K \cap F = 1$. We want to show K is the stabilizer in G of some nonidentity element in V. Since K is a cyclic π-subgroup of M, there exists a Hall π-subgroup H of M that contains K, and we may assume $H = C \dot{\times} Z_\pi$. Since $K \nsubseteq Z_\pi$, indeed H is the unique Hall π-subgroup of M that contains K.

Let $\mathcal{C}(K)$ denote the family of all subgroups $L \subseteq G$ such that $L \cap F = 1$ and $K < L$ with $|L{:}K|$ being prime. If $L \in \mathcal{C}(K)$, then L is a π-subgroup of M, and so $|L{:}K| \in \pi$, and indeed $L \subseteq H$. For each prime $q \in \pi$, let $\mathcal{C}_q(K)$ be the set of all subgroups $L \in \mathcal{C}(K)$ satisfying $|L{:}K| = q$. Note that $\mathcal{C}(K) = \bigcup \mathcal{C}_q(K)$, where this union runs over $q \in \pi$.

Now fix any prime $q \in \pi$, and note that the groups $C_q \in \mathrm{Syl}_q(C)$ and $Z_q \in \mathrm{Syl}_q(Z_\pi)$ are both cyclic. Thus the Sylow q-subgroup of the abelian group $H =$

$C \dot{\times} Z_\pi$ is $C_q \dot{\times} Z_q$, which has rank at most 2. As K is cyclic, write $K = Q \dot{\times} D$ where Q is a q-group and D is a q'-group. Since $K \subseteq H$, we have $Q \subseteq C_q \dot{\times} Z_q$ with $Q \cap Z_q = 1$. Every member of $\mathcal{C}_q(K)$ is a subgroup of H, and so $\mathcal{C}_q(K)$ consists of all subgroups of the form $Q_1 \dot{\times} D$, where Q_1 satisfies $Q < Q_1 \subseteq C_q \dot{\times} Z_q$ and $|Q_1 : Q| = q$ and $Q_1 \cap Z_q = 1$. But there are at most only q distinct subgroups Q_1 that satisfy these properties. Therefore $|\mathcal{C}_q(K)| \leq q$.

Assuming that K is not equal to the stabilizer in G of any element of $V^\# = V - \{0\}$, for each $v \in \mathbf{C}_{V^\#}(K)$ we have $\mathbf{C}_G(v) \supseteq L$ for some subgroup $L \in \mathcal{C}(K)$. Write $\pi = \{q_1, \dots, q_t\}$. For convenience, write $\mathcal{D}_i$ to denote the set $\mathcal{C}_q(K)$ for $q = q_i$. We then have

$$\mathbf{C}_{V^\#}(K) \subseteq \bigcup_{i=1}^{t} \Big(\bigcup_{L \in \mathcal{D}_i} \mathbf{C}_{V^\#}(L) \Big).$$

Write $|V| = p^n$ and $f = q_1 \cdots q_t$ and $k = n/(|K| f)$. Now [2, Theorem 15.16], implies that $|\mathbf{C}_{V^\#}(K)| = p^{kf} - 1$. For $1 \leq i \leq t$, write $f_i = f/q_i$, and note that each subgroup $L \in \mathcal{D}_i$ satisfies $|\mathbf{C}_{V^\#}(L)| = p^{kf_i} - 1$, again by [2, Theorem 15.16]. Now using the fact that $|\mathcal{D}_i| \leq q_i$ for $1 \leq i \leq t$, we obtain

$$p^{kf} - 1 = |\mathbf{C}_{V^\#}(K)| \leq \sum_{i=1}^{t} \Big(\sum_{L \in \mathcal{D}_i} |\mathbf{C}_{V^\#}(L)| \Big) \leq \sum_{i=1}^{t} q_i (p^{kf_i} - 1),$$

which contradicts Lemma 2.3. Therefore $K = \mathbf{C}_G(v)$ for some element $v \in V^\#$.

(ii) The set $\mathcal{S}$ consists of the numbers $|G|/|\mathbf{C}_G(v)|$ for all nonidentity elements $v \in V$. As $F\mathbf{C}_G(v)$ clearly splits over F, we have $F\mathbf{C}_G(v) \subseteq M$, and so $|\mathbf{C}_G(v)|$ divides $|M : F|$. This proves that $\mathcal{S} \cup \{|G|\} \subseteq \{|G|/k \mid k \text{ divides } |M : F|\}$. For the reverse inclusion, let C be a complement for F in M. For any divisor $k > 1$ of $|M : F|$, let K be the subgroup of order k in the cyclic group C. As $K \cap F = 1$, statement (i) above implies that $K = \mathbf{C}_G(v)$ for some nonidentity element $v \in V$. The G-orbit containing v has size $|G|/k$. ■

Following standard notation, we denote by $\mathrm{Irr}(G)$ the set of ordinary irreducible characters of a group G. Our proof of Theorem 1.5 uses the following result [4, Lemma 1.6].

Lemma 2.4 *If G is a nonnilpotent group with $\mathrm{cd}(G) = \{1, a\}$, then the following hold.*

(i) *$\mathbf{F}(G)$ is abelian, and $G/\mathbf{F}(G)$ is cyclic of order a.*
(ii) *There exists $N \lhd G$ such that G/N is a Frobenius group whose kernel is $\mathbf{F}(G)/N$, an elementary abelian q-group for some prime q.*
(iii) *If all Sylow subgroups of G are abelian, then $\mathbf{F}(G) = G' \dot{\times} \mathbf{Z}(G)$, and the action of $G/\mathbf{F}(G)$ on G' is Frobenius.*
(iv) *If a Sylow p-subgroup of G is nonabelian, then $a = p$.*

If N is a normal subgroup of a group G and $\varphi \in \mathrm{Irr}(N)$ is an irreducible character, we write $\mathbf{I}_G(\varphi)$ to denote the inertia subgroup of φ in G, which is the stabilizer of φ in the natural action of G on the set $\mathrm{Irr}(N)$. Let $\Phi(G)$ denote the Frattini subgroup of G.

Proof of Theorem 1.5 Let G be a minimal counterexample and write $\mathrm{cd}(G/F_1) = \{1, a\}$. As G/F_1 is nonnilpotent, Lemma 2.4 implies that F_2/F_1 is abelian, G/F_2 is cyclic of order a, and there exists $N/F_1 \lhd G/F_1$ such that G/N is a Frobenius group whose kernel is F_2/N, an elementary abelian q-group for some prime q. Thus F_2 is a group whose Fitting factor group F_2/F_1 is abelian, and so [1, Lemma 1.1] yields $|F_2{:}F_1| \in \mathrm{cd}(F_2)$. Hence $|F_2{:}F_1|$ divides some degree $b \in \mathrm{cd}(G)$. The prime q divides b but does not divide a, and so $b \neq a$.

If $S \lhd G$ is any normal subgroup such that $\mathbf{F}(G/S) = F_1/S$, then G/S inherits our hypotheses on G. If $S > 1$, then by minimality we obtain a chief factor F_1/K of G (with $S \subseteq K$) having all the properties stated in the conclusion, which would contradict that G is a counterexample. Hence $S = 1$ in this situation.

The preceding paragraph implies that $\Phi(G) = 1$ and $\mathbf{Z}(F_2) = 1$. By [1, III.4.5], we may write $F_1 = M_1 \dot{\times} \cdots \dot{\times} M_n$ where each M_i is an elementary abelian minimal normal subgroup of G. By [1, III.4.4], each subgroup M_i has a complement in G, and it follows by a routine argument that each character $\lambda \in \mathrm{Irr}(M_i)$ extends to its inertia subgroup $\mathbf{I}_G(\lambda)$.

For $1 \leq i \leq n$, let r_i be the unique prime divisor of $|M_i|$, and write $C_i = \mathbf{C}_G(M_i)$. Since $\mathbf{Z}(F_2) = 1$, we have $|F_2{:}C_i \cap F_2| > 1$. Note that $F_1 \subseteq C_i$, and so $F_1 \subseteq C_i \cap F_2 \subseteq F_2$, which says $F_2/(C_i \cap F_2)$ is abelian. As M_i is a faithful, completely reducible $F_2/(C_i \cap F_2)$-module in characteristic r_i, the prime r_i cannot divide $|F_2{:}C_i \cap F_2|$. Thus the faithful action of $F_2/(C_i \cap F_2)$ on $\mathrm{Irr}(M_i)$ has a regular orbit, by coprimeness, and so there exists $\lambda \in \mathrm{Irr}(M_i)$ such that $\mathbf{I}_{F_2}(\lambda) = C_i \cap F_2$. By the preceding paragraph, λ has an extension $\mu \in \mathrm{Irr}(C_i \cap F_2)$. Thus $\mu^{F_2} \in \mathrm{Irr}(F_2)$, and so in particular $|F_2{:}C_i \cap F_2| \in \mathrm{cd}(F_2)$.

For some integer m with $0 \leq m \leq n$, we may assume that G/C_i is nonnilpotent if and only if $i \leq m$. Since each M_i is G-isomorphic to a chief factor of G of the form F_1/K, the fact that G is a counterexample implies that r_i divides $|F_2{:}F_1|$ in case $i \leq m$. Let $D = \bigcap C_i$ for $i > m$. Note that $F_1 \subseteq D \subseteq G$ and that G/D is nilpotent. In view of the Frobenius group G/N mentioned in the first paragraph, we see that q divides $|D{:}F_1|$. Since $F_1 = \mathbf{C}_G(F_1) = \bigcap_{i=1}^{n} C_i$, we have $m \geq 1$, and we may assume that G/C_1 is nonnilpotent and has order divisible by q. Since q does not divide $|G{:}F_2|$, the prime q divides $|F_2{:}C_1|$. It follows that r_1 divides $|F_2{:}F_1|$.

Step 1: Every prime divisor of $|F_2{:}F_1|$ divides $|F_2{:}C_i \cap F_2|$ for some $1 \leq i \leq n$.

This follows from the fact that $F_1 = \bigcap_1^n C_i$.

Step 2: If $i \in \{1, \dots, n\}$ and H is a subgroup with $F_2 \subseteq H \subseteq G$, then H does not have a normal r_i-complement, and r_i fails to divide at least one member of $\mathrm{cd}(H) - \{1\}$.

If H has a normal r_i-complement, then F_2 has a normal r_i-complement L. The normal subgroups L and M_i of relatively prime orders must centralize each other,

https://doi.org/10.4153/CMB-2006-030-1 Published online by Cambridge University Press

and so $L \subseteq C_i \cap F_2 \subseteq F_2$. But recall that r_i fails to divide $|F_2 : F_2 \cap C_i| > 1$. Since $|F_2 : L|$ is a power of r_i, this is a contradiction. Now apply [2, Corollary 12.2] for the remainder of the statement.

Step 3:

(i) Each irreducible character of G of degree a restricts to the subgroup F_2 as a sum of linear characters.
(ii) None of the primes $r_1, \dots, r_n$ divides every degree in $\mathrm{cd}(G) - \{1, a\}$.

We show first that q divides every member of $\mathrm{cd}(F_2) - \{1\}$. Suppose instead that q fails to divide some degree $m \in \mathrm{cd}(F_2) - \{1\}$. Using the Frobenius group G/N and [2, Theorem 12.4], we deduce $am = |G : F_2| \cdot m \in \mathrm{cd}(G)$. Thus $\mathrm{cd}(G) = \{1, a, am, b\}$, and so b is the only member of $\mathrm{cd}(G)$ divisible by q. Write $c = |F_2 : F_2 \cap C_1|$, and recall that q divides $c \in \mathrm{cd}(F_2)$. Hence each character in $\mathrm{Irr}(G)$ lying over any character of degree c in $\mathrm{Irr}(F_2)$ has degree b. By [2, Corollary 11.29], we know that b/c divides $|G : F_2| = a$, and it follows that b divides ac. Recall that r_1 divides $|F_2 : F_1|$, which divides b. Hence r_1 divides $b = ac$, but we know that r_1 does not divide $|F_2 : F_2 \cap C_1| = c$. Thus r_1 divides a, and so r_1 divides every member of $\{a, am, b\} = \mathrm{cd}(G) - \{1\}$, thereby contradicting Step 2.

(i) Since q does not divide a, this follows from the preceding paragraph.
(ii) Suppose r_i divides every degree in $\mathrm{cd}(G) - \{1, a\}$. By Step 2, we see that r_i does not divide $a = |G : F_2|$. Let $\theta \in \mathrm{Irr}(F_2)$ with $\theta(1) > 1$, and choose $\psi \in \mathrm{Irr}(G|\theta)$. By part (i) we have $\psi(1) \in \mathrm{cd}(G) - \{1, a\}$, and so r_i divides $\psi(1)$. By [2, Corollary 11.29], $\psi(1)/\theta(1)$ divides $|G : F_2| = a$. As r_i does not divide a, it must divide $\theta(1)$. Hence r_i divides every member of $\mathrm{cd}(F_2) - \{1\}$, and this contradicts Step 2, now with $H = F_2$.

Step 4: For $1 \le i \le n$, if $|F_2 : C_i \cap F_2|$ and $|F_1|$ are not relatively prime, then

(i) $F_1 \subseteq C_i \subseteq F_2$ and $\mathbf{F}(G/C_i) = F_2/C_i$ and $\mathrm{cd}(G/C_i) = \{1, a\}$, and
(ii) the r_i-part of b is nontrivial and divides a, and r_i divides $|F_2 : F_1|$.

(i) Write $c = |F_2 : C_i \cap F_2|$, and let r be a prime dividing both c and $|F_1|$. Since c divides $|F_2 : F_1|$, which divides b, indeed r divides b. Thus, since $|\mathrm{cd}(G)| \le 4$, Step 3(ii) implies that b is the only member of $\mathrm{cd}(G) - \{1, a\}$ divisible by r. As r divides $c \in \mathrm{cd}(F_2)$, Step 3(i) implies that every character in $\mathrm{Irr}(G)$ lying over some character of degree c in $\mathrm{Irr}(F_2)$ must have degree b. Now by [2, Corollary 11.29] we know that b/c divides $|G : F_2| = a$, and it follows that b divides ac.

Since the full q-part of $|F_2 : F_1|$ divides b, while q does not divide a, we now see that the full q-part of $|F_2 : F_1|$ actually divides $c = |F_2 : C_i \cap F_2|$. This forces $F_2 \cap C_i \subseteq N \subseteq G$, and so in particular G/C_i is nonnilpotent. As $F_1 \subseteq C_i \subseteq G$ and $\mathrm{cd}(G/F_1) = \{1, a\}$, we deduce that $\mathrm{cd}(G/C_i) = \{1, a\}$. Now [1, Lemma 1.1] yields $1 < |G/C_i : \mathbf{F}(G/C_i)| \in \mathrm{cd}(G/C_i) = \{1, a\}$. Since $C_i F_2/C_i \subseteq \mathbf{F}(G/C_i)$, it follows that $\mathbf{F}(G/C_i) = F_2/C_i$.

(ii) As G/C_i is nonnilpotent and G is a counterexample, r_i must divide $|F_2 : F_1|$, which divides b. Recall that b divides ac, while r_i does not divide $|F_2 : F_2 \cap C_i| = c$.

Step 5: The contradiction.

As r_1 divides $|F_2{:}F_1|$, Step 1 asserts that r_1 divides $|F_2{:}C_i \cap F_2|$ for some index i. Clearly $i \neq 1$. By Step 4(i), G/C_i is nonnilpotent. Hence $i \leq m$ and we may assume $i = 2$. By Step 4(ii), the r_2-part of b is nontrivial and divides a, and r_2 divides $|F_2{:}F_1|$.

By Step 1 now, r_2 divides $|F_2{:}C_j \cap F_2|$ for some index j. Clearly $j \neq 2$. For brevity, write $r = r_j$ and $C = C_j$ and $M = M_j$. Write $X = G/C$. By Step 4 we see that $\mathbf{F}(X) = F_2/C$ and $\mathrm{cd}(X) = \{1, a\}$, while r divides a. Since r_2 and r are distinct prime divisors of a, Lemma 2.4(iv) asserts that all Sylow subgroups of X are abelian. Now the rest of Lemma 2.4 implies that $\mathbf{F}(X) = X' \dot{\times} \mathbf{Z}(X)$ is abelian, and that the action of $X/\mathbf{F}(X)$ on X' is Frobenius. In particular, X is a $(*)$-group.

Since r_2 divides the order a of the Frobenius complement $X/\mathbf{F}(X)$, we know r_2 does not divide the order of the Frobenius kernel X'. From the preceding paragraph, we know that r_2 divides $|F_2{:}C|$, which is the order of $\mathbf{F}(X)$. Hence r_2 divides the order of $\mathbf{Z}(X)$, and so in particular $\mathbf{Z}(X) > 1$. The action of X on $V = \mathrm{Irr}(M)$ is faithful and irreducible. It follows that the action of $\mathbf{Z}(X)$ on V is Frobenius, and hence $\mathbf{Z}(X)$ is cyclic.

We claim that the action of $\mathbf{F}(X)$ on V is Frobenius. Since V is irreducible as an X-module, it suffices to show that $\mathbf{F}(X)$ is cyclic. Let p be any prime dividing the order of X'. It suffices to show that the abelian group $\mathbf{O}_p(X)$ is cyclic. Write $P/C = \mathbf{O}_p(X)$ and suppose P/C is noncyclic. By [5, Lemma 2.6], there are characters $\lambda_1, \lambda_2 \in V$ such that $C \subseteq \mathbf{I}_P(\lambda_1) < \mathbf{I}_P(\lambda_2) < P$. Since λ_1 and λ_2 extend to their inertia subgroups and since the action of $\mathbf{Z}(X)$ on V is Frobenius, we get degrees c_1 and c_2 in $\mathrm{cd}(F_2)$ having distinct nontrivial p-parts and which are divisible by $|\mathbf{Z}(X)|$, and hence by r_2. Since p does not divide $|G{:}F_2|$, there are degrees d_1 and d_2 in $\mathrm{cd}(G)$, lying over c_1 and c_2 respectively, whose p-parts equal those of c_1 and c_2. It follows that $\mathrm{cd}(G) - \{1, a\} = \{d_1, d_2\}$. But r_2 divides d_1 and d_2, contradicting Step 3(ii). Hence the action of $\mathbf{F}(X)$ on V is Frobenius.

Recall that r does not divide the order of $F_2/C = \mathbf{F}(X)$ but does divide $a = |X{:}\mathbf{F}(X)|$. Thus X has a nontrivial Sylow r-subgroup whose intersection with $\mathbf{F}(X)$ is trivial. By Theorem 1.3 (taking $k = r$), there is a character $\lambda \in V$ such that $|G{:}\mathbf{I}_G(\lambda)| = |G{:}C|/r$. Since λ extends to its inertia subgroup, we obtain the degree $d = |G{:}C|/r$ in $\mathrm{cd}(G)$. We mentioned earlier that the r_2-part of the degree b is nontrivial and divides $a = |G{:}F_2|$. Since r_2 also divides $|F_2{:}C|$ however, the r_2-part of $|G{:}C|/r = d$ is larger than the r_2-part of b. In particular, $d \neq b$. To see that $d \neq a$, pick any prime divisor p of the order of X', and note that p divides $|G{:}C|/r = d$ but does not divide a. Therefore $\mathrm{cd}(G) - \{1, a\} = \{b, d\}$, which again contradicts Step 3(ii). The proof of Theorem 1.5 is now complete. ■

3 Examples

As promised at the end of the introduction, we now present a family of examples of finite solvable groups G such that if we let F_1 and F_2 denote the first two members of its Fitting series, G satisfies $\mathrm{h}(G) = 3$, $|\mathrm{cd}(G/F_1)| = 2$ and $|\mathrm{cd}(G)| = 5$, and yet G has no chief factor of the form F_1/M for which $|F_1{:}M|$ is relatively prime to $|F_2{:}F_1|$. This will show that the hypothesis $|\mathrm{cd}(G)| \leq 4$ in Theorem 1.5 is truly needed.

If N is a normal subgroup of a group G, we denote by $\mathrm{cd}(G|N)$ the set of degrees of the characters in the set $\mathrm{Irr}(G|N) = \{\chi \in \mathrm{Irr}(G) \mid N \nsubseteq \ker(\chi)\}$. Note that $\mathrm{Irr}(G) = \mathrm{Irr}(G/N) \cup \mathrm{Irr}(G|N)$ is a disjoint union, while $\mathrm{cd}(G) = \mathrm{cd}(G/N) \cup \mathrm{cd}(G|N)$ is not necessarily disjoint. For any given character $\theta \in \mathrm{Irr}(N)$, we denote by $\mathrm{cd}(G|\theta)$ the set of degrees of the characters in the set $\mathrm{Irr}(G|\theta) = \{\psi \in \mathrm{Irr}(G) \mid [\psi_N, \theta] \neq 0\}$.

For any given prime q and any positive integer n, it is standard terminology to say that a prime p is a *Zsigmondy prime* for $q^n - 1$ in case p divides $q^n - 1$ while p fails to divide $q^m - 1$ for every integer $1 \leq m < n$. For any given pair of distinct primes q and p, we introduce the notation $f(q,p)$ to denote the multiplicative order of the element q in the ring $\mathbb{Z}/p\mathbb{Z}$. Thus $f = f(q,p)$ is the smallest positive integer such that p divides $q^f - 1$. In particular, $f(q,p)$ is a divisor of $p-1$, and p is a Zsigmondy prime for $q^f - 1$.

We shall say that (p,r,s) is a $(*)$-*triple* if p, r, and s are distinct primes such that $f(r,p)/r$ is an integer divisible by $f(r,s)$, while $f(s,p)/r$ is an integer divisible by $f(s,r)$. Below we shall construct a finite solvable group corresponding to any given $(*)$-triple.

In a $(*)$-triple, r divides $f(r,p)$, which divides $p-1$, and so we deduce that r divides $p-1$. Further, since $f(r,s)$ divides $m = f(r,p)/r$, we see that s divides $r^m - 1$. These observations clearly suggest a method which, for any given prime p, generates all possible candidates for the primes r and s in a $(*)$-triple. Using this method, we find that the only $(*)$-triples for which $p \leq 17$ are $(5,2,3)$, $(13,2,7)$, $(13,3,2)$, $(17,2,3)$, $(17,2,5)$.

Construction Let (p,r,s) be a $(*)$-triple and write $q = r^{f(r,p)/r}$. Choose any positive integer h that divides $q^r - 1$ and that is divisible by both $c = (q^r - 1)/(q-1)$ and s. We construct a finite solvable group G that has the following properties.

(i) $\mathrm{h}(G) = 3$ and $\mathrm{cd}(G/\mathbf{F}(G)) = \{1, r\}$ and $\mathrm{cd}(G) = \{1, r, r^2p, h, r^2h\}$.

(ii) $\mathbf{F}(G) = W \times V$ where W and V are minimal normal subgroups of G, having orders $r^{f(r,p)}$ and $s^{f(s,p)}$ respectively. Furthermore, $|G : \mathbf{F}(G)| = hr^2$.

(iii) The primes r and s both divide $|\mathbf{F}_2(G) : \mathbf{F}(G)|$.

(iv) The groups $G/\mathbf{C}_G(W)$ and $G/\mathbf{C}_G(V)$ are both nonnilpotent.

Note that c is always odd. (If $r = 2$, then q is a power of 2, so $c = q+1$ is odd. If r is odd, then q is odd, so $c = 1 + q + \cdots + q^{r-1}$ is odd.) Thus, if p, r, s are all odd, as in the case of the $(*)$-triple $(41, 5, 13)$, then choosing $h = cs$ produces a group G of odd order.

We give the construction for G. For $m = f(r,p)/r$ and $n = f(s,p)/r$, the definition of $(*)$-triple implies that s divides $r^m - 1$ and that r divides $s^n - 1$. Because $mr = f(r,p)$ and $nr = f(s,p)$, we see that p is a Zsigmondy prime for both $r^{mr} - 1$ and $s^{nr} - 1$.

Let C be the subgroup of order c in the cyclic multiplicative group $\mathrm{GF}(r^{mr})^\times$ of order $r^{mr} - 1$, and note that $\mathrm{GF}(r^{mr})^\times = C \dot{\times} \mathrm{GF}(r^m)^\times$. Let σ be the field automorphism that raises every element of $\mathrm{GF}(r^{mr})$ to the power r^m, and note that σ has order r. The centralizer of σ in $\mathrm{GF}(r^{mr})^\times$ is $\mathrm{GF}(r^m)^\times$, which has a subgroup of order s, because s divides $r^m - 1$. The action of $\langle\sigma\rangle$ on C is Frobenius. As p divides

https://doi.org/10.4153/CMB-2006-030-1 Published online by Cambridge University Press

$r^{mr} - 1$ but not $r^m - 1$, we see that C contains a subgroup of order p, and it follows that r divides $p - 1$.

Let H be the subgroup of order h in $\mathrm{GF}(r^{mr})^\times$. Let R be a cyclic group of order r^2, acting on H in such a way that $A = \mathbf{C}_R(P)$ has order r, while the action of R/A on H is equivalent to the natural action of $\langle\sigma\rangle$ on H. For the corresponding semidirect product group RH, note that $\mathbf{F}(RH) = A \times H$ is cyclic of order rh, and so $\mathrm{cd}(RH) = \{1, r\}$.

We let RH act on the additive group $W = \mathrm{GF}(r^{mr})$ such that $\mathbf{C}_{RH}(W) = A$, and the action of the the nonnilpotent group RH/A on W is equivalent to the natural action of $H\langle\sigma\rangle$ on W. Since c divides $h = |H|$, we see that H has a subgroup of order p. Viewed as a $\mathrm{GF}(r)[RH]$-module, W is irreducible because p is a Zsigmondy prime for $r^{mr} - 1$. For each nonprincipal character $\lambda \in \mathrm{Irr}(W)$, note that $\mathbf{I}_{RH}(\lambda)$ is cyclic of order r^2.

We now show that if $r = 2$, then $s^n + 1$ is not a power of 2. Assuming this is false, recall that p is a Zsigmondy prime for $s^{nr} - 1 = s^{2n} - 1 = (s^n - 1)(s^n + 1)$. Thus p divides the 2-power $s^n + 1$, forcing $p = 2 = r$, which contradicts our assumption that $p \neq r$.

Let L be the subgroup of index p in H. Thus RH/L has order r^2h. By the preceding paragraph, the fact that r divides $s^n - 1$, and [3, Theorem 10], the group RH acts on the additive group $V = \mathrm{GF}(s^{nr})$ in such a way that $\mathbf{C}_{RH}(V) = L$, and the action of the nonnilpotent group RH/L on V is Frobenius. As a $\mathrm{GF}(s)[RH]$-module, V is irreducible because p is a Zsigmondy prime for $s^{nr} - 1$. Let G be the semidirect product corresponding to the action of RH on the direct product $W \times V$. Indeed $\mathbf{C}_{RH}(W \times V) = \mathbf{C}_{RH}(W) \cap \mathbf{C}_{RH}(V) = A \cap L = 1$. Hence $\mathbf{F}(G) = W \times V$, and so $\mathrm{h}(G) = 3$. Write $F_1 = \mathbf{F}(G)$.

Finally we determine $\mathrm{cd}(G|F_1)$. Each nonprincipal character $\varphi \in \mathrm{Irr}(F_1)$ has the form $\varphi = \lambda \times \mu$, with at least one of $\lambda \in \mathrm{Irr}(W)$ and $\mu \in \mathrm{Irr}(V)$ being nonprincipal, and of course $\mathbf{I}_{RH}(\varphi) = \mathbf{I}_{RH}(\lambda) \cap \mathbf{I}_{RH}(\mu)$. If λ is principal, then $\mathbf{I}_{RH}(\varphi) = \mathbf{I}_{RH}(\mu) = L$ has order h/p, and so, because $|RH| = r^2h$, we have $\mathrm{cd}(G|\varphi) = \{r^2p\}$, by [2, Corollary 11.22, Theorem 6.11]. If μ is principal, then $\mathbf{I}_{RH}(\varphi) = \mathbf{I}_{RH}(\lambda)$ is cyclic of order r^2, and so $\mathrm{cd}(G|\varphi) = \{h\}$. If both λ and μ are nonprincipal, then $\mathbf{I}_{RH}(\varphi) = \mathbf{I}_{RH}(\lambda) \cap \mathbf{I}_{RH}(\mu) = 1$, and so $\mathrm{cd}(G|\varphi) = \{r^2h\}$. It follows that $\mathrm{cd}(G|F_1) = \{r^2p, h, r^2h\}$, and so $\mathrm{cd}(G) = \mathrm{cd}(G/F_1) \cup \mathrm{cd}(G|F_1) = \{1, r, r^2p, h, r^2h\}$, as claimed.

Acknowledgements We thank I. M. Isaacs and Mark L. Lewis for their helpful suggestions.

References

[1] B. Huppert and O. Manz, *Degree problems I. Squarefree character degrees.* Arch. Math. Basel **45**(1985), no. 2, 125–132.
[2] I. M. Isaacs, *Character Theory of Finite Groups.* Dover, New York, 1994.
[3] M. L. Lewis and J. M. Riedl, *Affine semi-linear groups with three irreducible character degrees.* J. Algebra **246**(2001), no. 2, 708–720.
[4] T. Noritzsch, *Groups having three complex irreducible character degrees.* J. Algebra **175**(1995), no. 3, 767–798.

https://doi.org/10.4153/CMB-2006-030-1 Published online by Cambridge University Press

[5] J. M. Riedl, *Fitting heights of solvable groups with few character degrees.* J. Algebra **233**(2000), no. 1, 287–308.

[6] ———, *Fitting heights of odd-order groups with few character degrees.* J. Algebra **267**(2003), no. 2, 421–442.

Department of Mathematics
University of Akron
Akron, OH 44325-4002
U.S.A.
e-mail: riedl@uakron.edu