Rev. Mat. Iberoam. 39 (2023), no. 4, 1323–1347
DOI 10.4171/RMI/1333

On profinite groups with positive rank gradient

Nikolay Nikolov

Abstract. We prove that a profinite group G with positive rank gradient does not satisfy a group law. In the case when G is a pro-p group, we show that G contains a nonabelian dense free subgroup.

1. Introduction

Let G be a finitely generated group. We denote by $d(G)$ the minimal number of generators of G, with the convention that if G is a profinite group then $d(G)$ is the minimal number of topological generators. When p is a prime, $d_p(G)$ will denote the minimal number of generators of the pro-p completion of G, that is, $d_p(G) = \dim_{\mathbb{F}_p} \frac{G}{\Phi(G)}$, where $\Phi(G) = G^p[G,G]$ is the p-Frattini subgroup of G.

Assume additionally that G is residually finite. Let $G \geq H_1 \geq H_2 \geq \cdots$ be a chain of normal subgroups H_i, each having finite index in G and such that $\cap_i H_i = \{1\}$. The rank gradient of G with respect to (H_i) is defined as

$$\mathrm{RG}(G,(H_i)) := \lim_{i\to\infty} \frac{d(H_i)-1}{|G:H_i|}\cdot$$

When (H_i) is a chain of normal subgroups as above and additionally $|G:H_i|$ is a power of p for all $i \in \mathbb{N}$, we define the p-gradient $\mathrm{RG}_p(G,(H_i))$ in the same way:

$$\mathrm{RG}_p(G,(H_i)) := \lim_{i\to\infty} \frac{d_p(H_i)-1}{|G:H_i|}\cdot$$

From Schreier's inequality $d(H_i)-1 \leq |G:H_i|(d(G)-1)$ and its pro-p analogue, we deduce that $\mathrm{RG}(G,(H_i))$ and $\mathrm{RG}_p(G,(H_i))$ exist as a limits of monotonic non-increasing sequences.

It is an open problem whether the rank gradient depends or not on the choice of the chain (H_i), and this is related to the fixed price problem of topological dynamics, see [2]. In any case, we set

$$\mathrm{RG}(G) := \inf\Big\{\frac{d(H)-1}{|G:H|} \;\Big|\; H <_f G\Big\},$$

2020 Mathematics Subject Classification: Primary 20E18; Secondary 20F69.
Keywords: Rank gradient, group laws.

where the infimum is taken over all subgroups H of finite index G, and define $\mathrm{RG}_p(G)$ similarly:

$$\mathrm{RG}_p(G) := \inf\Big\{\frac{d_p(H)-1}{|G:H|} \mid H \lhd G,\ |G:H| = p^k,\ k \in \mathbb{N}\Big\}.$$

Suppose M is a subgroup of finite index of G. An easy exercise with the Schreier inequality gives that the infimum in the definition of $\mathrm{RG}(G)$ can be restricted to the set of finite index subgroups H of G contained in M. So we have

$$\mathrm{RG}(M) = |G:M| \cdot \mathrm{RG}(G).$$

When G is a profinite group, we define the rank gradient $\mathrm{RG}(G,(H_i))$ of G with respect to chains of open normal subgroups H_i with $\cap H_i = \{1\}$ using the same expression as above. In that case, a compactness argument shows that $\mathrm{RG}(G,(H_i))$ does not depend on the choice of the sequence (H_i) and is equal to $\mathrm{RG}(G)$.

Starting with the work of Lackenby [8], there has been a lot of interest in rank gradient of abstract residually finite groups, see e.g. [1, 2, 9]. It is tempting to believe that finitely generated abstract groups with positive rank gradient are in some way related to free groups. Notable progress in this was obtained by Lackenby [9], who proved that finitely presented residually p-groups with $\mathrm{RG}_p(G) > 0$ are large (meaning that a finite index subgroup has a free nonabelian homomorphic image). However, Osin [10] and Schlage-Puchta [11] constructed residually finite torsion groups with positive rank gradient, showing that the finite presentability condition in Lackenby's theorem cannot be omitted, and indeed the connection with free groups is not true in general.

In this paper we will focus on profinite groups, where the relationship between positive rank gradient and free groups is more compelling. Our main result is the following.

Theorem 1.1. *Let G be a finitely generated profinite group with positive rank gradient. Then G does not satisfy a nontrivial group law.*

A key ingredient in the proof is the following result of Dalla Volta and Lucchini [7]: the minimal size of a generating set of a finite group G registers in some quotient $\bar{G}$ which is a *crown-based power*, see Theorem 2.8 below.

Theorem 1.1 is related to the following question of A. Thom.

Question 1.2 (A. Thom). *Let Γ be a residually finite non-amenable group. Must the profinite completion $\hat{\Gamma}$ of Γ contain a nonabelian free group?*

A positive answer to Question 1.2 implies Theorem 1.1, since a dense finitely generated subgroup Γ of G must be non-amenable (see Theorem 5 in [1] or Theorem 3 in [2]). Therefore, if $\hat{\Gamma}$ contains a free group, then Γ (and hence G) cannot satisfy a non-trivial group law.

A positive answer to Question 1.2 will also imply the following.

Conjecture 1.3. *Let Γ be a finitely generated residually finite group which satisfies a non-trivial group law. Then* $\mathrm{RG}(\Gamma) = 0$.

While we could not prove this conjecture, Theorem 1.1 implies the following weaker result.

Corollary 1.4. *Let Γ be a finitely generated residually finite group which satisfies a non-trivial group law. Then*

$$\inf\left\{\frac{d(\Delta^{\mathrm{ab}})-1}{|\Gamma:\Delta|}\;\middle|\;\Delta <_f \Gamma\right\} = 0,$$

where $\Gamma^{\mathrm{ab}} = \Gamma/[\Gamma,\Gamma]$ denotes the abelianization of Γ and the infimum is taken over all subgroups Δ of finite index in Γ.

Indeed, let $G = \hat{\Gamma}$ be the profinite completion of Γ. Since G satisfies the group laws of Γ, Theorem 1.1 gives $\mathrm{RG}(G) = 0$. In particular,

$$\frac{d(G_i)-1}{|G:G_i|} \to 0$$

for some sequence of open subgroups G_i of G. Let $\Gamma_i = \Gamma \cap G_i$ and observe that G_i is the profinite completion of Γ_i, hence $d(\Gamma_i^{\mathrm{ab}}) = d((\hat{\Gamma}_i)^{\mathrm{ab}}) \le d(G_i)$. Corollary 1.4 follows.

Question 1.2 has the following profinite version.

Question 1.5. *Must a profinite group with positive rank gradient contain a nonabelian free subgroup?*

A *coset identity* on a group G is a nontrivial group word $w(x_1,\dots,x_k)$ in k letters, a normal subgroup H of finite index in G, and k cosets $g_1H,\dots,g_kH$ from G/H, such that $w(g_1h_1,\dots,g_kh_k) = 1$ for all $h_1,\dots,h_k \in H$. In case G is a profinite group, we also require that H is open in G.

An affirmative answer to Question 1.5 will follow if one can prove that a finitely generated profinite group with positive rank gradient does not satisfy a coset identity. While the author believes that this is true, the method of proof of Theorem 1.1 does not give it. We will prove the following.

Theorem 1.6. *Let G be a finitely generated profinite group which satisfies a coset identity of length m. Assume that $d(G) > 6m$. Then G has an open normal subgroup H with*

$$\frac{d(H)-1}{|G:H|} < \alpha\,(d(G)-1),$$

where $\alpha = (2m-1)/(2m)$.

Theorem 1.1 is easily deduced by repeated applications of Theorem 1.6. We cannot use the same method to answer Question 1.5 because, unlike group laws, coset identities may not induce coset identities on subgroups.

We prove an affirmative answer to Question 1.5 in the case of pro-p groups.

Theorem 1.7. *Let G be a finitely generated pro-p group with positive rank gradient. Then G contains a dense non-abelian free subgroup.*

The proof of Theorem 1.7 is much shorter than the proof of Theorem 1.1. It relies on an application of Schlage-Puchta's result [11], together with Lie algebra methods originally developed by Wilson and Zelmanov [12] to study Golod–Shafarevich groups, as well as Zelmanov's results [13] on Lie algebras with identities.

2. Proofs

All modules in the paper will be left modules, and to be consistent, we will write group actions on the left as well. This applies in particular to conjugation: for two elements a, b of a group G we write ${}^{a}b := aba^{-1}$. For sets X and Y, we write $X \backslash Y$ for the elements of X outside Y. By way of contrast, $G/H := \{xH \mid x \in G\}$ will denote the left cosets of a subgroup H of a group G.

2.1. Proof of Theorem 1.7

Recall the following useful result of Levai and Pyber. We add a proof of it for completeness.

Proposition 2.1 (Levai–Pyber, 1998). *A pro-p group G contains no dense non-abelian free subgroups if and only if G satisfies a coset identity.*

Proof. A coset identity of G induces a coset identity on its dense subgroups. Therefore, if G satisfies a coset identity, G has no dense non-abelian free subgroups.

Conversely, suppose G has no dense non-abelian free subgroups. Let $g_1, \dots, g_k$ be a topological generating set of G; without loss of generality we can take $k \geq 2$. Let $Y = (g_1\Phi(G)) \times \cdots \times (g_k\Phi(G))$. Then Y is a closed and open subset of $G^k = G \times \cdots \times G$ (k times). Note than any tuple $\mathbf{y} = (y_1, \dots, y_k) \in Y$ generates a dense subgroup $\Gamma_{\mathbf{y}} := \langle y_1, \dots, y_k \rangle$ of G. Since $\Gamma_{\mathbf{y}}$ is not a free group, there is a reduced word $w \neq 1$ in the free group F_k on k letters such that $w(y_1, \dots, y_k) = 1$.

It follows that $Y = \cup_{w \in F_k \backslash \{1\}} Z_w$, where

$$Z_w = \{\mathbf{y} = (y_1, \dots, y_k) \in Y \mid w(y_1, \dots, y_k) = 1\}.$$

Each Z_w is a closed subset of Y. Since Y is compact, Hausdorff and a union of countably many closed sets Z_w, the Baire category theorem implies that some Z_{w_0} contains a nonempty open set. The base of the topology of G is given by cosets of open normal subgroups. Therefore there are some open normal subgroup H of G and cosets $u_1H, \dots, u_kH$ such that $(u_1H) \times \cdots \times (u_kH) \subseteq Z_{w_0}$. This means $w_0(u_1H, \dots, u_kH) = 1$, and so G satisfies a coset identity. ∎

For a group Γ and a prime p, we recall $(D_n(\Gamma))_{n=1}^{\infty}$, the Zassenhaus filtration of Γ, defined by $D_n(\Gamma) = \{g \in \Gamma \mid g - 1 \in I^n\}$, where I is the augmentation ideal of the group algebra $\mathbb{F}_p\Gamma$. The Lie algebra $\mathcal{L}_p(\Gamma)$ is defined as

$$\mathcal{L}_p(\Gamma) = \bigoplus_{i=0}^{\infty} \frac{D_i(\Gamma)}{D_{i+1}(\Gamma)}$$

with Lie bracket $[gD_{i+1}(\Gamma), g'D_{j+1}(\Gamma)] = [g, g']D_{i+j+1}(\Gamma)$ for all $g \in D_i(\Gamma)$ and $g' \in D_j(\Gamma)$. The following was proved in [12].

Theorem 2.2. *Let Γ be a residually finite p-group which satisfies a coset identity. Then $\mathcal{L}_p(\Gamma)$ satisfies a Lie algebra identity.*

We shall need the following variation of a result of Schlage-Puchta proved in [11] in the case when Γ is a free group.

Theorem 2.3. *Let p be a prime integer and let Γ be a finitely generated group with an infinite chain $\Gamma > \Gamma_1 > \cdots$ of normal subgroups of p-power index in Γ. Let*

$$\hat{\Gamma} = \varprojlim(\Gamma/\Gamma_i)$$

be the completion of Γ with respect to (Γ_i) and assume that $\mathrm{RG}_p(\hat{\Gamma}) > 0$. Then Γ has a quotient Δ with a chain (Δ_i) such that $\mathrm{RG}_p(\Delta, (\Delta_i)) > 0$ and Δ is an infinite residually finite p-torsion group.

This theorem can be deduced easily from the results in [11], and for completeness we give a proof of it in the next subsection. We continue with the proof of Theorem 1.7. Suppose that the claimed result is false and that G is a pro-p group which is a counterexample. By Proposition 2.1, G satisfies a coset identity. Let (G_n) be a chain of normal subgroups with trivial intersection in G. We choose a finitely generated dense subgroup Γ inside G and let $\Gamma_i = G_i \cap \Gamma$. For each $i \in \mathbb{N}$ we have $G/G_i \simeq \Gamma/\Gamma_i$, and therefore the profinite completion of Γ with respect to (Γ_i) is G.

Since $\mathrm{RG}_p(G) > 0$, Theorem 2.3 implies that Γ has an infinite p-torsion quotient Δ. On the other hand, since G satisfies a coset identity, then so does Γ and its quotient Δ. Therefore by Theorem 2.2, $\mathcal{L}_p(\Delta)$ satisfies a Lie algebra identity. In addition, every homogeneous element of $\mathcal{L}_p(\Delta)$ is ad-nilpotent since Δ is p-torsion. By Theorem 1.1 of [13], the Lie algebra $\mathcal{L}_p(\Delta)$ is finite dimensional and hence Δ must be finite, a contradiction. Theorem 1.7 follows. ■

2.2. Proof of Theorem 2.3

Let F be a nonabelian free group and let $g \in F\backslash\{1\}$. We define $\nu_F(g)$ as the largest integer $k \geq 0$ such that $g = h^{p^k}$ for some $h \in F$. For completeness, we set $\nu_F(1) = \infty$.

For a subset $X \subseteq F$, define

$$\delta_F(X) = \sum_{g \in X} p^{-\nu_F(g)},$$

with the convention that $\delta_F(X) = \infty$ if the above sum diverges.

Observe that if $g \in X$ with $\nu_F(g) \geq 1$, then $g \in F^p \leq \Phi(F)$, where $\Phi(F) = F^p[F,F]$ is the p-Frattini subgroup of F. In particular, $p^{-\nu_F(g)} = 1$ for every $g \in X\backslash\Phi(F)$, giving

$$|X\backslash\Phi(F)| \leq \delta_F(X). \tag{2.1}$$

The following technical result is proved in [11] as part of the proof of Theorem 2 there.

Lemma 2.4. *Let F be a nonabelian free group and let $N = \langle {}^F X\rangle \leq F$ be a subgroup which is the normal closure in F of a set X. Let H be a subnormal subgroup of F with $H \geq N$ and $|F : H| = p^n$ for some $n \in \mathbb{N}$. Then N contains a subset $Y \subseteq {}^F X$ such that $N = \langle {}^H Y\rangle$ is the normal closure of Y in H and $\delta_H(Y) \leq |F : H| \cdot \delta_F(X)$.*

We are now ready to prove Theorem 2.3. Adopt the notation and hypothesis of the theorem and let $\varepsilon = \mathrm{RG}_p(\hat{\Gamma})$. Let F be a free group projecting onto Γ. Without loss of generality we may assume that $\Gamma = F/M$, where M is a normal subgroup of F. Let F_i be the normal subgroups of F such that $\Gamma_i = F_i/M$. We define the open subgroups of F to be the preimages of the open subgroups of $\hat{\Gamma}$ under the composition $F \to \Gamma \to \hat{\Gamma}$. Specifically, a subgroup H of F is open if H contains some F_i.

Let $w_1, w_2, \ldots$ be an enumeration of the elements of $F \backslash \{1\}$, and define

$$X = \{w_1^{p^{m_1}}, w_2^{p^{m_2}}, \ldots\},$$

where $m_1 < m_2 < \cdots$ is a sequence of integers such that $\sum_{i=1}^{\infty} p^{-m_i} < \varepsilon/2$.

Let $N = \langle {}^F X \rangle$ be the normal closure of X in F, and note that by construction we have that $\delta_F(X) < \varepsilon/2$ and that F/N is a p-torsion group.

Let $\tilde{\Gamma} := F/MN$ and define the open subgroups of $\tilde{\Gamma}$ to be the images of the open subgroups of F, i.e., a subgroup $\tilde{H} = \frac{H}{MN} \leq \tilde{\Gamma}$ is open in $\tilde{\Gamma}$ if H contains some F_i. We will prove the following.

Proposition 2.5. *Let $\tilde{H}$ be an open subgroup of $\tilde{\Gamma}$. Then there is an open subgroup $\tilde{A}$ of $\tilde{\Gamma}$ with $\tilde{H} > \tilde{A} \geq \Phi(\tilde{H})$ and*

$$d_p(\tilde{H}/\tilde{A}) - 1 > \frac{1}{2}\,\varepsilon |\tilde{\Gamma} : \tilde{H}|.$$

Proof. Let $n = |\tilde{\Gamma} : \tilde{H}|$ and let $\tilde{H} = H/NM$, where $H \geq NM$ is an open subgroup of F with $|F : H| = n$. Denote by L the closure of $H/M \leq \Gamma$ inside $\hat{\Gamma}$; this is an open subgroup of $\hat{\Gamma}$ of index n. Since $\mathrm{RG}_p(\Gamma) = \varepsilon$, we have $(d_p(L) - 1)/n \geq \varepsilon$.

We have $d_p(L) = \dim_{\mathbb{F}_p}(L/\Phi(L))$, where the Frattini subgroup $\Phi(L)$ is an open subgroup of L and of $\hat{\Gamma}$.

Let $B/M = \Phi(L) \cap \Gamma$. Thus B is an open subgroup of F with $H \geq B \geq \Phi(H)M$ and $d_p(H/B) = \dim_{\mathbb{F}_p}(L/\Phi(L)) \geq 1 + \varepsilon n$.

By Lemma 2.4 applied to $N = \langle {}^F X \rangle$ and the open subgroup $H \geq N$, we deduce that $N = \langle {}^H Y \rangle$ is the normal closure in H of a set Y with $\delta_H(Y) \leq |F : H| \cdot \delta_F(X) < \varepsilon n/2$. Let $A = NB$, since $A \geq B$ this is an open subgroup of F and so $\tilde{A} = A/MN$ is an open subgroup of $\tilde{\Gamma}$. We have $H \geq A \geq \Phi(H)MN$ and hence $\tilde{H} \geq \tilde{A} \geq \Phi(\tilde{H})$. Let Y_0 be the subset of Y outside $\Phi(H)$. By (2.1), we have $|Y_0| \leq \delta_H(Y) < \varepsilon n/2$. Since H/B is an elementary abelian p-group, we have $A = NB = \langle Y_0 \rangle B$ and

$$d_p(\tilde{H}/\tilde{A}) = \dim_{\mathbb{F}_p} \frac{H}{A} \geq \dim_{\mathbb{F}_p} \frac{H}{B} - |Y_0| > 1 + \varepsilon n - \frac{\varepsilon n}{2} = 1 + \frac{\varepsilon n}{2} \cdot$$

Observe that since $d_p(\tilde{H}/\tilde{A}) > 1$, it follows that $\tilde{H} > \tilde{A}$. Proposition 2.5 follows. ■

We can apply Proposition 2.5 successively to find a sequence $\tilde{\Gamma}_1 = \tilde{\Gamma} > \tilde{\Gamma}_2 > \cdots$ of open subgroups of $\tilde{\Gamma}$ such that $\tilde{\Gamma}_i > \tilde{\Gamma}_{i+1} \geq \Phi(\tilde{\Gamma}_i)$ and

$$\frac{d_p(\tilde{\Gamma}_i/\tilde{\Gamma}_{i+1}) - 1}{|\tilde{\Gamma} : \tilde{\Gamma}_i|} > \frac{\varepsilon}{2}$$

for all $i \in \mathbb{N}$. Noting that $\tilde{\Gamma}$ is a p-torsion group, Theorem 2.3 follows by setting $\Lambda = \tilde{\Gamma}/U$ and $\Lambda_i = \tilde{\Gamma}_i/U$, where $U = \cap_{i=1}^{\infty} \tilde{\Gamma}_i$. ■

2.3. Proof of Theorem 1.1

Suppose G satisfies a non-trivial group law of length m. We will show that $\mathrm{RG}(G) = 0$. This is clear if G has a subsequence of subgroups $(G_i)_{i=1}^{\infty}$ such that $d(G_i)$ is bounded and $|G:G_i| \to \infty$. Therefore we may assume that $d(H) \to \infty$ as H ranges over all open subgroups of G and $|G:H| \to \infty$. In particular, there is an open subgroup $G_0 \leq G$ such that $d(H) > 6m$ for all open subgroups $H \leq G_0$. Since $\mathrm{RG}(G_0) = |G:G_0| \cdot \mathrm{RG}(G)$, it is sufficient to show $\mathrm{RG}(G_0) = 0$. Hence by replacing G with G_0 we may assume that $d(H) > 6m$ for any open subgroup H of G.

Since a group law is also a coset identity of G, Theorem 1.6 gives that G has an open normal subgroup H with $\frac{d(H)-1}{|G:H|} < \alpha(d(G)-1)$, where $\alpha = (2m-1)/(2m)$.

By replacing G with H and iterating Theorem 1.6 n times, we obtain a sequence of open subgroups $H_n < H_{n-1} < \cdots < H_1 < H_0 = G$ such that $\frac{d(H_i)-1}{|H_{i-1}:H_i|} < \alpha(d(H_i)-1)$ for each i, giving that $\frac{d(H_n)-1}{|G:H_n|} < \alpha^n d(G)$. Since $\alpha < 1$, by letting $n \to \infty$, we obtain $\mathrm{RG}(G) \leq \mathrm{RG}(G,(H_i)) = 0$.

2.4. Proof of Theorem 1.6

Without loss of generality, we may assume that the length m of the coset identity on G is minimal possible. Let $F(X)$ be the free group on $X = \{x_1, \ldots, x_k\}$. Let $w(x_1, \ldots, x_k) \in F(X)$ be a reduced group word of minimal length m which is a coset identity on G. Thus there are an open normal subgroup H of G and elements $g_1, \ldots, g_k \in G$ such that $w(g_1H, \ldots, g_kH) = 1$.

Let $w(x_1, \ldots, x_k) = w_1 w_2 \cdots w_m$, where $w_i = x_{t_i}^{\varepsilon_i}$ for $i = 1, \ldots, m$, with $\varepsilon_i \in \{\pm 1\}$ and $x_{t_i} \in X$. Put $u_j = w_1 \ldots, w_j$ for $j = 1, \ldots, m$. We will refer to u_j as the initial subwords of w. Without loss of generality, we may assume $t_1 = \varepsilon_1 = 1$ so that $u_1 = w_1 = x_1$. Moreover, $w_m \neq w_1^{-1} = x_1^{-1}$, otherwise w will be conjugate to the shorter identity $w_2 \cdots w_{m-1}$.

We claim that by passing to a G-normal subgroup of H and replacing g_i with appropriate elements from $g_j H$, we may assume that the evaluations of the initial subwords $h_j := u_j(g_1, \ldots, g_k)$ are non-trivial for $j = 1, 2, \ldots, m-1$.

Indeed, suppose that we have obtained that $h_1, \ldots, h_{r-1} \neq 1$ for some $r < m$. Now replace H with a smaller open normal subgroup of G such that $h_j \notin H$ for $j = 1, \ldots, r-1$. For any choice of $x_i \in H$ $(i = 1, \ldots, k)$, we have $u_j(g_1x_1, \ldots, g_kx_k) \equiv h_j \bmod H$ and in particular $u_j(g_1x_1, \ldots, g_kx_k) \neq 1$ for $j = 1, \ldots, r-1$. As $r < m$, by the minimality of m, the word u_r is not a coset identity of G and therefore we can find elements $x_i \in H$ with $u_r(g_1x_1, \ldots, g_kx_k) \neq 1$. Replace g_i with g_ix_i and we have achieved $h_j \neq 1$ for $j = 1, \ldots, r$.

Repeating this procedure, increasing r one at a time, we obtain that $h_1, \ldots, h_{m-1} \neq 1$, proving the claim.

Next, by replacing H with a smaller open normal subgroup of G, we may assume that $h_j \notin H$ for $j = 1, 2, \ldots, m-1$.

Choose an element $y \in H$ and write $w(yg_1, g_2, \ldots, g_k) = u \cdot w(g_1, \ldots, g_k)$, where $u = u(y) \in H$ can be written as a product of several conjugates of $y^{\pm 1}$:

$$u(y) = y \cdot {}^{b_1}y^{e_1} \cdots {}^{b_s}y^{e_s}.$$

Here $s \geq 0$ is the number of occurrences of $x_1^{\pm 1}$ among the $w_2, \ldots, w_m$, $e_i \in \{\pm 1\}$, and $(b_1, \ldots, b_s)$ is a subsequence of $(h_1, \ldots, h_{m-1})$. Notice that we use the fact that $w_m \neq x_1^{-1}$ here to remove the possibility that the last b_s could end up equal to $h_m = w(g_1, \ldots, g_k) = 1$. Since H is normal in G and $y \in H$, we have $yg_1 \in g_1 H$ and therefore $w(yg_1, g_2, \ldots, g_k) = w(g_1, g_2, \ldots, g_k) = 1$. We conclude that $u(y) = 1$ for all $y \in H$.

We now arrive at the main technical result of this paper.

Theorem 2.6. *Let G be a profinite group with an open normal subgroup H and consider elements $b_1, \ldots, b_s \in G \backslash H$. Let $e_i \in \{\pm 1\}$ for $i = 1, \ldots, s$. For any $y \in H$, define $u(y) = y \cdot {}^{b_1}y^{e_1} \cdots {}^{b_s}y^{e_s}$ and assume $u(y) = 1$ for all $y \in H$. Assume that $d(G) > 6s + 6$. Then*

$$\frac{d(H) - 1}{|G:H|} < \alpha(d(G) - 1),$$

where $\alpha = \alpha(s) = (2s + 1)/(2s + 2)$.

Since $s \leq m - 1$, we have $\alpha(s) \leq (2m - 1)/(2m)$, and Theorem 1.6 follows from Theorem 2.6 and the above discussion.

Note that if $s = 0$ then $u(y) = y$, which implies that $H = \{1\}$ and the claimed inequality holds trivially. Therefore without loss of generality we may assume that $s \geq 1$ (and hence $H \neq G$) in the rest of the argument.

For a profinite group H, the minimal number of generators $d(H)$ is the minimum of $d(\bar{H})$ for all finite topological images $\bar{H}$ of H. Hence in order to prove Theorem 2.6 we may assume that H and G are finite groups. We shall also need more information on the minimal quotients of H which realize $d(H)$ and the notion of a *crown-based power*.

2.5. Crown-based powers

Let L be a non-cyclic finite group with a unique minimal normal subgroup N. If N is abelian, then we also require that N has a complement in L. For $k \geq 2$, the crown-based power L_k of L is defined as

$$L_k = \{(a_1, \ldots, a_k) \in L^k \mid a_1 N = a_2 N = \cdots = a_k N\},$$

where $L^k = L \times L \times \cdots \times L$ (k times). For later use, we define the projections

$$t_i : L_k \to L, \quad t_i(a_1, \ldots, a_k) = a_i, \quad \forall (a_1, \ldots, a_k) \in L_k,\ i = 1, \ldots, k, \tag{2.2}$$

and note that $t_1(x) \equiv \cdots \equiv t_k(x) \bmod N$ for every $x \in L_k$.

The precise relationship between $d(L_k)$ and the integer k is established in the following theorem from [5]. When N is nonabelian, by $P_{L,N}(d)$ we denote the probability that d random elements of L generate it, provided they generate L/N. By Theorem 1.1 of [7], we have $53/90 \leq P_{L,N}(d) \leq 1$.

When N is abelian, then N is a simple faithful L/N-module and we denote $E = \mathrm{End}_{L/N}(N)$, a finite field.

Theorem 2.7 ([5], Theorem 2.7). *Let L_k be a crown-based power of L and choose an integer $d \geq d(L)$. Then $d(L_k) \leq d$ if and only if one of the following holds:*

1. *The group N is abelian and $k \leq (d - 1) \dim_E N - \dim_E H^1(L/N, N)$.*
2. *The group N is nonabelian and $k \leq P_{L,N}(d)|N|^d / |C_{\mathrm{Aut}(N)}(L/N)|$.*

Crown-based powers are the minimal among the d-generated finite groups in the following sense.

Theorem 2.8 ([5], Theorem 1.4). *Let H be a finite group with $d(H) = d > 2$. Then H has a normal subgroup $M < H$ such that H/M is isomorphic to some crown-based power L_k as above with $d(L_k) = d > d(L)$.*

Before we start the proof of Theorem 2.6, we recall some standard notation. Let A be a group with a (left) action of a group H on A by automorphisms. By a H-chief factor of A we mean a section Y/X, where X and Y are normal H-invariant subgroups of A such that there are no H-invariant normal subgroups Z of A with $X < Z < Y$. Further, we say that two H-groups A and B are H-isomorphic if there is a group isomorphism $\pi\colon A \to B$ which is compatible with the action of H, i.e., $h \cdot \pi(a) = \pi(h \cdot a)$ for all $h \in H$ and $a \in A$.

When $A = H$ and the action of H is given by conjugation, we shall refer to the H-chief factors of H as the *chief factors* of H. We will need two additional technical results.

Proposition 2.9. *Let H be a finite group with a normal subgroup U. Let $K_i \leq U$ be k distinct normal subgroups of H such that U/K_i is a chief factor of H for $i = 1, \dots, k$. Then* (C1) $\Rightarrow$ (C2) $\Rightarrow$ (C3) *below.*

(C1) *Each U/K_i is non-abelian.*

(C2) *For each $i = 1, 2, \dots, k$, we have $K_i \not\geq \cap_{j \neq i} K_j$.*

(C3) *The diagonal homomorphism $U \to \prod_{i=1}^k (U/K_i)$ induces an isomorphism*

$$\frac{U}{\cap_i K_i} \to \prod_{i=1}^{k} \frac{U}{K_i}.$$

Proof. We will first show that (C2) implies (C3). Let R be the intersection of $K_2, \dots, K_k$. By assumption $K_1 \not\geq R$ and hence $K_1 < K_1 R = U$, by the maximality of K_1 in U. Therefore

$$\frac{U}{\cap_{i=1}^k K_i} = \frac{U}{K_1 \cap R} \simeq \frac{U}{K_1} \times \frac{U}{R}.$$

The subset $K_2, \dots, K_k$ satisfies (C2) as well, and hence the conclusion follows by induction on k.

Next we show that (C1) implies (C2). Indeed, suppose that K_1 contains $\cap_{i=2}^k K_i$ and choose a subset $X \subseteq \{K_2, \dots, K_k\}$ minimal with respect to $K_1 \geq \cap_{K_i \in X} K_i$. Then X satisfies (C2), and therefore the diagonal homomorphism induces an isomorphism

$$\frac{U}{\bigcap_{K_i \in X} K_i} \to \prod_{K_i \in X} \frac{U}{K_i}.$$

Let $\bar{K}$ be the image of $K_1/(\cap_{K_i \in X} K_i)$ in $\prod_{K_i \in X}(U/K_i)$. Since $K_1 K_i = U$ for each $K_i \in X$, we have that $\bar{K}$ projects onto each direct factor U/K_i of $\prod_{K_i \in X}(U/K_i)$. In particular, since $\bar{K}$ is a normal subgroup, it follows that

$$\bar{K} \geq [\bar{K}, (U/K_i)] = [(U/K_i), (U/K_i)] = U/K_i$$

for each $K_i \in X$, since U/K_i is perfect being a nonabelian chief factor of H.

Therefore $\bar{K} = \prod_{K_i \in X}(U/K_i)$ giving $K_1 = U$, contradiction. Hence (C1) implies (C2) as claimed. ∎

We will also need the following result which detects crown-based powers.

Proposition 2.10. *Let L be a noncyclic finite group with a unique minimal normal subgroup N. If N is abelian, assume additionally that N is complemented in L. Let H be a finite group with a normal subgroup U. Let $K_i \le U$ for $i = 1, \dots, k$ be pairwise distinct normal subgroups of H together with an isomorphism $\alpha\colon H/K_1 \to L$ such that $\alpha(U/K_1) = N$.*

Assume that for each $i = 1, 2 \dots, k$, there is an isomorphism $\beta_i\colon H/K_i \to H/K_1$ such that $\beta_i(hU/K_i) = hU/K_1$ for all $h \in H$.

Then $H/(\cap_{i=1}^k K_i)$ is isomorphic to a crown-based power $L_{k'}$ for some $k' \le k$. Moreover, if N is non-abelian, then $k' = k$.

Proof. If there is some $i \in \{1, \dots, k\}$ such that $K_i \ge \cap_{j \ne i} K_j$, then we can omit K_i from our list of normal subgroups and the statement to be proved remains unaffected. Therefore we may assume that each K_i does not contain the intersection of the rest of the K_j. By Proposition 2.9, this is automatically the case if N is non-abelian.

For each $i = 1, \dots, k$, let $\tilde{\beta}_i\colon H \to L$ be the composition $\tilde{\beta}_i(h) = \alpha \circ \beta_i(hK_i)$ with the kernel K_i, and note that

$$\tilde{\beta}_1(h)N = \tilde{\beta}_2(h)N = \cdots = \tilde{\beta}_k(h)N, \quad \forall h \in H. \tag{2.3}$$

Consider the map $\delta\colon H \to L^k$ defined by $\delta(h) = (\tilde{\beta}_1(h), \dots, \tilde{\beta}_k(h))$ for all $h \in H$ and note that $\ker \delta = \cap_i K_i$. Moreover, the image of δ is a subgroup of L_k by (2.3) above.

By Proposition 2.9, we have $U/(\cap K_i) \simeq \prod_i (U/K_i)$ since condition (C2) holds. Comparing sizes of $H/(\cap_i K_i)$ and L_k, we deduce that $\delta(H) = L_k$, as required. ∎

2.6. Proof of Theorem 2.6: Reduction

Suppose first that G has a subgroup N with $N \ge H$ and $d(N) < d(G)$. In particular, $|G:N| \ge 2$. Using the Schreier inequality and the fact that $\alpha(s) > 1/2$, we obtain

$$\frac{d(H)-1}{|G:H|} \le \frac{d(N)-1}{|G:N|} < \frac{d(G)-1}{2} < \alpha(s)(d(G)-1).$$

Theorem 2.6 follows.

From now on we shall assume that

$$d(N) \ge d(G) > 6s + 6 \tag{2.4}$$

for any subgroup of G with $N \ge H$.

In particular, $d(H) \ge d(G) > 2$ and hence Theorem 2.8 applies to H. Let M be the normal subgroup of H provided by Theorem 2.8. So H/M is isomorphic to some crown-based power L_k as above with $d(L_k) = d(H)$.

In this section we will reduce the theorem to proving Proposition 2.15, which assumes that M is normal in G. We will refer to the chief factors of H as H-chief factors.

Let U/M be the socle (i.e., the product of the minimal normal subgroups) of H/M. Thus U is normal in H and U/M is isomorphic to N^k, where each summand N is an H-chief factor.

Let $J = N_G(U)$ and choose representatives $a_1 = 1, a_2, \dots, a_r$ in G for the left cosets G/J of J. Define $U_1 = U, U_2 = {}^{a_2}U, \dots, U_r = {}^{a_r}U$; these are the distinct conjugates of U in G.

We define

$$T_i = \bigcap_{g \in a_i J} {}^{g}M \quad (i = 1, 2, \dots, r).$$

In particular, $T_1 = \cap_{g \in J} {}^{g}M$ is normalized by J and $T_i = {}^{a_i}T_1$. Proposition 2.12 below will show that $T_1, \dots, T_r$ are all distinct and in particular the action of G by conjugation on $U_1, \dots, U_r$ is the same as the action of G on $T_1, \dots, T_r$.

By definition, U_i/T_i is a subdirect product of all the $U_i/{}^{g}M$ with $g \in a_i J$. Moreover, for $g \in a_i J$ we have $H/{}^{g}M \simeq L_k$ with $U_i/{}^{g}M \simeq N^k$. In particular, $U_i/{}^{g}M$ is a direct product of k H-chief factors, each being a g-conjugate of a H-chief factor appearing in U/M.

In particular, when N is abelian, then U_i/T_i is a semisimple H/U_i module, all of whose simple factors are faithful H/U_i-modules.

When N is nonabelian, observe that an element $l \in L \setminus N$ cannot act as an inner automorphism on N, otherwise we get that $C_L(N) \neq \{1\}$, contradicting the uniqueness of the minimal normal subgroup N of L.

We summarise the above discussion in the following result.

Proposition 2.11. *The H-chief factors of U_i/T_i are contained in the union of the H-chief factors of $U_i/{}^{g}M$ for $g \in a_i J$. If C is a H-chief factor of U_i/T_i and $h \in H$ with $h \notin U_i$, then conjugation by h induces a non-inner automorphism of C.*

We define $\mathfrak{U} = \cap_{i=1}^{r} U_i$ and $\mathfrak{T} = \cap_{i=1}^{r} T_i$. Then $\mathfrak{U}$ and $\mathfrak{T}$ are normal subgroups of G, being the intersection of all G-conjugates of U and M, respectively.

Consider the diagonal homomorphism $\mathfrak{f}\colon \mathfrak{U} \to \prod_{i=1}^{r}(U_i/T_i)$ defined, for each $y \in \mathfrak{U}$, by $\mathfrak{f}(y) = (yT_1, \dots, yT_r)$. We have $\ker \mathfrak{f} = \cap_{i=1}^{r} T_i = \mathfrak{T}$.

Proposition 2.12. *The homomorphism $\mathfrak{f}$ is surjective and induces an isomorphism $\mathfrak{U}/\mathfrak{T} \to \prod_{i=1}^{r}(U_i/T_i)$ with the conjugation action of G on $\mathfrak{U}/\mathfrak{T}$ permuting the direct factors U_i/T_i in the same way as G acts on $U_1, \dots, U_r$.*

Proof. The result is trivial if $r = 1$ and so we may assume $r > 1$. In particular, since $U_i \neq U_j$ for $i \neq j$ and $|H : U_i| = |H : U_j|$, it follows that $\mathfrak{U}$ is a proper subgroup of U_i for each $i = 1, 2 \dots, r$.

Claim. $\mathfrak{U}T_i = U_i$ for each $i = 1, 2, \dots, r$.

Assume this for the moment. Therefore $\mathrm{Im}(\mathfrak{f})$ is isomorphic as an H-group to a subdirect product of all U_i/T_i for $i = 1, \dots, r$. Observe that for $i \neq j$ every H-chief factor of U_i/T_i is not H-isomorphic to any H-chief factor of U_j/T_j. Indeed, whenever C is a H-chief factor of U_i/T_i Proposition 2.11 gives that the kernel of the composition $H \to \mathrm{Aut}(C) \to \mathrm{Out}(C)$ is precisely U_i, and the groups U_j and U_j are distinct. This proves that $U_1/T_1, \dots, U_r/T_r$ do not share common H-chief factors. Now the Jordan–Hölder theorem gives that a subdirect product of these is in fact the full direct product.

Therefore $\mathfrak{f}$ is surjective. The preimage of the direct factor U_i/T_i under $\mathfrak{f}$ is $\mathfrak{U} \cap (\cap_{j \neq i} T_j)$. In particular, the groups $T_1, \dots, T_r$ are pairwise distinct. Thus the conjugation action of G on $U_1, \dots, U_r$ is the same as the conjugation action of G on $T_1, \dots, T_r$, in turn this is the same as the conjugation action of G on the $r-1$ element subsets of $\{T_1, \dots, T_r\}$ and this results in the same action of G on the direct factors of $\prod_{i=1}^r (U_i/T_i)$.

Proposition 2.12 follows once we prove the claim above.

Proof of Claim. Suppose $\mathfrak{U}T_i < U_i$ and choose a subset $X \subseteq \{U_1, \dots, U_r\}$ of minimal size subject to $\cap_{U_j \in X} U_j = \mathfrak{U}$. Since G acts transitively by conjugation on the $U_1, \dots, U_r$, we may assume that $U_i \in X$. Since $r > 1$ and $\mathfrak{U} \neq U_i$, we must have $|X| > 1$. Let R be the intersection of all members of $X \backslash \{U_i\}$, thus R is a normal subgroup of H such that $\mathfrak{U} = U_i \cap R$. By the minimality of X, we have $U_i \not\supseteq R$ and we choose $h \in R \backslash U_i$. Now $[U_i, R] \leq U_i \cap R = \mathfrak{U}$ and therefore R acts trivially by conjugation on $Q = U_i/\mathfrak{U}T_i$. In particular, h centralizes every H-chief factor of Q and those are a subset of the H-chief factors in U_i/T_i. This contradicts Proposition 2.11 since we chose $h \notin U_i$. Hence we must have $U_i = \mathfrak{U}T_i$, and the claim is proved. ■

Returning to the proof of Theorem 2.6, choose $y_0 \in U_1$, and let $y \in \mathfrak{U}$ be such that $\mathfrak{f}(y) = (y_0 T_1, 1, 1, \dots, 1) \in \prod_{i=1}^r (U_i/T_i)$.

Recall that conjugation by an element $g \in G$ sends the direct factor U_1/T_1 to a different direct factor U_i/T_i of $\prod_{i=1}^r (U_i/T_i)$, unless $g \in N_G(U) = J$. Let $b_{i_1}, b_{i_2}, \dots, b_{i_t}$ be the subsequence of those elements from $b_1, \dots, b_s$ which lie in J, in the same order.

It follows that $\mathfrak{f}(u(y)) = (u_0(y_0)T_1, *, \dots, *)$, where we write $*$ for coordinates we are not interested in, and

$$u_0(y_0) := y_0 \cdot {}^{b_{i_1}} y_0^{e_{i_1}} \cdots {}^{b_{i_t}} y_0^{e_{i_t}}.$$

Since $u(y) = 1$, we must have $u_0(y_0) \in T_1$ for all $y_0 \in U_1$.

Suppose that we show that $\frac{d(H)-1}{|J:H|} \leq \alpha(t)(d(J)-1)$. Then

$$\frac{d(H)-1}{|G:H|} \leq \frac{\alpha(t)(d(J)-1)|J:H|}{|G:H|} = \alpha(t)\,\frac{d(J)-1}{|G:J|} \leq \alpha(t)\,(d(G)-1), \tag{2.5}$$

where the last inequality follows from Schreier's bound $\frac{d(J)-1}{|G:J|} \leq d(G)-1$. Theorem 2.6 then follows from (2.5), since $t \leq s$ and $\alpha(t) \leq \alpha(s)$.

By (2.4), we may assume that $d(J) > 6s + 6$. Therefore, by replacing G with J and $u(y)$ with $u_0(y)$, we have reduced Theorem 2.6 to the following.

Proposition 2.13. *Let G be a finite group with $d(G) > 6s + 6$ for some integer $s \geq 1$. Let H be a normal subgroup of G, let $b_i \in G \backslash H$ and $e_i \in \{\pm 1\}$ for $i = 1, \dots, s$. Let $M < H$ be a normal subgroup of H such that H/M is isomorphic to a crown based power L_k with $d(L_k) = d(H) > d(L)$. Let $U/M = \mathrm{soc}(H/M)$ and assume that U is a normal subgroup of G. Let $T = \cap_{g \in G} {}^g M$ and assume that $u(y) \in T$ for all $y \in U$, where $u(y) = y \cdot {}^{b_1} y^{e_1} \cdots {}^{b_s} y^{e_s}$. Then*

$$\frac{d(H)-1}{|G:H|} < \alpha(s)(d(G)-1),$$

where $\alpha(s) = (2s+1)/(2s+2)$.

From now on, assume that G, H, M, T and u are as in the above proposition. Our next aim is to reduce the proof to the case where M is normal in G, namely Proposition 2.15 below. It will turn out that U/T is a direct product of crown based powers of L, but these may be larger than $H/M \simeq L_k$. More precisely, we have the following.

Proposition 2.14. *There is a normal subgroup R of H with $R \leq M$ such that*

(1) *we have $H/R \simeq L_{k'}$ with $k' \geq k$,*

(2) *if $R = R_1, R_2, \ldots, R_l$ are the distinct conjugates of R in G, then*

$$T = R_1 \cap \cdots \cap R_l$$

and the diagonal homomorphism $f: U \to \prod_{i=1}^{l}(U/R_i)$ induces an isomorphism

$$\frac{U}{T} \to \prod_{i=1}^{l}(U/R_i). \tag{2.6}$$

Under this isomorphism, the conjugation action of G on U/T permutes the direct factors U/R_i of $\prod_{i=1}^{l}(U/R_i)$ in the same way as G permutes $R_1, \ldots, R_l$.

Proof. We fix a surjection $\pi: H \to L_k$ with $\pi(U) = N^k$ and $\ker \pi = M$.

For $i = 1, \ldots, k$, let $K_i = \ker(t_i \circ \pi)$, where $t_i: L_k \to L$ is the projection defined in (2.2). It follows that each K_i is a normal subgroup of H such that $\cap_{i=1}^{k} K_i = M$. From the definition of L_k, we have that t_i is surjective onto L and $U = (t_i \circ \pi)^{-1}(N)$, therefore $K_i < U$, $H/K_i \simeq L$ and $U/K_i \simeq N$ is a chief factor of H. Let $\beta_i: H/K_i \to L$ be the isomorphism induced by $t_i \circ \pi$, that is, $\beta_i(hK_i) := t_i(\pi(h))$ for all $h \in H$. For all $1 \leq i, j \leq k$ we have $t_i(l) \equiv t_j(l) \bmod N$ for all $l \in L$. Therefore

$$\beta_i(hK_i) \equiv \beta_j(hK_j) \mod N, \quad \forall h \in H. \tag{2.7}$$

Let $Y := \{{}^g K_i \mid g \in G,\ i = 1, \ldots, k\}$ and define an equivalence relation $\sim$ on Y as follows.

We say that $K \sim K'$ if there is an isomorphism $\alpha: H/K \to H/K'$ such that α induces the identity on H/U, i.e., $\alpha(hU/K) = hU/K'$ for each $h \in H$.

For $1 \leq i, j \leq k$, we can take $\alpha = \beta_j^{-1} \circ \beta_i: H/K_i \to H/K_j$, which together with (2.7) proves that $K_i \sim K_j$.

We claim that the conjugation action of G on Y preserves $\sim$. Indeed, if $K \sim K'$ with isomorphism α as above, then for any $g \in G$ we have an isomorphism

$$f_{g,K'} \circ \alpha \circ f_{g,K}^{-1}: \ H/({}^g K) \to H/({}^g K'),$$

where $f_{g,K}: H/K \to H/{}^g K$ defined by $f_{g,K}(xK) = {}^g x\, {}^g K$ $(x \in H)$ is the isomorphism induced by the conjugation map on H. Therefore ${}^g K \sim {}^g K'$, and the claim is proved.

Let $E_1, \ldots, E_l$ be the equivalence classes of $\sim$ on Y. We showed that $K_1 \sim K_2 \sim \cdots \sim K_k$, and without loss of generality we may assume $\{K_1, \ldots, K_k\} \subseteq E_1$. Recall that $Y := \{{}^g K_i \mid g \in G,\ i = 1, \ldots, k\}$. It follows that E_1 intersects nontrivially each orbit of G on Y. Therefore the conjugation action of G on Y induces a transitive action of G on the equivalence classes of $\sim$. Let $R_i = \cap_{K \in E_i} K$ and put $R = R_1$. By Proposition 2.10, we have $H/R \simeq L_{k'}$ for some $k' \geq k$ and $R \leq M = \cap_{i=1}^{k} K_i$. Further, $\cap_{i=1}^{l} R_i = \cap_{A \in Y} A = \cap_{g \in G} {}^{g}M = T$, as required.

It remains to prove (2.6). If N is nonabelian, this follows from Proposition 2.9 since, in that case,

$$U/T = U/(\cap_{K \in Y} K) \simeq \prod_{K \in Y} U/K$$

with $U/R_i \simeq \prod_{K \in E_i} U/K$.

When N is abelian and $K \in Y$, then $H/K \simeq L$ is a split extension isomorphic to $(U/K) \rtimes (H/U)$ and in particular, for $K, K' \in Y$, the relation $K \sim K'$ is equivalent to the requirement that the two H/U-modules U/K and U/K' are isomorphic. Therefore, if $i \neq j$, the H-chief factors of U/R_i are not isomorphic (as H-modules) to the H-chief factors of U/R_j. Hence again the Jordan–Hölder theorem implies that $U/(\cap_{i=1}^{l} R_i)$, being a subdirect product of all U/R_i, must in fact be isomorphic to $\prod_{i=1}^{l}(U/R_i)$.

Finally, the preimage $f^{-1}(\{1\} \times \cdots \times U/R_i \times \cdots \times \{1\})$ of the direct factor U/R_i of $\prod_{i=1}^{l}(U/R_i)$ is equal to $\cap_{j \neq i} R_j$ and of course G permutes the $l-1$ element subsets of $\{R_1, \ldots, R_l\}$ in the same way as G permutes $R_1, \ldots, R_l$.

Proposition 2.14 is proved. ∎

Let $R = R_1, R_2, \ldots, R_l$ be the normal subgroups of H from Proposition 2.14. Let $J_1 = N_G(R_1)$ be the normaliser of R_1 in G. Recall the identity $u(y) \equiv 1 \bmod T$ for all $y \in U$, where $u(y) = y \cdot {}^{b_1}y^{e_1} \cdots {}^{b_s}y^{e_s}$. Let $b_{i_1}, \ldots, b_{i_t}$ be the subsequence of $b_1, \ldots, b_s$ of elements $b_i \in J_1$, and let

$$u_0(y) := y \cdot {}^{b_{i_1}}y^{e_{i_1}} \cdots {}^{b_{i_t}}y^{e_{i_t}}.$$

We will use the diagonal map $f: U \to \prod_{i=1}^{l}(U/R_i)$ from Proposition 2.14, namely $f(y) = (yR_1, \ldots, yR_l)$ for all $y \in U$.

We choose $y_0 \in U$ and let $y \in U$ be an element such that

$$f(y) = (y_0 R_1, 1 \ldots 1) \in \prod_{i=1}^{l}(U/R_i).$$

We have, just as before, $f(u(y)) = (u_0(y_0), *, \ldots, *)$, and therefore $u_0(y_0) \in R_1$ for all $y_0 \in U$.

We have shown that H/R_1 is isomorphic to a crown based power L_{k_1} with $k_1 \geq k$, and in particular $d(L_{k_1}) \geq d(L_k) = d(H)$. Since obviously $d(L_{k_1}) = d(H/R_1) \leq d(H)$, it follows that $d(H/R_1) = d(H)$.

Further, from (2.4) we have $d(J_1) \geq d(G) > 6s + s$.

The inequality (2.5) with J_1 in place of J gives that Proposition 2.13 (and hence Theorem 2.6) will follow if we prove

$$\frac{d(H) - 1}{|J_1 : H|} < \alpha(t) \cdot (d(J_1) - 1).$$

Therefore we can replace G with J_1, M with R_1 and u with u_0, and we are reduced to proving the following result.

Proposition 2.15. *Let G be a finite group with $d(G) > 6s + 6$ for some integer $s \geq 1$. Let H be a normal subgroup of G, let $b_i \in G \backslash H$ and $e_i \in \{\pm 1\}$ for $i = 1, \dots, s$. Let $M < H$ be a normal subgroup of G such that H/M is isomorphic to a crown based power L_k with $d(L_k) = d(H) > d(L)$. Let $U/M = \operatorname{soc}(H/M)$ and assume $u(y) \in M$ for all $y \in U$, where $u(y) = y \cdot {}^{b_1}y^{e_1} \cdots {}^{b_s}y^{e_s}$. Then*

$$\frac{d(H) - 1}{|G:H|} < \alpha(s)(d(G) - 1),$$

where $\alpha(s) = (2s + 1)/(2s + 2)$.

2.7. Proof of Proposition 2.15

Our argument splits into considering two cases.

2.7.1. Case 1: the socle N of L is non-abelian. First we set up notation for the canonical embedding of L in $\operatorname{Aut}(N)$. For $l \in L$, denote by $\theta(l) \in \operatorname{Aut}(N)$ the automorphism $\theta(l)(x) = {}^l x$ $(x \in N)$ given by conjugation by l. Since $C_L(N) = 1$, the map $\theta\colon L \to \operatorname{Aut}(N)$ is a monomorphism. Note that $\theta(N) = \operatorname{Inn}(N)$, the group of inner automorphisms of N. We will denote by $\bar{\theta}\colon L/N \to \theta(L)/\theta(N)$ the induced isomorphism $\bar{\theta}(lN) := \theta(l)\theta(N)$. When there is no possibility of confusion, we identify L/N with $\theta(L)/\theta(N)$, for example we write $C_{\operatorname{Aut}(N)}(L/N)$ below for the centralizer of $\theta(L)/\theta(N)$ in $\operatorname{Aut}(N)$.

We will need a bound for the size of $C_{\operatorname{Aut}(N)}(L/N)$.

Since N is the unique minimal normal subgroup of L, it follows that $N \simeq S^m$, a direct product of m copies of some nonabelian simple group S. Moreover, the conjugation action of L permutes the direct factors of N transitively. Using this it is easy to show that $|C_{\operatorname{Aut}(N)}(L/N)| \leq m|N||\operatorname{Out}(S)|$, see the proof of Lemma 1 of [6]. Now the classification of finite simple groups gives that $|\operatorname{Out}(S)| \leq |S|$, and since $m|S| \leq |S|^m = |N|$, we have

$$|N| \leq |C_{\operatorname{Aut}(N)}(L/N)| \leq |N|^2$$

Let $d = d(G)$ and $d' = d(H) = d(L_k) > d(L)$. Theorem 2.7 together with the estimate for $|C_{\operatorname{Aut}(N)}(L/N)|$ above gives

$$k > P_{L,N}(d' - 1) \frac{|N|^{d'-1}}{|C_{\operatorname{Aut}(N)}(L/N)|} > \frac{1}{2} |N|^{d'-3} \tag{2.8}$$

using the fact that $P_{L,N}(d' - 1) \geq 53/90 > 1/2$ proved in [7].

Fix an isomorphism $\phi\colon H/M \to L_k$ and recall that U/M is the socle of H/M. Therefore $\phi(U/M) = N^k \leq L_k$, a direct product N^k of k copies of N. Let $\pi\colon L^k \to L/N$ be the surjection with kernel N^k. Denote by $\rho\colon H/U \to L/N$ the isomorphism induced by $\pi \circ \phi$, namely $\rho(hU) = \pi \circ \phi(hM)$ for each $h \in H$.

Let us write $N^k = N_1 \times \cdots \times N_k$, where $N_i \simeq N$ are the minimal normal subgroups of L_k, and let $V_i = \phi^{-1}(N_i)$ $(i = 1, \dots, k)$. Then $V_1, \dots, V_k$ are all the minimal normal subgroups of H/M and $U/M = V_1 \times \cdots \times V_k$.

Given a factor V_i of U/M, let P_i/M be its complement in U/M, i.e., we set $P_i/M := \prod_{j \neq i} V_j$ for a normal subgroup $P_i < U$ of H. Define the isomorphism $\eta_i\colon H/P_i \to L$ as

$\eta_i(hP_i) = t_i \circ \phi(hM)$, where $t_i\colon L_k \to L$ is the projection in (2.2). We have $\eta_i(U) = N$. From the definition of L_k it follows that the isomorphism $\bar{\eta}_i\colon H/U \to L/N$ induced by η_i is equal to ρ above.

Choose any $b \in G\backslash H$. Let D be the subgroup of G generated by b and H. Since $\{V_1, \dots, V_k\}$ is the set of the minimal normal subgroups of H/M, any automorphism of H/M permutes these k groups among themselves. In particular, this applies to the action of b by conjugation on H/M.

Proposition 2.16. *The element b normalizes at most $|N|^{d(D)}$ of the groups $V_1, \dots, V_k$.*

Proof. Choose $i \in \{1,\dots,k\}$ and write $V = V_i$ from now on. Let $P = P_i$ and $\eta = \eta_i$ be as above, i.e., P/M is the complement to V in U/M and $\eta\colon H/P \to L$ is the isomorphism associated to the projection $t_i \circ \phi\colon H \to L$.

Suppose that ${}^bV = V$. This is equivalent to ${}^b(P/M) = P/M$, i.e., P is normalized by $D = \langle b, H\rangle$.

The conjugation action of D on U/P together with η induce a homomorphism $f\colon D \to \mathrm{Aut}(N)$ defined by

$$f(g)(x) = \eta({}^g\eta^{-1}(x)) \quad \forall g \in D, \forall x \in N.$$

Note that if $h \in H$, then $f(h)$ is the conjugation by $\eta(hP)$ on N, and therefore $f(h) = \theta(\eta(hP))$. In particular, $f(H) = \theta(L) \le \mathrm{Aut}(N)$ and $f(U) = \theta(N) = \mathrm{Inn}(N)$.

The homomorphism $\bar{f}\colon H/U \to \theta(L)/\theta(N)$ induced by f is given by

$$\bar{f}(hU) := f(h)\theta(N) = \theta(\eta(hP)N)\theta(N) = \bar{\theta}(\eta(hP)N) = \bar{\theta} \circ \bar{\eta}(hU)$$

for all $h \in H$. Therefore $\bar{f} = \bar{\theta} \circ \bar{\eta} = \bar{\theta} \circ \rho$ and does not depend on the choice of $V = V_i$. Observe that f determines P (and hence V) since $P = \ker f \cap H$.

Define the set $\mathfrak{F}$ to consist of all homomorphisms $f\colon D \to \mathrm{Aut}(N)$ such that $f(H) = \theta(L)$, $f(U) = \theta(N) = \mathrm{Inn}(N)$ and $\bar{f} = \bar{\theta} \circ \rho$, where $\bar{f}\colon H/U \to \theta(L)/\theta(N)$ is the isomorphism induced by f.

We summarize the above discussion in the following result.

Proposition 2.17. *The number of direct factors V_i of U/M normalized by b is bounded above by the number of different subgroups $H \cap \ker f$ where $f \in \mathfrak{F}$.*

We will prove that $|\mathfrak{F}| \le |C_{\mathrm{Aut}(N)}(L/N)| \cdot |N|^{d(D)}$.

Let $f \in \mathfrak{F}$ and let $\sigma := f(b) \in \mathrm{Aut}(N)$. We first estimate the possibilities for σ. For $h \in H$ we have

$$\bar{\theta} \circ \rho({}^bhU) = f({}^bh)\,\theta(N) = {}^\sigma f(h)\,\theta(N) = {}^\sigma(\bar{\theta}\,\rho(hU)).$$

Thus the action of σ by conjugation on $\theta(L)/\theta(N)$ is uniquely determined by ρ and the conjugation action of b on H/U. So any two choices σ and σ' for $f(b)$ satisfy that $\sigma^{-1}\sigma'$ centralizes $\theta(L)/\theta(N)$. Hence there are at most $|C_{\mathrm{Aut}(N)}(L/N)| \le |N|^2$ possibilities for $\sigma = f(b)$ in $\mathrm{Aut}(N)$.

Let $Q := f(D) \le \mathrm{Aut}(N)$ be the image of f in $\mathrm{Aut}(N)$. Observe that $Q = \langle \theta(L), \sigma\rangle$ since $D = \langle H, b\rangle$ and $f(H) = \theta(L)$. Therefore σ uniquely determines Q.

The induced map $\tilde{f}\colon D/U \to Q/\theta(N) \leq \mathrm{Out}(N)$, defined by $\tilde{f}(gU) = f(g)\theta(N)$ for all $g \in D$, is also uniquely determined by $\sigma = f(b)$. Indeed, D/U is generated by H/U together with $bU \in G/U$ as a subgroup of G/U. The restriction $\tilde{f}|_{H/U}$ of $\tilde{f}$ to H/U equals $\bar{f} = \bar{\theta} \circ \rho$, while of course $\tilde{f}(bU) = \sigma\theta(N)$ is determined by σ.

Therefore any choice of $\sigma = f(b)$ uniquely determines the group $f(D) = Q \leq \mathrm{Aut}(N)$ and $\tilde{f}\colon D/U \to Q/\theta(N)$.

Next we estimate the possibilities for f given Q and $\tilde{f}$. Let $r = d(D)$ and choose a generating set $g_1, \dots, g_r$ of D. We count how many possibilities are there for the images $f(g_1), \dots, f(g_r)$ in Q. Since $f(g_i)\theta(N) = \tilde{f}(g_i U)$ is a uniquely determined coset of $Q/\theta(N)$, we obtain that there are at most $|N|$ choices for each $f(g_i) \in Q$. Thus for any chosen $\sigma = f(b)$ there at most $|N|^r$ possibilities for f, and hence $|\mathfrak{F}| \leq |C_{\mathrm{Aut}(N)}(L/N)|\,|N|^r$.

Next we define an action of $C_{\mathrm{Aut}(N)}(L/N)$ on $\mathfrak{F}$ by

$$^{\gamma}f(g) := \gamma \circ f(g) \circ \gamma^{-1} \quad \text{for all } f \in \mathfrak{F},\ g \in D,\ \gamma \in C_{\mathrm{Aut}(N)}(L/N).$$

We claim that $C_{\mathrm{Aut}(N)}(L/N)$ acts semi-regularly on $\mathfrak{F}$. Indeed, suppose $f = {}^{\gamma}f$, i.e., $f(g) = \gamma \circ f(g) \circ \gamma^{-1}$ for all $g \in D$. In particular, by letting g range over U and using $f(U) = \theta(N)$, we deduce that $\theta(x) \circ \gamma = \gamma \circ \theta(x)$ for all $x \in N$. This means that ${}^{x}\gamma(y) = \gamma({}^{x}y) = {}^{\gamma(x)}\gamma(y)$ for all $x, y \in N$. Therefore $x^{-1}\gamma(x) \in N$ centralizes all elements of N, and so $x = \gamma(x)$, since N is a nonabelian minimal normal subgroup of L. Thus $\gamma = 1$ and hence the action of $C_{\mathrm{Aut}(N)}(L/N)$ on $\mathfrak{F}$ is indeed semi-regular.

Finally, observe that $\ker f = \ker({}^{\gamma}f)$. Therefore by Proposition 2.17 the number of factors V_i normalized by b is bounded above by the number of orbits of $C_{\mathrm{Aut}(N)}(L/N)$ on $\mathfrak{F}$, which is at most $|N|^r$. Proposition 2.16 follows. ∎

We will apply Proposition 2.16 with $b = b_i \in G \setminus H$ from the statement of Proposition 2.15. Note that $D = \langle H, b \rangle \neq H$.

Recall that $d' = d(H)$ and $d = d(G)$.

We have $r = d(D) \leq (d-1)|G:D| + 1$, and from $D \neq H$ we have $|G:D| \leq \frac{1}{2}|G:H|$, whence $r \leq \frac{1}{2}(d-1)|G:H| + 1$.

Proposition 2.16 gives that each b_i can normalize at most $A := |N|^{|G:H|(d-1)/2+1}$ of the factors V_i of U/M.

Assume, for the sake of contradiction, that $d' = d(H) \geq \frac{3}{4}|G:H|(d-1) + 1$ and recall that $k > \frac{1}{2}|N|^{d'-3}$ from (2.8). Therefore

$$k > \frac{1}{2}|N|^{\frac{3}{4}|G:H|(d-1)-2} = \frac{1}{2}A|N|^{\frac{1}{4}|G:H|(d-1)-3}.$$

Since $|G:H| \geq 2$ and $|N| \geq 60$, we have

$$k > \frac{1}{2}A\,|N|^{(d-1)/2-3} \geq \frac{1}{2}A\,60^{(d-7)/2}.$$

Using that $60^a > a \ln 60 > 4a$ for $a > 0$ and that $d = d(G) > 6s + 6 > s + 7$, we obtain $\frac{1}{2}60^{(d-7)/2} > d - 7 > s$, and hence $k > As$.

It follows that there is a direct factor, say V_1, of $U/M = V_1 \times \cdots \times V_k$ such that ${}^{b_i}V_1 \neq V_1$ for each $i = 1, \dots, s$.

Recall the identity $u(y) = y \cdot {}^{b_1}y^{e_1} \cdots {}^{b_s}y^{e_s} \equiv 1 \bmod M$ for all $y \in U$. Choose $y \in V_1 \backslash \{1\}$. It follows that the projection of $u(y)$ onto V_1 is equal to $y \neq 1$, hence $u(y) \neq 1 \bmod M$, contradiction. Therefore

$$d(H) < \frac{3}{4}|G:H|(d-1)+1$$

and Proposition 2.15 follows since $\alpha(s) \geq 3/4$.

2.7.2. Case 2: the socle N of L is abelian. Let p be the exponent of the abelian group N. Then p is a prime and N is a simple $\mathbb{F}_p(L/N)$-module.

Recall that U/M is the socle of H/M. Thus U is a normal subgroup of G and we define $\Gamma = G/U$ and $\Delta = H/U$. We will consider U/M as a left module for the action of Γ and Δ by conjugation.

Fix an isomorphism $\phi: H/M \to L_k$ with $\phi(U/M) = N^k = \mathrm{soc}(L_k)$. Then ϕ induces an isomorphism $\bar{\phi}: \Delta \to L_k/N^k \simeq L/N$ given by $\bar{\phi}(hU) = \phi(hM)N^k$ for all $h \in H$. From now on we will consider N as $\mathbb{F}_p\Delta$-module via $\bar{\phi}$.

The isomorphism between U/M and $\phi(U/M) = \mathrm{soc}(L_k) = N^k$ gives that U/M is a semisimple $\mathbb{F}_p\Delta$-module which is a direct sum of k isomorphic copies of N.

Let $B \leq U/M$ be any simple $\mathbb{F}_p\Delta$-submodule of U/M. Then B is isomorphic to N. Let $g \in \Gamma$. The submodule $g^{-1}B \leq U/M$ is also a simple $\mathbb{F}_p\Delta$-submodule of U/M and hence is isomorphic to B and N. Let $\sigma: B \to B$ be the linear map such that $x \mapsto g^{-1}\sigma(x)$ is an isomorphism of $\mathbb{F}_p\Delta$-modules between B and $g^{-1}B$. This means that $g^{-1}\sigma(hx) = hg^{-1}\sigma(x)$ for all $x \in B$ and $h \in \Delta$, which is equivalent to $\sigma(hx) = {}^g h \cdot \sigma(x)$. Using that B and N are isomorphic $\mathbb{F}_p\Delta$-modules, we deduce the following.

Proposition 2.18. *Let $g \in \Gamma$. There is a bijective linear map $\sigma = \sigma_g: N \to N$ such that $\sigma(hx) = {}^g h\, \sigma(x)$ for all $x \in N$ and $h \in \Delta$.*

For a $\mathbb{F}_p\Delta$-module A, define

$$\Re_N(A) = \cap\{\ker f \mid f \in \mathrm{Hom}_\Delta(A, N)\},$$

where f ranges over all $\mathbb{F}_p\Delta$-homomorphisms from A to N.

Thus $A/\Re_N(A)$ is the largest semisimple quotient of A whose simple factors are isomorphic to N. Suppose that A is in addition a $\mathbb{F}_p\Gamma$-module with a $\mathbb{F}_p\Delta$-submodule B. Let $f \in \mathrm{Hom}_\Delta(B, N)$ and $g \in \Gamma$. Define ${}^g f: gB \to N$ by ${}^g f(x) := \sigma_g \circ f(g^{-1}x)$ for all $x \in gB$. Note that ${}^g f \in \mathrm{Hom}_\Delta(gB, N)$ and $\ker {}^g f = g \ker f$. Therefore $\Re_N(gB) \leq g\Re_N(B)$, and by reversing the roles of B and gB we get

$$\Re_N(gB) = g\Re_N(B). \tag{2.9}$$

In particular, $\Re_N(A)$ is a $\mathbb{F}_p\Gamma$-submodule of A.

We would need to know more about the action of Γ on U/M.

Let $\mathcal{G}$ be the free group on $d = d(G)$ generators $x_1, \ldots, x_d$ and fix a surjective homomorphism $\pi: F \to G/M$. Let $\mathcal{H}$ and $\mathcal{U}$ be the preimages of H/M and U/M, respectively, and let $\mathcal{M} = \ker \pi$. We will identify $\Gamma = G/U$ and $\Delta = H/U$ with $\mathcal{G}/\mathcal{U}$ and $\mathcal{H}/\mathcal{U}$ via π. Thus the semisimple $\mathbb{F}_p\Gamma$-module U/M is isomorphic to the $\mathbb{F}_p(\mathcal{G}/\mathcal{U})$-module $\mathcal{U}/\mathcal{M}$. In turn, $\mathcal{U}/\mathcal{M}$ is a quotient of the $\mathbb{F}_p\Gamma$-module $\mathcal{U}_p^{\mathrm{ab}} = \mathcal{U}/\mathcal{U}^p[\mathcal{U},\mathcal{U}]$, the mod-$p$ relation module of the presentation

$$1 \to \mathcal{U} \to \mathcal{G} \to \Gamma \to 1.$$

We will denote by $\Phi(\mathcal{U}) = \mathcal{U}^p[\mathcal{U},\mathcal{U}]$ the p-Frattini subgroup of $\mathcal{U}$.

The cellular chain complex of the Cayley graph of Γ with respect to the generators $\pi(x_1),\dots,\pi(x_d)$ gives rise to the exact sequence of $\mathbb{F}_p\Gamma$-modules

$$0 \to \mathcal{U}_p^{\mathrm{ab}} \xrightarrow{\rho} (\mathbb{F}_p\Gamma)^d \to \mathbb{F}_p\Gamma \to \mathbb{F}_p \to 0.$$

The injection $\rho\colon \mathcal{U}_p^{\mathrm{ab}} \to (\mathbb{F}_p\Gamma)^d$ can be described explicitly by

$$\rho(u\Phi(\mathcal{U})) = \Big(\overline{\frac{\partial u}{\partial x_1}},\dots,\overline{\frac{\partial u}{\partial x_d}}\Big), \quad \forall u \in \mathcal{U}. \tag{2.10}$$

Here $\partial u/\partial x_i \in \mathbb{F}_p\mathcal{G}$ is the Fox derivative of u with respect to x_i, and $\bar{y}$ denotes the image of $y \in \mathbb{F}_p\mathcal{G}$ under the reduction $\mathbb{F}_p\mathcal{G} \to \mathbb{F}_p\Gamma$. See [4], §I.5, Proposition (5.4) and Exercise 3 (d) for proofs.

Let $\mathcal{M}_0 = \mathcal{M}/\Phi(\mathcal{U})$ be the image of $\mathcal{M}$ in $\mathcal{U}_p^{\mathrm{ab}}$, thus U/M, $\mathcal{U}/\mathcal{M}$ and $\mathcal{U}_p^{\mathrm{ab}}/\mathcal{M}_0$ are all isomorphic as $\mathbb{F}_p\Gamma$-modules.

The following result can be deduced from the fact that for any $\mathbb{F}_p\Delta$-module S we have

$$H^2(\Delta, S) = \operatorname{Coker}\big(\operatorname{Hom}_\Delta((\mathbb{F}_p\Gamma)^d, S) \to \operatorname{Hom}_\Delta(\mathcal{U}^{\mathrm{ab}}, S)\big)$$

and [4], §IV.2, Exercise 4. For completeness, we give a proof of it in Section 2.8.

Proposition 2.19. *Let $\mathcal{K}$ be a normal subgroup of $\mathcal{H}$ with $\Phi(\mathcal{U}) \le \mathcal{K} \le \mathcal{U}$, and let $S := \mathcal{U}/\mathcal{K}$ considered as $\mathbb{F}_p\Delta$-submodule under conjugation by $\mathcal{H}$. Let $f\colon \mathcal{U}_p^{\mathrm{ab}} \to S$ be the associated epimorphism of $\mathbb{F}_p\Delta$-modules, namely $f(u\Phi(\mathcal{U})) = u\mathcal{K}$ for all $u \in \mathcal{U}$. Then $\mathcal{U}/\mathcal{K}$ has a complement in $\mathcal{H}/\mathcal{K}$ if and only if there is a $\mathbb{F}_p\Delta$-module homomorphism $\theta\colon (\mathbb{F}_p\Gamma)^d \to S$ such that $f = \theta \circ \rho$.*

We claim that $\mathcal{M}$ is an intersection of groups $\mathcal{K}_i \le \mathcal{U}$ for $i = 1,\dots,k$ such that $\mathcal{U}/\mathcal{K}_i$ is $\mathbb{F}_p\Delta$-isomorphic to N and has a complement in $\mathcal{H}/\mathcal{K}_i$. In view of the isomorphisms $\mathcal{H}/\mathcal{M} \to H/M \to L_k$, it is sufficient to prove the corresponding statement for $\{0\}$ in L_k and take preimages. For $i = 1,\dots,k$, let $t_i\colon L_k \to L$ be the projection defined in (2.2). Then $\cap_{i=1}^k \ker t_i = \{0\}$ and $L_k/\ker t_i \simeq L$, which splits over N. This proves the claim.

The groups $\mathcal{K}_i$ satisfy the requirements of Proposition 2.19, hence if $f_i\colon \mathcal{U}_p^{\mathrm{ab}} \to N$ are epimorphisms with $\ker f_i = \mathcal{K}_i/\Phi(\mathcal{U})$, there exist $\mathbb{F}_p\Delta$-epimorphisms $\theta_i\colon (\mathbb{F}_p\Gamma)^d \to N$ such that $f_i = \theta_i \circ \rho$.

Let $Q := \Re_N((\mathbb{F}_p\Gamma)^d)$ and note that Q is a $\mathbb{F}_p\Gamma$ submodule of $(\mathbb{F}_p\Gamma)^d$.

Now we prove $Q \cap \rho(\mathcal{U}_p^{\mathrm{ab}}) \le \rho(\mathcal{M}_0)$. Let $x \in \mathcal{U}_p^{\mathrm{ab}}$ be such that $\rho(x) \in Q$. In particular, $f_i(x) = \theta_i(\rho(x)) = 0$ for $i = 1,\dots,k$ and hence x belongs to

$$\bigcap_{i=1}^k \ker f_i = \bigcap_{i=1}^k \mathcal{K}_i/\Phi(\mathcal{U}) = \mathcal{M}/\Phi(\mathcal{U}) = \mathcal{M}_0.$$

Therefore $Q \cap \rho(\mathcal{U}_p^{\mathrm{ab}}) \leq \rho(\mathcal{M}_0)$, which gives $\rho(\mathcal{U}_p^{\mathrm{ab}}) \cap (\rho(\mathcal{M}_0) + Q) = \rho(\mathcal{M}_0)$. In particular, we have the following isomorphisms of $\mathbb{F}_p\Gamma$ modules:

$$\frac{U}{M} \simeq \frac{\mathcal{U}}{\mathcal{M}} \simeq \frac{\mathcal{U}_p^{\mathrm{ab}}}{\mathcal{M}_0} \simeq \frac{\rho(\mathcal{U}_p^{\mathrm{ab}})}{\rho(\mathcal{M}_0)} \simeq \frac{\rho(\mathcal{U}_p^{\mathrm{ab}}) + Q}{\rho(\mathcal{M}_0) + Q}.$$

Let $\bar{b}_i = b_i U$ be the images of $b_i \in G$ in $\Gamma = G/U$ and let $W := (\mathbb{F}_p\Gamma)^d/Q$. The condition $u(y) \in M$ for all $y \in U$ in Proposition 2.15 is equivalent to

$$(1 + e_1\bar{b}_1 + \cdots + e_s\bar{b}_s)\,\frac{U}{M} = \{0\}.$$

Therefore $1 + e_1\bar{b}_1 + \cdots + e_s\bar{b}_s$ annihilates the sub-quotient $\frac{\rho(\mathcal{U}_p^{\mathrm{ab}})+Q}{\rho(\mathcal{M}_0)+Q}$ of W.

Recall a basic result from linear algebra.

Proposition 2.20. *Let V be a vector space over a field $\mathbb{F}$ and let $T\colon V \to V$ be a linear transformation with a pair $X \geq Y$ of T-invariant subspaces such that $T(X/Y) = \{0\}$, i.e., $T(X) \subseteq Y$. Then* $\dim_{\mathbb{F}} \ker T \geq \dim_{\mathbb{F}} X/Y$.

In particular, we deduce

$$\dim_{\mathbb{F}_p} \ker(1 + e_1\bar{b}_1 + \cdots + e_s\bar{b}_s)|_W \geq \dim_{\mathbb{F}_p} U/M = k \dim_{\mathbb{F}_p} N. \tag{2.11}$$

We now investigate the structure of W. Let $m := |\Gamma : \Delta|$ and choose coset representatives $\gamma_1, \gamma_2, \ldots, \gamma_m$ for Γ/Δ in Γ. We can write $\mathbb{F}_p\Gamma = \oplus_{i=1}^m \gamma_i(\mathbb{F}_p\Delta)$ as a direct sum where each factor $\gamma_i(\mathbb{F}_p\Delta) = (\mathbb{F}_p\Delta)\gamma_i$ is a free $\mathbb{F}_p\Delta$-module. In particular, (2.9) gives

$$\mathfrak{R}_N(\mathbb{F}_p\Gamma) = \bigoplus_{i=1}^m \mathfrak{R}_N(\gamma_i(\mathbb{F}_p\Delta)) = \bigoplus_{i=1}^m \gamma_i\,\mathfrak{R}_N(\mathbb{F}_p\Delta).$$

Therefore

$$W = \frac{(\mathbb{F}_p\Gamma)^d}{\mathfrak{R}_N((\mathbb{F}_p\Gamma)^d)} = \Big(\bigoplus_{i=1}^m \frac{\gamma_i\mathbb{F}_p\Delta}{\gamma_i\,\mathfrak{R}_N(\mathbb{F}_p\Delta)}\Big)^d.$$

Let $V_i = \big(\frac{\gamma_i\mathbb{F}_p\Delta}{\gamma_i\mathfrak{R}_N(\mathbb{F}_p\Delta)}\big)^d$ so that $W = V_1 \oplus \cdots \oplus V_m$. If $\gamma \in \Gamma$, then the action of γ on W permutes the spaces $V_1, \ldots, V_m$ in the same way as γ acts on Γ/Δ, namely $\gamma V_i = V_j$, where $\gamma\gamma_i\Delta = \gamma_j\Delta$.

We need the following elementary result.

Proposition 2.21. *Let $V = V_1 \oplus \cdots \oplus V_m$ be a vector space over a field $\mathbb{F}$ which decomposes as a direct sum of its subspaces $V_1, \ldots, V_m$. Let $s \in \mathbb{N}$, and for $i = 1, \ldots, s$, let $T_i\colon V \to V$ be bijective linear transformations preserving the above direct sum decomposition. Assume that for all $i = 1, \ldots, s$ and $j = 1, \ldots, m$ we have $T_i(V_j) \in \{V_1, \ldots, V_m\} \setminus \{V_j\}$. Then*

$$\dim_{\mathbb{F}} \ker(1 + T_1 + \cdots + T_s) \leq \frac{s}{s+1} \dim_{\mathbb{F}} V.$$

Proof. Let $\mathfrak{G} \leq \mathrm{GL}(V)$ be the subgroup of $\mathrm{GL}(V)$ generated by $T_1, \ldots, T_s$. Let $E_1, \ldots, E_r$ be the orbits of $\mathfrak{G}$ acting on the direct summands $\{V_1, \ldots, V_m\}$, and for $j = 1, \ldots, r$, define $\mathfrak{V}_j = \oplus_{V_i \in E_j} V_i$. Since each $\mathfrak{V}_j$ is invariant under $\mathfrak{G}$ and satisfies the same hypothesis as V, it will be sufficient to prove the claimed inequality for each $\mathfrak{V}_j$ in place of V, and then add them for $j = 1, \dots, r$. Therefore without loss of generality we may assume that $\mathfrak{G}$ acts transitively on $V_1, \dots, V_m$. In particular, since $\dim V_i = \dim g(V_i)$ for each V_i and each $g \in \mathfrak{G}$, we have $\dim V_1 = \cdots = \dim V_m$.

Let $t = \lceil \frac{m}{s+1} \rceil$. We construct inductively a sequence $V_{a_1}, \dots, V_{a_t}$ as follows: put $V_{a_1} = V_1$, and for $i = 2, \dots, t$, choose V_{a_i} to be any element in

$$\{V_1, \dots, V_m\} \backslash \Big(\bigcup_{j=1}^{i-1} \{V_{a_j}, T_1(V_{a_j}), \dots, T_s(V_{a_j})\} \Big).$$

Such V_{a_i} exists as long as $(i-1)(s+1) < m$, i.e., $i \le t$.

Let $\pi_i \colon V \to V_i$ be the projection onto V_i. The choice of $\{V_{a_i}\}_{i=1}^t$ ensures that for all pairs $1 \le j < i \le t$,

$$\pi_{a_i} \circ (1 + T_1 + \cdots + T_s)(V_{a_j}) = \{0\},$$

while the condition $T_r(V_{a_i}) \ne V_{a_i}$ for $r = 1, \dots, s$ ensures that

$$\pi_{a_i} \circ (1 + T_1 + \cdots T_s)|_{V_{a_i}} = 1_{V_{a_i}}.$$

It follows that the t subspaces $\{(1 + T_1 + \cdots + T_s)(V_{a_i})\}_{i=1}^t$ generate their direct sum in V. Moreover, $\dim(1 + T_1 + \cdots + T_s)(V_{a_i}) = \dim V_{a_i} = \dim V_1$ for all $i = 1, \dots, t$.

Therefore,

$$\dim(1 + T_1 + \cdots T_s)(V) \ge t \dim V_1 \ge \frac{m}{s+1} \dim V_1 = \frac{1}{s+1} \dim V,$$

and Proposition 2.21 follows from the rank-nullity theorem. ■

Let $J(\mathbb{F}_p\Delta)$ be the Jacobson ideal of $\mathbb{F}_p\Delta$. By the theory of semisimple algebras, the multiplicity of N in $\mathbb{F}_p\Delta / J(\mathbb{F}_p\Delta)$ is equal to $c := \dim_E N$, where $E = \mathrm{End}_\Delta(N)$ is a finite extension field of $\mathbb{F}_p$. Therefore $\frac{\mathbb{F}_p\Delta}{\mathfrak{R}_N(\mathbb{F}_p\Delta)} \simeq N^c$, and hence

$$\dim_{\mathbb{F}_p} W = d \cdot m \cdot c \cdot \dim_{\mathbb{F}_p} N,$$

where $d = d(G)$ and $m = |G : H| = |\Gamma : \Delta|$.

Apply Proposition 2.21 with $V = W$, $V_i = \big(\frac{\gamma_i \mathbb{F}_p\Delta}{\gamma_i \mathfrak{R}_N(\mathbb{F}_p\Delta)}\big)^d$ and $T_j(x) = e_j \bar{b}_j x$ for $x \in W$ and $j = 1, \dots, s$. Since $\bar{b}_j \notin \Delta$, we have $\bar{b}_j \gamma_i \Delta \ne \gamma_i \Delta$ for any coset $\gamma_i \Delta$ and hence $\bar{b}_j V_i \ne V_i$. We deduce

$$\dim_{\mathbb{F}_p} \ker(1 + e_1 \bar{b}_1 + \cdots + e_s \bar{b}_s)|_W \le \frac{s}{s+1} \dim_{\mathbb{F}_p} W = \frac{s}{s+1} d \cdot m \cdot c \dim_{\mathbb{F}_p} N.$$

From (2.11), we have $\dim_{\mathbb{F}_p} \ker(1 + \bar{b}_1 + \cdots + \bar{b}_s)|_W \ge k \dim_{\mathbb{F}_p} N$, and therefore $k \le (sdmc)/(s+1)$ On the other hand, if we set $d' = d(H) = d(L_k)$, Theorem 2.7 gives

$$k > (d' - 2)c - \dim_E H^1(L/N, N).$$

Moreover, since N is a faithful L/N-module, we have $|H^1(L/N, N)| < |N|$ by Theorem A of [3], and therefore $k > (d'-2)c - c = (d'-3)c$. Hence

$$(d'-3)c < k \le \frac{sdmc}{s+1}$$

and so $d' < (sdm)/(s+1) + 3$. Now

$$\frac{sdm}{s+1} + 3 = \frac{(2s+1)(d-1)m}{2s+2} + 1 + C,$$

where

$$C = \frac{2s+1}{2s+2} m + 2 - \frac{dm}{2s+2} < m + 2 - 3m \le 0,$$

since $d = d(G) > 6(s+1)$. Therefore,

$$d' = d(H) < \frac{sdm}{s+1} + 3 < \frac{(2s+1)(d-1)m}{2s+2} + 1,$$

and recalling that $m = |\Gamma : \Delta| = |G : H|$, we obtain

$$\frac{d(H)-1}{|G:H|} = \frac{d'-1}{m} < \frac{2s+1}{2s+2}(d-1) = \alpha(s)(d(G)-1).$$

The proof of Proposition 2.15 is complete.

2.8. Proof of Proposition 2.19

First we show that it suffices to prove Proposition 2.19 in the special case when $\mathcal{H} = \mathcal{G}$. Let $d = d(\mathcal{G})$ and let B_d be the graph with a single vertex and d edges, namely the bouquet of d circles. We identify $\mathcal{G}$ with $\pi_1(B_d)$, the fundamental group of B_d. Let $\tilde{B_d}$ be the universal cover of B_d; this is just the Cayley graph of $\mathcal{G}$. The cellular chain complex $R_1 := C_*(\tilde{B_d}, \mathbb{F}_p)$ of $\tilde{B_d}$ together with the action of $\mathcal{G}$ by translation on $\tilde{B_d}$ results in the free $\mathbb{F}_p\mathcal{G}$- resolution of $\mathbb{F}_p$:

$$R_1 : \quad 0 \to (\mathbb{F}_p\mathcal{G})^d \to \mathbb{F}_p\mathcal{G} \to \mathbb{F}_p \to 0.$$

Let Z be the quotient graph of $\tilde{B_d}$ by the action of $\mathcal{H} \le \mathcal{G}$. Then Z is a cover of B_d of degree $|\mathcal{G} : \mathcal{H}|$ with fundamental group $\pi_1(Z) = \mathcal{H}$. In fact, Z is the Cayley graph of $\mathcal{G}/\mathcal{H}$ with respect to the image of the generating set of $\mathcal{G}$.

By contracting a maximal tree in Z to a point, we obtain a homotopy equivalence

$$\alpha : Z \to B_{d'}$$

of Z with the bouquet of d' circles $B_{d'}$, where $d' = d(\mathcal{H}) = (d-1)|\mathcal{G} : \mathcal{H}| + 1$. The homotopy equivalence α induces an isomorphism of fundamental groups $\alpha_\pi : \mathcal{H} = \pi_1(Z) \to \pi_1(B_{d'})$, and we will identify $\mathcal{H}$ with $\pi_1(B_{d'})$ via α_π from now on. Moreover, α induces a homotopy equivalence of chain complexes of $\mathbb{F}_p\mathcal{H}$-modules between $R_1 =$

$C_*(\tilde{Z}, \mathbb{F}_p)$ and the cellular chain complex $R_2 := C_*(\tilde{B}_{d'}, \mathbb{F}_p)$ of the universal cover $\tilde{B}_{d'}$ of $B_{d'}$, namely

$$R_2: \quad 0 \to (\mathbb{F}_p\mathcal{H})^{d'} \to \mathbb{F}_p\mathcal{H} \to \mathbb{F}_p \to 0.$$

Specifically, there are chain maps of complexes of $\mathbb{F}_p\mathcal{H}$-modules $\tilde{\alpha}_*\colon R_1 \to R_2$ and $\tilde{\beta}_*\colon R_2 \to R_1$ such that the composition $\tilde{\alpha}_* \circ \tilde{\beta}_*$ (respectively, $\tilde{\beta}_* \circ \tilde{\alpha}_*$) is homotopic to the identity map on $R2$ (respectively, $R1$). Passing to $\mathcal{U}$-coinvariants by applying $\mathbb{F}_p \otimes_{\mathbb{F}_p\mathcal{U}} -$ (i.e., factoring out the action of $\mathcal{U}$), we deduce that $\tilde{\alpha}_*$ and $\tilde{\beta}_*$ induce homotopy equivalence between the complexes of $\mathbb{F}_p\Delta$-modules

$$(\mathbb{F}_p\Gamma)^d \xrightarrow{\delta'} \mathbb{F}_p\Gamma \to \mathbb{F}_p \to 0 \quad \text{and} \quad (\mathbb{F}_p\Delta)^{d'} \xrightarrow{\delta''} \mathbb{F}_p\Delta \to \mathbb{F}_p \to 0.$$

In particular, there are $\mathbb{F}_p\Delta$-homomorphisms in degree 1, $\bar{\alpha}\colon (\mathbb{F}_p\Gamma)^d \to (\mathbb{F}_p\Delta)^{d'}$ and $\bar{\beta}\colon (\mathbb{F}_p\Delta)^{d'} \to (\mathbb{F}_p\Gamma)^d$, which induce mutually inverse bijections between $X_1 = \ker\delta'$ and $X_2 = \ker\delta''$. The canonical isomorphisms $\rho_i\colon \mathcal{U}_p^{\mathrm{ab}} \to X_i$ from (2.10) give $\bar{\alpha}|_{X_1} = \rho_2 \circ \rho_1^{-1}$ and $\bar{\beta}|_{X_2} = \rho_1 \circ \rho_2^{-1}$, since the homotopy α induces the identity on the fundamental group $\mathcal{H}$ with our identification.

Let S be a $\mathbb{F}_p\Delta$-module and let $f\colon \mathcal{U}_p^{\mathrm{ab}} \to S$ be a $\mathbb{F}_p\Delta$-homomorphism. If $f = \theta \circ \rho_1$ for some $\theta \in \mathrm{Hom}_\Delta((\mathbb{F}_p\Gamma)^d, S)$, then $f = \zeta \circ \rho_2$, where $\zeta := \theta \circ \bar{\beta}$ belongs to $\mathrm{Hom}_\Delta((\mathbb{F}_p\Delta)^{d'}, S)$. Conversely, if $f = \zeta \circ \rho_2$ for $\zeta \in \mathrm{Hom}_\Delta((\mathbb{F}_p\Delta)^{d'}, S)$ then $f = \theta \circ \rho_1$ with $\theta := \zeta \circ \bar{\alpha}$ in $\mathrm{Hom}_\Delta((\mathbb{F}_p\Gamma)^d, S)$.

Hence the validity of Proposition 2.19 depends only on the presentation

$$1 \to \mathcal{U} \to \mathcal{H} \to \Delta \to 1,$$

without reference to $\mathcal{G}$, and we may assume from now on that $\mathcal{G} = \mathcal{H}$ and $\Gamma = \Delta$.

Let us restate the notation of Proposition 2.19 in this setting.

Let $d = d(\mathcal{G})$ and fix a generating set $x_1, \dots, x_d$ of $\mathcal{G}$. The isomorphism $\rho\colon \mathcal{U}_p^{\mathrm{ab}} \to (\mathbb{F}_p\Gamma)^d$ given by (2.10) completes the exact sequence of $\mathbb{F}_p\Gamma$-modules

$$0 \to \mathcal{U}_p^{\mathrm{ab}} \xrightarrow{\rho} (\mathbb{F}_p\Gamma)^d \to \mathbb{F}_p\Gamma \to \mathbb{F}_p \to 0$$

associated to the presentation $1 \to \mathcal{U} \to \mathcal{G} \to \Gamma \to 1$.

Let $\mathcal{K}$ be a normal subgroup of $\mathcal{G}$ with $\Phi(\mathcal{U}) \le \mathcal{K} \le \mathcal{U}$. Let S be the $\mathbb{F}_p\Gamma$-module $\mathcal{U}/\mathcal{K}$ and let $f \in \mathrm{Hom}_\Gamma(\mathcal{U}_p^{\mathrm{ab}}, S)$ be the map $u\Phi(\mathcal{U}) \mapsto u\mathcal{K}$ ($u \in \mathcal{U}$). We need to show that f lifts to a $\mathbb{F}_p\Gamma$-homomorphism $\theta\colon (\mathbb{F}_p\Gamma)^d \to S$ such that $f = \theta \circ \rho$ if and only if $\mathcal{U}/\mathcal{K}$ is complemented in $\mathcal{G}/\mathcal{K}$.

We have the following basic result.

Proposition 2.22. *The group $\mathcal{U}/\mathcal{K}$ is complemented in $\mathcal{G}/\mathcal{K}$ if and only if there is a homomorphism $\phi\colon \mathcal{G} \to \mathcal{G}/\mathcal{K}$ such that*

(P1) *$\phi(y) \equiv y\mathcal{K}$ mod $\mathcal{U}/\mathcal{K}$ for each $y \in \mathcal{G}$, and*

(P2) *$\mathcal{U} \subseteq \ker\phi$.*

Proof. Suppose there is a homomorphism $\phi\colon \mathcal{G} \to \mathcal{G}/\mathcal{K}$ with properties (P1) and (P2). Define $\Theta := \phi(\mathcal{G}) \le \mathcal{G}/\mathcal{K}$. Suppose $\phi(x) \in (\mathcal{U}/\mathcal{K}) \cap \Theta$ for some $x \in \mathcal{G}$. From (P1),

$x\mathcal{K} \equiv \phi(x) \bmod \mathcal{U}/\mathcal{K}$ and therefore $x \in \mathcal{U}$. By (P2), we have $\phi(x) = 1$ and we have proved $\Theta \cap (\mathcal{U}/\mathcal{K}) = 1_{\mathcal{G}/\mathcal{K}}$. In addition, (P1) gives $\Theta \cdot (\mathcal{U}/\mathcal{K}) = \mathcal{G}/\mathcal{K}$. Therefore Θ is the required complement to $\mathcal{U}/\mathcal{K}$.

Now assume that $\Theta \leq \mathcal{G}/\mathcal{K}$ is a complement to $\mathcal{U}/\mathcal{K}$. For $i = 1, \dots, d$, we can write $x_i\mathcal{K}$ uniquely as $x_i\mathcal{K} = z_i y_i$, with $z_i \in \Theta$ and $y_i \in \mathcal{U}/\mathcal{K}$. Define $\phi(x_i) = z_i$ $(i = 1, \dots, d)$ and extend ϕ to a homomorphism $\phi\colon \mathcal{G} \to \Theta \leq \mathcal{G}/\mathcal{K}$. By its definition, ϕ satisfies (P1). If $u \in \mathcal{U}$, then (P1) with $y = u$ shows $\phi(u) \in \mathcal{U}/\mathcal{K}$. Thus $\phi(u) \in \phi(\mathcal{G}) \cap \mathcal{U}/\mathcal{K} = \Theta \cap \mathcal{U}/\mathcal{K} = \{1_{\mathcal{H}/\mathcal{K}}\}$ and hence $u \in \ker \phi$. Therefore (P2) holds as well. ∎

The maps $\phi\colon \mathcal{G} \to \mathcal{G}/\mathcal{K}$ which satisfy property (P1) from Proposition 2.22 are in bijective correspondence with maps $h\colon \mathcal{G} \to S = \mathcal{U}/\mathcal{K}$ defined by $\phi(g) = h(g)g\mathcal{K}$ for each $g \in \mathcal{G}$. We observe that ϕ is a group homomorphism if and only if

$$h(g_1 g_2) = h(g_1)\, {}^{g_1}h(g_2) \quad \forall g_1, g_2 \in \mathcal{G},$$

that is, h is a derivation from $\mathcal{G}$ into S (where, as usual, $\mathcal{G}$ acts on S via the projection $\mathcal{G} \to \Gamma = \mathcal{G}/\mathcal{U}$).

In addition, ϕ satisfies property (P2) if and only if $h(u)u\mathcal{K} = 1_{\mathcal{U}/\mathcal{K}}$ for all $u \in \mathcal{U}$, which in the additive group $(S, +)$ becomes $h(u) = -f(u\Phi(\mathcal{U}))$ for each $u \in \mathcal{U}$.

In summary, the above discussion shows that $\mathcal{U}/\mathcal{K}$ is complemented in $\mathcal{G}/\mathcal{K}$ if and only if there is a derivation $h\colon \mathcal{G} \to S$ such that

$$h(u) = -f(u\Phi(\mathcal{U})), \quad \forall u \in \mathcal{U}. \tag{2.12}$$

A derivation $h\colon \mathcal{G} \to S$ is specified uniquely by its values $s_i := h(x_i) \in S$ on the generating set $x_1, \dots, x_d$ of $\mathcal{G}$, and then h is determined by

$$h(w) = \sum_{i=1}^{d} \overline{\frac{\partial w}{\partial x_i}}\, s_i \quad \forall w \in \mathcal{G}.$$

Here $\partial w/\partial x_i \in \mathbb{F}_p\mathcal{G}$ are the Fox derivatives of the group algebra $\mathbb{F}_p\mathcal{G}$ and $y \mapsto \bar{y} \in \mathbb{F}_p\Gamma$ is the reduction $\mathbb{F}_p\mathcal{G} \to \mathbb{F}_p\Gamma$ of $\mathbb{F}_p\mathcal{G}$ modulo its ideal generated by $\mathcal{U} - 1$. For a proof, see [4], §IV.2, Exercise 3.

Recall the description of $\rho\colon \mathcal{U}_p^{\mathrm{ab}} \to (\mathbb{F}_p\Gamma)^d$ in (2.10):

$$\rho(u\Phi(\mathcal{U})) = \Big(\overline{\frac{\partial u}{\partial x_1}}, \dots, \overline{\frac{\partial u}{\partial x_d}}\Big), \quad \forall u \in \mathcal{U}.$$

Let $\theta\colon (\mathbb{F}_p\Gamma)^d \to S$ be the homomorphism defined by $\theta(a_1, \dots, a_d) = \sum_{i=1}^{d} a_i s_i$ for all $a_i \in \mathbb{F}_p\Gamma$.

Combining the formulas for h and ρ above, we obtain $h(u) = \theta \circ \rho(u\Phi(\mathcal{U}))$ for all $u \in \mathcal{U}$. Hence the condition (2.12) required from the derivation h is equivalent to $-f(x) = \theta \circ \rho(x)$ for each $x \in \mathcal{U}_p^{\mathrm{ab}}$, i.e., $f = (-\theta) \circ \rho$. Proposition 2.19 follows. ∎

Acknowledgements. The author thanks the anonymous referees for helpful comments which improved the exposition.

References

[1] Abért, M., Jaikin-Zapirain, A. and Nikolov, N.: The rank gradient from a combinatorial viewpoint. *Groups Geom. Dyn.* **5** (2011), no. 2, 213–230.

[2] Abért, M. and Nikolov, N.: Rank gradient, cost of groups and the rank versus Heegaard genus problem. *J. Eur. Math. Soc. (JEMS)* **14** (2012), no. 5, 1657–1677.

[3] Aschbacher, M. and Guralnick, R.: Some applications of the first cohomology group. *J. Algebra* **90** (1984), no. 2, 446–460.

[4] Brown, K.: *Cohomology of groups*. Graduate Texts in Mathematics 87, Springer, New York-Berlin, 1982.

[5] Dalla Volta, F. and Lucchini, A.: Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc. Ser. A* **64** (1998), no. 1, 82–91.

[6] Dalla Volta, F. and Lucchini, A.: The smallest group with non-zero presentation rank. *J. Group Theory* **2** (1999), no. 2, 147–155.

[7] Detomi, E. and Lucchini, A.: Probabilistic generation of finite groups with a unique minimal normal subgroup. *J. Lond. Math. Soc. (2)* **87** (2013), no. 3, 689–706.

[8] Lackenby, M.: Expanders, rank and graphs of groups. *Israel J. Math.* **146** (2005), 357–370.

[9] Lackenby, M.: Detecting large groups. *J. Algebra* **324** (2010), no. 10, 2636–2657.

[10] Osin, D.: Rank gradient and torsion groups. *Bull. Lond. Math. Soc.* **43** (2011), no. 1, 10–16.

[11] Schlage-Puchta, J.-C.: A p-group with positive rank gradient. *J. Group Theory* **15** (2012), no. 2, 261–270.

[12] Wilson, J. S. and Zelmanov, E.: Identities for Lie algebras of pro-p groups. *J. Pure Appl. Algebra* **81** (1992), no. 1, 103–109.

[13] Zelmanov, E.: Lie algebras and torsion groups with identity. *J. Comb. Algebra* **1** (2017), no. 3, 289–340.

Received September 28, 2021; revised December 12, 2021. Published online January 19, 2022.

Nikolay Nikolov
Mathematical Institute, University of Oxford,
Woodstock Road, Oxford, OX2 6GG, United Kingdom;
nikolov@maths.ox.ac.uk