Recognizing the prime divisors of the index of a proper subgroup

Andrea Lucchini a,*, Marta Morigi b

a Dipartimento di Matematica Pura e Applicata, Università di Padova, Via Trieste 63, 35121 Padova, Italy
b Dipartimento di Matematica, Università di Bologna, Piazza di Porta San Donato 5, 40126 Bologna, Italy

Article history:
Received 21 December 2010
Available online 30 March 2011
Communicated by E.I. Khukhro

MSC:
20F05
20D60

Keywords:
Generators
Index

Abstract

Let $G$ be a finite group and let $C$ be a subgroup of $G$. We prove that in order to get information on the set of primes dividing the index $|G:C|$ of $C$ in $G$ it is enough to look at the primes dividing $|H:C \cap H|$, where $H$ is a suitable subgroup of $G$ with few generators.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

In a recent paper, Camina, Shumyatsky and Sica proved the following theorem: let $x$ be an element of a finite group $G$ and let $\text{Ind}_C(x)$ be the index in $G$ of the centralizer $C_G(x)$ of $x$ in $G$; if $\text{Ind}_{\langle a, b, x \rangle}(x)$ is a prime-power for every $a, b \in G$, then $\text{Ind}_C(x)$ is a prime-power [2]. The above theorem can be restated as follows: let $x$ be an element of a finite group $G$ and let $C = C_G(x)$; if there is more than one prime dividing $|G:C|$, then there exist $a, b \in G$ such that $|\langle a, b, x \rangle : C \cap \langle a, b, x \rangle|$ is divisible by more than one prime.

In this paper we aim at generalizing this result. If we want to consider any subgroup $C$ of $G$, instead of limiting ourselves to centralizers of elements, it is more natural to look at $|H:C \cap H|$.
where \( H \) is a subgroup with “few” generators. If \( n \) is a positive integer we denote by \( \pi(n) \) the set of primes dividing \( n \). Our result is the following.

**Theorem A.** Let \( G \) be a finite group and let \( X, C \) be two subgroups of \( G \) such that \( X \leq C \). Then there exist \( a, b, c \in G \) such that \( \pi(|G : C|) \subseteq \pi(|(a, b, c) : C \cap (a, b, c)|) \).

When \( X \) is the identity subgroup we obtain the type of result we were originally aiming at.

**Corollary B.** Let \( G \) be a finite group and let \( C \) be a subgroup of \( G \). Then there exist \( a, b, c \in G \) such that 
\[
\pi(|G : C|) \subseteq \pi(|(a, b, c) : C \cap (a, b, c)|).
\]

When \( X = C \) we have a new type of result.

**Corollary C.** Let \( G \) be a finite group and let \( C \) be a subgroup of \( G \). Then there exist \( a, b, c \in G \) such that 
\[
\pi(|G : C|) = \pi(|(a, b, c) : C|).
\]

In order to deal with the case of prime-power index we need a stronger conclusion than that of Theorem A.

**Theorem D.** Let \( G \) be a finite group and let \( X, C \) be two subgroups of \( G \) such that \( X \leq C \). If \( |\pi(|G : C|)| \geq 2 \), then there exist \( a, b \in G \) such that 
\[
|\pi(|(a, b, X) : C \cap (a, b, X)|)| \geq 2.
\]

This imply the result in [2] when \( C = C_C(x) \) and \( X = \{x\} \).

We conjecture that Theorem A can be improved, because just 2 suitable generators could be enough in order to reach the conclusion, instead of 3, but proving this would need good estimates on the probability of generating 2-generated almost simple groups with 2 elements, and these results are not available at the moment. On the other hand, just one suitable generator is not enough to reach the conclusion of Theorem A, as the example of \( G = S_3 \) shows, when taking \( X = C = 1 \).

The following two propositions support this conjecture and give partial answers, in the case of soluble groups and in the case when no “small” prime divides \( |G : C| \).

**Theorem E.** Let \( G \) be a finite soluble group and let \( X, C \) be two subgroups of \( G \) such that \( X \leq C \). Then there exist \( a, b \in G \) such that 
\[
\pi(|G : C|) \subseteq \pi(|(a, b, X) : C \cap (a, b, X)|).
\]

**Theorem F.** Let \( G \) be a finite group and let \( X, C \) be two subgroups of \( G \) such that \( X \leq C \). Then there exists an absolute constant \( \hat{c} \) with the following property: if \( \mathcal{Q} \) is the set of primes which are bigger than \( \hat{c} \), then there exist \( a, b \in G \) such that 
\[
\pi(|G : C|) \cap \mathcal{Q} \subseteq \pi(|(a, b, X) : C \cap (a, b, X)|).
\]

2. Background material

In what follows \( d(G) \) denotes the minimal number of generators of the group \( G \) and if \( X \) is a subset of \( G \) then \( d_X(G) \) denotes the minimum integer \( d \) such that there exist \( d \) elements \( g_1, \ldots, g_d \in G \) with the property that \( G = \langle X, g_1, \ldots, g_d \rangle \). If \( p \) is a prime, \( |G|_p \) denotes the order of a Sylow \( p \)-subgroup of \( G \) and if \( x \) is an element of \( G \) then we will write \( |x|_p \) instead of \( |\langle x \rangle|_p \). Moreover, \( \text{Aut}(G) \) is the automorphism group of \( G \) and we recall that the socle \( \text{Soc}(G) \) of \( G \) is the subgroup generated by all minimal normal subgroups of \( G \).

Throughout the paper, we will often have to consider a quotient group \( G/N \) of a group \( G \). For the sake of brevity, if \( g \) (resp. \( U \)) is an element (resp. subgroup) of \( G \), then \( \bar{g} \) (resp. \( \bar{U} \)) will denote the image of \( g \) (resp. \( U \)) in \( G/N \).

Let \( L \) be a primitive monolithic group, that is a group with a unique minimal normal subgroup \( A \) such that if \( A \) is abelian, then it has a complement in \( L \). For each positive integer \( k \) we let \( L^k \) be the
A. Lucchini, M. Morigi / Journal of Algebra 337 (2011) 335–344

$k$-fold direct power of $L$. The crown-based power of $L$ of size $k$ is the subgroup $L_k$ of $L^k$ defined by

$$L_k = \{ (l_1, \ldots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \mod A \}. $$

Clearly, $\text{Soc}(L_k) = A^k$ and $L_k/\text{Soc}(L_k) \cong L/\text{Soc}(L)$. Note also that if $A$ has a complement $T$ in $L$, then $\text{diag}(T)$ is a complement of $\text{Soc}(L_k)$ in $L_k$ (here, if $U$ is a subset of $L$, $\text{diag}(U)$ denotes the following subset of $L_k$: $\text{diag}(U) = \{(u, \ldots, u) \mid u \in U\}$).

Crown-based powers arise naturally when studying finite groups that need more generators than any proper quotient, and they are a main tool also in the study of $d_X(G)$. The following theorem is a straightforward consequence of Proposition 12, Theorem 20 and Corollary 21 of [6].

**Theorem 1.** Let $X$ be a subset of a finite group $G$ and let $N$ be a normal subgroup of $G$ such that $N$ is maximal with the property that $d_{XN}(G) = d_X(G)$. Then there exist a monolithic primitive group $L$ and an isomorphism $\varphi : G/N \to L_k$ such that $\varphi(X) \leq \text{diag}(L)$. Moreover, if $A$ is abelian and $T$ is a complement of $A$ in $L$, then $\varphi(X) \leq \text{diag}(T)$.

In the setting of Theorem 1, we are interested in bounding $d_X(G)$ in terms of $k$. If $H$ is a finite group, $X$ is a subset of $H$ and $M$ is a normal subgroup of $H$ assume that $h_1, \ldots, h_k \in H$ and $X$ generate $H$ modulo $M$, that is $H = \langle h_1, \ldots, h_k, X, M \rangle$. It follows from Proposition 16 of [6] that the number $\Phi_{H,M}(X,s)$ of elements $(u_1, \ldots, u_s) \in M^s$ with the property that $H = \langle h_1u_1, \ldots, h_ku_s, X \rangle$ is independent of the choice of $h_1, \ldots, h_k$.

We will first study the case when the socle $A$ of the monolithic group $L$ is non-abelian. The following lemma is a sharpening of Lemma 1 of [3]. The proof is very technical and follows the same lines as the proof of Theorem 1.1 in [7] but at each step we take care of lifting generators in as many ways as we can.

**Lemma 2.** Let $L$ be a monolithic primitive group whose socle $A$ is isomorphic to $S^n$ for some non-abelian simple group $S$ and some natural number $n$. Moreover, let $X$ be a subset of $L$. Then there exists an almost simple group $S \leq H \leq \text{Aut} S$ which is isomorphic to a section of $L$, can be generated by $2$ elements and satisfies

$$\Phi_{L,A}(X,s) \geq n|S|^{n-1}\Phi_{H,S}(2)|A|^{s-2},$$

for each $s \geq 2$ such that $s \geq d_{XA}(L)$.

**Proof.** The hypothesis that $A \cong S^n$ is the unique minimal normal subgroup of $L$ implies that we may identify $L$ with a subgroup of $\text{Aut}(S^n) = \text{Aut} S \rtimes \text{Sym}(n)$, the wreath product of $\text{Aut} S$ with the symmetric group of degree $n$. So the elements of $L$ are of the kind $l = (\alpha_1, \ldots, \alpha_n)\sigma$, with $\alpha_i \in \text{Aut} S$ and $\sigma \in \text{Sym}(n)$. Let $\pi : \text{Aut} S \rtimes \text{Sym}(n) \to \text{Sym}(n)$ be the homomorphism which maps $(\alpha_1, \ldots, \alpha_n)\sigma$ to $\sigma$.

As $s \geq d_{XA}(L)$ there exist $l_1, \ldots, l_s \in L$ such that $L = \langle l_1, \ldots, l_s, X, A \rangle$. We want to count the number of elements $(u_1, \ldots, u_s)$ in $A^s$ with the property that $L = \langle u_1l_1, \ldots, l_sl_s, X \rangle$. Since this number is independent on the choice of $l_1, \ldots, l_s$ we may suppose that $\pi(l_1)$ is not a cycle of length $n$; moreover if $\pi(l_1)$ has no fixed points but then exist $l_1, l_2 \in L$ such that $L = \langle l_1, l_2, l_3, \ldots, l_s, X, A \rangle$ and $\pi(l_1)$ has a fixed point, then we substitute $l_1, l_2$ by $l_1, l_2$.

With this choice of $l_1, \ldots, l_s$ the proof of Theorem 1.1 in [7] shows how $u_1, \ldots, u_s \in M$ can be constructed with the property $L = \langle u_1l_1, \ldots, u_sl_s, X \rangle$. Let us describe this construction.

First we arbitrarily choose $u_3, \ldots, u_s \in A$, so that we have $|A|^{s-2}$ choices, then we show that $u_1, u_2 \in A$ can be chosen in at least $n|S|^{n-1}\Phi_{H,S}(2)$ ways. So from now on $u_3, \ldots, u_s \in A$ will be fixed, and we will say for shortness that the $2n$-tuple $(x_1, \ldots, x_n, y_1, \ldots, y_n) \in S^{2n}$ is good if $u_1 = (x_1, \ldots, x_n)$ and $u_2 = (y_1, \ldots, y_n)$ have the property that $L = \langle u_1l_1, u_2l_2, l_3, \ldots, l_s, X \rangle$.

In [7] it is proved that there exists a prime $r$ which divides $|S|$ and has the following property: for every $\alpha \in \text{Aut} S$ we can find an element $\beta \in S$ such that $\alpha \beta \neq 1$ and $|\alpha|_r \neq |\alpha \beta|_r$. So we can define a
quasi-ordering relation on the set of the cyclic permutations which belong to the group \( \text{Sym}(n) \). Let \( \sigma_1, \sigma_2 \in \text{Sym}(n) \) be two cyclic permutations (including cycles of length 1); we define \( \sigma_1 \preceq \sigma_2 \) if either \( |\sigma_1| < |\sigma_2| \) or \( |\sigma_1| = |\sigma_2| \) and \( \sigma_1 \preceq \sigma_2 \).

Let \( l_1 = (\alpha_1, \ldots, \alpha_n) \rho, \ l_2 = (\beta_1, \ldots, \beta_n) \sigma \), with \( \alpha_i, \beta_j \in \text{Aut} \ S \) and \( \rho, \sigma \in \text{Sym}(n) \). Then write \( \rho = \rho_1 \cdots \rho_s(\rho), \ \sigma = \sigma_1 \cdots \sigma_q(\sigma) \) as product of disjoint cycles (including possible cycles of length 1), in such a way that:

(a) \( \rho_1 \leq \cdots \leq \rho_s(\rho) \);
(b) \( \supp(\sigma_1) \cap \supp(\rho_1) \neq \emptyset \) if and only if \( i \leq q \);
(c) \( \sigma_1 \leq \cdots \leq \sigma_q \).

Let \( \rho_i = (m_{i,1}, \ldots, m_{i,|\rho_i|}), \ 1 \leq i \leq s(\rho), \ \sigma_j = (n_{j,1}, \ldots, n_{j,|\sigma_j|}), \ 1 \leq j \leq q \). We assume \( m_{1,1} = n_{1,1} = m \). For each integer \( c \geq 2 \) dividing the common divisor of \( |\rho_1| \) and \( |\sigma_1| \) define \( j_c = \frac{|\rho_1|(|\sigma_1|-1)}{c} \) and let \( n_{t,tc} = m_{t,tc} \), \( n_{tc,tc} = n_{tc,tc} \sigma_1^{-1} \). Note that when \( |\rho_1| \neq 1 \) then by our assumptions \( \sigma \) has no fixed points, so \( n_{t,tc} \neq n_{tc,tc} \). Consider the following subsets of \( \{1, \ldots, n\} \):

\[
\Omega_1 = \{m_{i,1} \mid 1 \leq i \leq s(\rho)\}, \quad \Omega_2 = \{n_{j,1} \mid 1 \leq j \leq q\},
\]

\[
\Omega_3 = \{n_{t,tc}, n_{tc,tc} \mid c \geq 2, \ c \text{ divides } \gcd(\{|\rho_1|, |\sigma_1|\})\}.
\]

Moreover let

\[
\Omega_2^* = \Omega_2 \setminus \Omega_3 \quad \text{and} \quad q^* = |\Omega_2^*|.
\]

Now, if \( u_1 = (x_1, \ldots, x_n), u_2 = (y_1, \ldots, y_n) \in A = S^n \) define \( \tilde{\alpha}_t = x_t \alpha_t, \ \tilde{\beta}_t = y_t \beta_t, \ 1 \leq r \leq n \) and \( a_t = \tilde{\alpha}_{m_{t,1}} \cdots \tilde{\alpha}_{m_{t,|\rho_t|}}, \ 1 \leq t \leq s(\rho), \ b_j = \tilde{\beta}_{n_{j,1}} \cdots \tilde{\beta}_{n_{j,|\sigma_j|}}, \ 1 \leq j \leq q \).

Moreover let \( a = a_{m_{1,1}} \tilde{\alpha}_{m_{1,2}} \cdots \tilde{\alpha}_{m_{1,|\rho_1|}}, b = b_{t_1} \tilde{\beta}_{t_2} \cdots \tilde{\beta}_{t_q} \) and consider \( H = \langle a, b, S \rangle \). It follows from the main result in [4] that \( H \) is 2-generated.

By [7] the 2n-tuple \( (x_1, \ldots, x_n, y_1, \ldots, y_n) \) is good if the following set \( \mathcal{M} \) of conditions is satisfied:

1. \( \langle a_1, b_1 \rangle = \langle x_m a, y_m b \rangle = H \); note that there are \( \Phi_H.S(2) \) pairs \( (x_m, y_m) \in S^2 \) satisfying this property.
2. \( a_{t_j}^{\rho_1 \cdots \rho_j} \neq a_{t_j} \) and \( a_{t_j}^{\rho_1 \cdots \rho_j} \neq a_{t_j}^{\rho_1} \) are not conjugate in \( \text{Aut} \ S \), for every \( 2 \leq j \leq s(\rho) \).
3. \( b_{t_j}^{\sigma_1 \cdots \sigma_j} \neq b_{t_j} \) and \( b_{t_j}^{\sigma_1 \cdots \sigma_j} \neq b_{t_j}^{\sigma_1} \) are not conjugate in \( \text{Aut} \ S \), for every \( 2 \leq j \leq q \).
4. This condition is quite technical and we will not report it here. The relevant fact for our purposes is that it must hold for every \( c \geq 2 \) dividing \( \gcd(\{|\rho_1|, |\sigma_1|\}) \), and if the 2n-tuple \( \eta = (x_1, \ldots, x_n, y_1, \ldots, y_m) \) satisfies some subset \( \mathcal{N} \) of \( \mathcal{M} \) but not condition (4) for some \( c \), then there are two elements \( \gamma_1 \) and \( \gamma_2 \) of \( \text{Aut} \ S \) such that for every \( z \in S \) with the property that \( \gamma_1^z \neq \gamma_2 \), the 2n-tuple obtained from \( \eta \) by replacing \( y_{m_{tc}} \) with \( z^{-1} y_{m_{tc}} \) and by replacing \( y_{n_{tc}} \) with \( y_{n_{tc}} \beta_{n_{tc}} \sigma_1 \beta_{n_{tc}}^{-1} \) satisfies condition (4) for \( c \) and still satisfies all the conditions in \( \mathcal{N} \).

Note that we can choose \( z \) in at least \( |S| - |\mathcal{C}_S(\gamma_1)| \geq 4|S|/5 \) possible ways.

Now we choose \( x_{m_1} \) and \( y_{m_1} \) in such a way that condition (1) is satisfied; there are \( \Phi_H.S(2) \) choices.

Now we fix \( i \) such that \( 2 \leq i \leq s(\rho) \). The main lemma of [7] guarantees the existence of \( x_{m_1} \in S \) such that \( a_i \neq 1 \) and \( a_i^{\rho_1 \cdots \rho_j} \neq a_i^{\rho_1} \) is not conjugate in \( \text{Aut} S \) to \( a_i^{\rho_1 \cdots \rho_j} \), and in particular \( |a_i| \neq |a_i| \). Now we will show that \( x_{m_1} \) can be modified in at least 4 more ways. If \( w \in S \) is such that \( a_i^{w} \neq a_i \) then we can choose \( x_{m_1}^{w} \) such that \( a_i^{w} = a_i^{w} x_{m_1}^{w} \alpha_{m_2} \cdots \alpha_{m_{|\rho_1|}} \). Then \( x_{m_1}^{w} \neq x_{m_1} \) and \( (a_i^{w})^{\rho_1 \cdots \rho_j} \neq a_i^{\rho_1 \cdots \rho_j} \) and \( a_i^{\rho_1 \cdots \rho_j} \neq a_i^{\rho_1} \) cannot be conjugate. The possible choices for \( a_i^{w} \neq a_i \) are \( |S| : \mathcal{C}_S(a_i) \geq 4 \), so we can choose \( x_{m_1}^{w} \) in at least 4 more ways.
This is true for every $i$ such that $2 \leq i \leq s(\rho)$, and the same argument can be used also when $2 \leq j \leq q$. We will do so for all $2 \leq j \leq q$ such that $n_{j,1} \in \Omega_2^s$. So the number of choices for this step is at least $5^{|\Omega_1|+|\Omega_2^s|-2}$.

If $|\rho_1| = 1$ then $\Omega_2 = \emptyset$ and $q = q^* = 1$, so the total number of choices is at least

$$\Phi_{H,S}(2)|S|^{2n-s(\rho)-1} 5^s(\rho)-1.$$

It suffices to prove that $|S|^{n-s(\rho)+s(\rho)-1} \geq n$. As the right-hand side of the last inequality is minimum for $s(\rho) = n$ we need that $5^{n-1} \geq n$, which is true for every $n \geq 1$.

Now suppose $|\rho_1| \neq 1$. Then we need to consider the set of conditions in (4) as well. As $\rho$ has no fixed point, by our choice of $l_1$ and $l_2$, $\sigma \rho^k$ is fixed-point-free for all $k \in \mathbb{N}$. This implies in particular that if $c_1 \neq c_2$, then we have $\{n_{i,c_1,t_1}, n_{i,c_1,u_1}\} \cap \{n_{i,c_2,t_2}, n_{i,c_2,u_2}\} = \emptyset$. Indeed suppose for example that there exist $i$ and $j$ with

$$n_{i,c_1,t_1} = n_{i,j} = m_{1,jc_1} \quad \text{and} \quad n_{i,c_1,u_1} = n_{i,j+1} = m_{1,jc_2}.$$

This would imply that $n_{i,j} \rho^k = n_{i,j} \rho^k = n_{i,j+1}$ for some $k \in \mathbb{N}$ and $n_{i,j} \sigma = n_{i,j+1} \sigma$, but then $\sigma \rho^{-k}$ fixes $n_{i,j}$, a contradiction. The same argument proves that $m \neq \Omega_3$. In particular it follows that $|\Omega_3| = 2^r$ where $r$ denotes the number of integers $c \geq 2$ dividing $\text{g.c.d.}(|\rho_1|, |\sigma_1|)$.

Now for each $l \in \Omega_3 \cap \Omega_2$ we can argue as we did for the elements of $\Omega_2^s$, finding an appropriate $y_l$ in order to satisfy condition (3). Then for every value of $c$ we choose $z$ as in condition (4), we replace $y_{n_{c,l}c}$ with $y_{n_{c,l}c}^{-1} y_{n_{c,l}c}$ and we replace $y_{n_{c,l}c}$ with $y_{n_{c,l}c} \rho_{n_{c,l}c} \rho_{n_{c,l}c}^{-1}$. Remember that $z$ can be chosen in at least $4|S|/5$ different ways. This means that the number of possibilities for the pair $(y_{n_{c,l}c}, y_{n_{c,l}c^-})$ is at least $4|S|/5$. It follows that the number of $2n$-tuples which are good is at least

$$\Phi_{H,S}(2)|S|^{2n-s(\rho)-q^*-r} 5^s(\rho)+q^*+2 \cdot (4/5)^r.$$

So it suffices to prove that

$$|S|^{n+1-s(\rho)-q^*-r} 5^s(\rho)+q^*+2 \cdot (4/5)^r \geq n.$$

Note that

$$|S|^{n+1-s(\rho)-q^*-r} 5^s(\rho)+q^*+2 \cdot (4/5)^r = f(s(\rho)+q^*+r) g(r),$$

where

$$f(x) = |S|^{n+1-x} 5^x \quad \text{and} \quad g(x) = 5^{-2-x} \cdot (4/5)^x.$$

We will study separately the two functions $f(x)$ and $g(x)$. Since $|\rho_1| \neq 1$ and $\rho_1 \leq \rho_i$ for $1 \leq i \leq s(\rho)$, we have

$$s(\rho) - 1 \leq n - \frac{|\rho_1|}{2}.$$
Moreover it is easy to see that

\[ \gamma \leq \frac{g \cdot d \cdot (|\rho|, |\sigma|)}{2} \leq \frac{|\rho|}{2}, \]

so

\[ s(\rho) + q^* + \gamma \leq \frac{n}{2} - \frac{|\rho|}{2} + q^* + \frac{|\sigma|}{2} + 1. \]

Since \( q^* \leq q \leq |\rho| \) and \( q + |\sigma| \leq n + 1 \) we conclude

\[ s(\rho) + q^* + \gamma \leq \left[ \frac{n}{2} - \frac{|\rho|}{2} + q^* + \frac{|\sigma|}{2} + 1 \right] \leq \left[ n + \frac{3}{2} \right] = n + 1. \]

where with \([x]\) we denote the integer \( v \) such that \( v \leq x < v + 1 \). Since \( f(x) \) is a decreasing function we have

\[ f(s(\rho) + q^* + \gamma) \geq f(n + 1) = 5^{n+1}. \]

Note that \( |\rho| \leq n - 2 \), because \( \rho \) is not a cycle and has no fixed points, so \( \gamma \leq |\rho|/2 \leq n/2 - 1 \). As \( g(x) \) is also a decreasing function we have

\[ g(x) \geq g(n/2 - 1) = 2^{n-2} \cdot 5^{-n}. \]

It follows that

\[ |S|^{n+1-s(\rho)-q^*-\gamma} \cdot 5^{s(\rho)+q^*-2} \cdot (4/5)^{\gamma} \geq 2^{n-2} \cdot 5 \geq n, \]

as we wanted. \( \square \)

**Lemma 3.** Let \( L \) be a monolithic primitive group with non-abelian socle \( A \) and let \( X \subseteq L \). Assume that \( t \leq |\pi ((A))| + 1 \). Then the following hold:

(i) \( d_{\text{diag}(X)}(L_t) \leq \max \{ 3, d_{X^t}(L_t) \} \).

(ii) There exists an absolute constant \( \tilde{c} \) such that if the maximum of the set \( \pi ((A)) \) is bigger than \( \tilde{c} \) then \( d_{\text{diag}(X)}(L_t) \leq \max \{ 2, d_{X^t}(L_t) \} \).

**Proof.** Let \( s \geq \max \{ 2, d_{X^t}(L_t) \} \) be an integer. It follows from Proposition 16, formulas (3.2) and Lemma 18 of [6] that there exist \( g_1, \ldots, g_s \in L_t \) such that \( L_t = \langle \text{diag}(X), g_1, \ldots, g_s \rangle \) if and only if

\[ t \leq \Phi_{L^tA}(X, s)/\gamma, \tag{1} \]

where \( \gamma = |C_{\text{Aut}(A)}(L/A) \cap C_{\text{Aut}(A)}(X)\| \). Let \( A = S^n \), where \( S \) is a non-abelian simple group. In the proof of Lemma 1 in [4] it is shown that \( |C_{\text{Aut}(A)}(L/A)| \leq n |S|^{n-1} |C_{\text{Aut}(S)}(H/S)| \), where \( H \) is the subgroup of \( \text{Aut} S \) which appears in the statement of Lemma 2. As \( \gamma \leq |C_{\text{Aut}(A)}(L/A)| \), by Lemma 2 we have

\[ \frac{\Phi_{L^tA}(X, s)}{\gamma} \geq n |S|^{n-1} |\Phi_{H,S}(2)|A|^{s-2} = \frac{\Phi_{H,S}(2)|A|^{s-2}}{|C_{\text{Aut}(S)}(H/S)|}. \]

In order to prove the first part of the lemma note that \( \frac{\Phi_{H,S}(2)}{|C_{\text{Aut}(H/S)}|} \geq 1 \) (see for instance Theorem 2.7 of [3]), so \( \frac{\Phi_{L^tA}(X, s)}{\gamma} \geq |A|^{s-2} \). Take \( s = \max \{ 3, d_{X^t}(L_t) \} \); then \( t \leq |\pi ((A))| + 1 \leq |A| \leq |A|^{s-2} \) so condition (1) is satisfied and statement (i) follows.
Now, by Proposition 2.7 of [9], there exists a constant $c_S$ depending on $S$ such that $\Phi_{H,S}(2) \geq |S|^2 c_S$ and $\lim_{|S| \to \infty} c_S = 1$. Moreover, by Lemma 1.3 of [8], we have $|\text{Aut} S| \leq \beta |S| \log_2 |S|$ for some positive constant $\beta$.

It follows that

$$\frac{\Phi_{L,A}(X,s)}{\gamma} \geq \frac{\Phi_{H,S}(2)|A|^{s-2}}{|C_{\text{Aut} S}(H/S)|} \geq \frac{\Phi_{H,S}(2)}{|\text{Aut} S|} \geq \frac{c_S|S|}{\beta \log_2 |S|^2}.$$ 

Let $m_S$ be the maximum of the set $\pi(|S|) = \pi(|A|)$. Note that when $m_S$ tends to infinity then $|S|$ tends to infinity as well, so there exists an absolute constant $\bar{c}$, independent on $S$, with the following property: for any non-abelian simple group $S$ such that $m_S \geq \bar{c}$ we have $\beta(\log_2 |S|)^2 \leq c_S |S|$. Note that $|\pi(|A|)| + 1 \leq \log_2 |S|$; so taking $s = \max(2, d_{X\mathcal{A}}(L))$ we have if $m_S \geq \bar{c}$ then condition (1) is satisfied, thus $d_{\text{diag}}(\langle L \rangle) \leq s = \max(2, d_{X\mathcal{A}}(L))$, as we wanted. \(\square\)

In order to deal with the case when the socle of $L$ is abelian we will need Theorem A of [1]. In the following, if $G$ is a finite group and $V$ is a $G$-module, then $H^1(G, V)$ denotes the first cohomology group of $G$ on $V$. Note that there is a bijection between $H^1(G, V)$ and the set of conjugacy classes of complements of $V$ in the semidirect product $V G$.

**Theorem 4.** Let $p$ be a prime. If $G$ is a finite group and $V$ is a faithful irreducible $G$-module over the field with $p$ elements, then $|H^1(G, V)| < |V|$.

The following lemma bounds $d_Y(L)$ for a primitive monolithic group $L$.

**Lemma 5.** Let $L$ be a monolithic primitive group with socle $A$ and let $Y \subseteq L$. Then $d_Y(L) \leq \max(2, d_{A\mathcal{Y}}(L))$.

**Proof.** Let $s = \max(2, d_{A\mathcal{Y}}(L))$. If $A$ is non-abelian it follows from Lemma 2 that $\Phi_{L,A}(Y,s) > 0$, so $d_Y(L) = s$. If $A$ is central then $A = L$ is cyclic of prime order and the result is trivially true. So we may assume that $A$ is abelian and not central in $L$. Consider $z_1, \ldots, z_s$ such that $T = \langle Y, z_1, \ldots, z_s \rangle$ and let $Q = \langle Y, z_2, \ldots, z_s \rangle$. We will prove that there exist $w_1, w_2 \in A$ such that $L = \langle Q, z_1 w_1, z_2 w_2 \rangle$. If not, then $\langle Q, z_1 w_1, z_2 w_2 \rangle$ is a complement of $A$ in $L$ for every $w_1, w_2 \in A$. Moreover, if $(w_1, w_2), (w_1^*, w_2^*) \in A^2$ are such that $\langle Q, z_1 w_1^*, z_2 w_2^* \rangle = \langle Q, z_1 w_1, z_2 w_2 \rangle = H$, then $w_1^{-1} w_1^*, w_2^{-1} w_2^* \in A \cap H = 1$, so $(w_1, w_2) = (w_1^*, w_2^*)$. It follows that $A$ has at least $|A|^2$ complements in $L$. On the other side, by Theorem 4, there are less than $|A|$ conjugacy classes of complements of $A$ in $L$, so there are less than $|A|^2$ complements of $A$ in $L$. This contradiction proves that $L = \langle Q, z_1 w_1, z_2 w_2 \rangle$ for some $w_1, w_2 \in A$, so $d_Y(L) \leq s$, and this is enough to conclude the proof. \(\square\)

Finally, we will need the following fact.

**Lemma 6.** Let $S$ be a finite non-abelian simple group. Then both $S$ and $S \times S$ are 2-generated.

**Proof.** The first statement is a well-known consequence of the classification of finite simple groups (see for example [1, Theorem B]). Let $x_1, x_2$ be two non-trivial elements of $S$, such that $|x_1| \neq |x_2|$. By the main corollary of [5, p. 745] there exist $y_1, y_2 \in S$ such that $S = \langle x_1, y_1 \rangle = \langle x_2, y_2 \rangle$. It follows that the two elements $(x_1, x_2)$ and $(y_1, y_2)$ generate either $S \times S$ or a diagonal subgroup of the form $D = \{(x, \varphi(x)) \mid x \in S\}$, for some $\varphi \in \text{Aut} S$. But this last possibility cannot occur by the choice of $(x_1, x_2)$. So the second statement is proved. \(\square\)

3. Proofs of the theorems

We will describe a key step of our proof in the following lemma.
Lemma 7. Let $G$ be a finite group, let $X, C$ be two subgroups of $G$ such that $X \subseteq C$ and let $Q \subseteq \pi (\langle G : C \rangle)$. Assume that $G$ has no proper subgroups $H$ containing $X$ such that $Q \subseteq \pi (\langle H : C \cap H \rangle)$. Assume also that for some positive integer $t$ and some non-trivial monolithic primitive group $L$ there exists an epimorphism $\varphi : G \to L_t$ such that $\varphi (X) \leq \text{diag}(L)$ and $\varphi (X) \leq \text{diag}(T)$ if the socle $A$ of $L$ is abelian, where $T$ is a complement of $A$ in $L$. Then the following hold:

(i) If $A$ is abelian, then $t = 1$.
(ii) If $A$ is non-abelian then $t \leq \beta + 1$, where $\beta = |Q \cap \pi (\langle A \rangle)|$.

Proof. Let $N$ be the kernel of $\varphi$, so that $\tilde{G} = G/N$ is isomorphic to $L_t$. We will identify $\tilde{G}$ and $\varphi (G) = L_t$ in the obvious way. Let $\tilde{K} = \text{diag}(L)$ if $A$ is non-abelian, and let $\tilde{K} = \text{diag}(T)$ if $A$ is abelian. It follows from our hypotheses that $X \subseteq K$.

Let $M = \text{Soc}(\tilde{G}) = N_1 \times \cdots \times N_t$. We will define two subsets $\mathcal{P}$ and $\mathcal{P}^*$ of $Q$.

\[ \mathcal{P} = \{ p \in Q : p \text{ divides } |\tilde{G} : \tilde{C}| \text{ and } |\tilde{M} \cap \tilde{C}|_p < |\tilde{M}|_p \} \]

\[ \mathcal{P}^* = \{ p \in Q : p \text{ divides } |\tilde{G} : \tilde{C}| \text{ and } |\tilde{M} \cap \tilde{C}|_p = |\tilde{M}|_p \} \]

Note that $\mathcal{P} \subseteq \pi (\langle A \rangle)$. If $p$ is in $\mathcal{P}$ there exists $i_p$ such that $|\tilde{N}_{i_p} \cap \tilde{C}|_p < |\tilde{N}_{i_p}|_p$. Let $A = \{ i_p | p \in \mathcal{P} \}$ and let $\tilde{H} = \tilde{K} \prod_{i \in A} N_i$. Note that $|A| \leq \beta$ and if $A$ is non-abelian, either $t = \beta$ or $\tilde{H} \cong l_{A|+1}$. If $A$ is abelian, then it is an elementary abelian $p$-group for some prime $p$, so $|\mathcal{P}| \leq 1$ and $\tilde{K}$ is isomorphic either to $L_t$ or to $T$.

Now we prove that $\mathcal{P} \subseteq \pi (\langle H : C \cap H \rangle)$. If not, for some prime $p \in \mathcal{P}$ there exists a Sylow $p$-subgroup $U$ of $H$ which is contained in $C$. Then $\tilde{U} \cap \tilde{N}_{i_p}$ is a Sylow $p$-subgroup of $\tilde{N}_{i_p}$, but this contradicts the fact that $|\tilde{N}_{i_p} \cap \tilde{C}|_p < |\tilde{N}_{i_p}|_p$.

We will prove that also $\mathcal{P}^* \subseteq \pi (\langle H : C \cap H \rangle)$. Let $p \in \mathcal{P}^*$, so that $p$ does not divide $|\tilde{M} : \tilde{M} \cap \tilde{C}| = |\tilde{M} \cap \tilde{C}|$. As $|\tilde{G} : \tilde{C}| = |\tilde{G} : \tilde{M} \cap \tilde{C}| = |\tilde{M} \cap \tilde{C}|$, we have $p$ must divide $|\tilde{G} : \tilde{M} \cap \tilde{C}| = |G : MC|$. Moreover $G = KM = HM$ so it follows that $p$ divides $|HM : MC|$, which in turn divides $|HMC : MC| = |H : H \cap C|$. Then $p$ divides $|H : H \cap C|$, as we wanted.

Now if $p \in Q \setminus (\mathcal{P} \cup \mathcal{P}^*)$ we have $p$ divides $|G : C| = |G : CN||CN : C|$ but does not divide $|G : CN|$. So $p$ divides $|CN : C| = |N : N \cap C|$ and no Sylow $p$-subgroup of $N$ is contained in $C$. Now let $U$ be any Sylow $p$-subgroup of $H$; as $U \cap N$ is a Sylow $p$-subgroup of $N$, it follows that $U$ cannot be contained in $C$. This proves that $p \in \pi (\langle H : C \cap H \rangle)$.

So we have $Q \subseteq \pi (\langle H : C \cap H \rangle)$ and thus $H = G$ by our hypothesis. Now part (b) follows immediately when $A$ is non-abelian.

If $A$ is abelian, then either $\tilde{G} = \tilde{H} \cong L_t$ which implies that $t = 1$, or $\tilde{G} = \tilde{K}$, which contradicts the fact that $L_t$ is an epimorphic image of $G$. This proves part (a) and concludes the proof of the lemma.

Theorems A, E and F and Corollaries B and C are an immediate consequence of the following proposition.

Proposition 8. Let $G$ be a finite group, let $X, C$ be two subgroups of $G$ such that $X \subseteq C$ and let $Q \subseteq \pi (\langle G : C \rangle)$. Assume that $G$ has no proper subgroup $H$ containing $X$ such that $Q \subseteq \pi (\langle H : C \cap H \rangle)$. Then $d_X (G) \leq 3$. Moreover, if $G$ is soluble or if the minimum $m$ of $Q$ is bigger than the absolute constant $\tilde{c}$ defined in Lemma 3, then $d_X (G) \leq 2$.

Proof. Let $N$ be a normal subgroup of $G$ such that $N$ is maximal with the property that $d_X (G) = d_X (G) = d$. Then, by Theorem 1, there exist a monolithic primitive group $L$ and an isomorphism $\varphi : G/N \to L_t$ satisfying the conditions of Lemma 7. We have $\varphi (XN/N) = \text{diag}(Y)$ for some $Y \subseteq L$. Moreover, by maximality of $N$, if $M/N = \text{Soc}(G/N)$ then $d_X (G/N) = d_Y (L) \leq d - 1$. Let $\delta = 3$ in the general case, and let $\delta = 2$ if $G$ is soluble or $m > \tilde{c}$. Assume by contradiction that $d \geq \delta$. 
If $A$ is abelian, then it follows from Lemma 7 that $t = 1$, so $G/N$ is isomorphic to $L$ and, by Lemma 5, $d_X(G) = d_Y(L) \leq \max(2, d_Y(A(L))) \leq \max(2, d - 1)$, a contradiction. This settles the case when $A$ is abelian and proves the proposition when $G$ is soluble.

If $A$ is non-abelian, then it follows from Lemma 7 that $t \leq \beta + 1$, where $\beta = |Q \cap \pi(|A|)| \leq \pi(|A|)$. If $d > 3$, by Lemma 3(i) we have $d_X(G) = d_{\text{diag}}(L_t) \leq \max(3, d_Y(A(L))) \leq d - 1$, a contradiction.

So we are left with the case when $d = 3$, $\delta = 2$ and $m > \tilde{c}$. Then two possibilities may occur. If $\beta = 0$ then $t = 1$ and, by Lemma 5, $d_X(G) = d_Y(L) \leq \max(2, d - 1)$, a contradiction. Otherwise $\beta \geq 1$, which implies that $Q \cap \pi(|A|)$ is not empty. So there exists a prime $p > \tilde{c}$ which divides $|A|$; in particular the maximum of $\pi(|A|)$ is greater than $\tilde{c}$, and by Lemma 3(ii) we get that $d_X(G) = d_{\text{diag}}(L_t) \leq \max(2, d_Y(A(L))) \leq d - 1$. This contradiction concludes the proof. $\square$

The next proposition establishes Theorem D.

**Proposition 9.** Let $G$ be a finite group, let $X, C$ be two subgroups of $G$ such that $X \leq C$. Assume that $|\pi(|G : C|)| \geq 2$ and that $G$ has no proper subgroup $H$ containing $X$ such that $|\pi(H : C \cap H)| \geq 2$. Then $d_X(G) \leq 2$.

**Proof.** Let $N$ be a normal subgroup of $G$ such that $N$ is maximal with the property that $d_{XN}(G) = d_X(G)$. Then by Theorem 1 there exist a monolithic primitive group $L$ and an isomorphism $\varphi : G/N \to L_t$ satisfying the conditions of Lemma 7. We identify $\tilde{G} = G/N$ with $L_t$. Let $A = \text{Soc}(L)$, let $K = \text{diag}(L)$ and let $M = \text{Soc}(\tilde{G})$.

If $t = 1$, then we can conclude by using the same arguments as in the proof of Proposition 8. More precisely, assume by contradiction $d_X(G) = d > 2$. By maximality of $N$ we have $d_{\tilde{X}}(L_t) \leq d - 1$.

It follows from Lemma 5 that $d_X(G) = d_X(L_t) \leq \max(2, d_Y(A(L))) \leq \max(2, d - 1)$, a contradiction. This settles the case $t = 1$.

By Lemma 7(i) if $A$ is abelian then $t = 1$, so we may assume that $A = S^n$ where $S$ is a non-abelian simple group.

The next statement is a key step in our argument:

\[(*) \text{ If there exist two primes } p \text{ and } q \text{ which divide } |\tilde{M} : \tilde{M} \cap \tilde{C}| \text{ then } d_X(G) \leq 2.\]

We will now prove statement $(*)$. We have $\tilde{M} = S_1 \times \cdots \times S_m$, where $S_k$ is isomorphic to $S$ for every $k = 1, \ldots, nt$. So there exist $i$ and $j$ such that $|S_i \cap \tilde{C}|_p < |S_i|_p$ and $|S_j \cap \tilde{C}|_q < |S_j|_q$. Note that $(S_i, S_j)$ is isomorphic either to $S$ or to $S^2$, so by Theorem 6 we have $(S_i, S_j)$ is 2-generated, and let $\bar{y}_1, \bar{y}_2 \in \tilde{G}$ be such that $(S_i, S_j) = (\bar{y}_1, \bar{y}_2)$. We will assume that $|\pi(|H : H \cap \tilde{C}|)| \geq 2$. Assume by contradiction that $p$ does not divide $|H : H \cap \tilde{C}|$. Then there exists a Sylow $p$-subgroup $\tilde{U}$ of $H$ such that $\tilde{U} \leq \tilde{C}$. Since $S_i$ is a subnormal subgroup of $H$, we have $\tilde{U} \cap S_i$ is a Sylow $p$-subgroup of $S_i$ and it is contained in $\tilde{C}$, a contradiction. Similarly, we have $q$ divides $|H : H \cap \tilde{C}|$. So $|\pi(|H : H \cap C|)| \geq |\pi(|H : H \cap \tilde{C}|)| \geq 2$ and $H$ cannot be a proper subgroup of $G$. Thus $G = H$ and $d_X(G) \leq 2$, so statement $(*)$ is proved.

Now let $Q = \pi(|G : C|)$ and define $P, P^*$ as in the proof of Lemma 7. By statement $(*)$ we can assume that $|P| \leq 1$. We will prove that if $P = \{p\}$ then $p$ divides $|K : K \cap C|$. As $|M \cap \tilde{C}|_p < |\tilde{M}|_p$, there exists $i$ such that $|S_i \cap \tilde{C}|_p < |S_i|_p$. We have $\bar{B} = S_i \cap \tilde{C}$ is a proper subgroup of $S_i$. Moreover $|S_i : B|$ is a power of $p$, because $|M \cap \tilde{C}|_p < |\tilde{M}|_p$.

Note that $K \cap \tilde{M} = \text{diag}(A)$ so $\pi_t(K \cap \tilde{M}) = S_i$. As $K \cap \tilde{C} \cap \tilde{M}$ normalizes $\bar{B}$, it follows that $D = \pi_t(K \cap \tilde{C} \cap \tilde{M})$ normalizes $\pi_t(B)$; $\tilde{B}$. This implies that no Sylow $p$-subgroup of $S_i$ is contained in $D$, otherwise $\pi(\bar{B})$ would be a non-trivial proper normal subgroup of $S_i$. So $p$ divides $|S_i : D| = |\pi_t(K \cap \tilde{M}) : \pi_t(K \cap \tilde{C} \cap \tilde{M})|$ and thus $p$ divides $|K \cap \tilde{M} : K \cap \tilde{C} \cap \tilde{M}| = |(K \cap \tilde{M})(K \cap \tilde{C}) : K \cap \tilde{C}|$.

It follows that $p$ divides $|K : K \cap C|$, as we wanted.

Arguing as in Lemma 7 for the primes in $P^*$ and in $Q \setminus (P \cup P^*)$, we obtain that $Q \leq \pi(|K : K \cap C|)$, so $K = G$ by minimality of $G$ and again $t = 1$. This concludes the proof. $\square$
Acknowledgment

The authors are grateful to Pavel Shumyatsky for driving their attention to this subject.

References