Remarks on profinite groups having few open subgroups

Dan Segal

October 16, 2017

1 Introduction

This paper is kind of a survey. The aim is to shed some light on the topic by putting together mainly known results, adding a few new ones (that rely on fairly standard techniques), and to draw attention to a couple of questions.

A profinite group is *small* if for each $n \in \mathbb{N}$ it has only finitely many open subgroups of index at most n.

Every finitely generated profinite group is small: indeed it is clear that a d-generator group has at most $n!^d$ subgroups of index n (see [LS], Chapter 2 for sharper estimates). Small groups also arise in number theory: if S is a finite set of primes and K is the maximal algebraic extension of $\mathbb{Q}$ unramified outside S then $\mathrm{Gal}(K/\mathbb{Q})$ is a small profinite group ([K], Theorem 1.48). Whether all such Galois groups are in fact finitely generated seems to be a hard open problem, and group-theoretical methods are extemely unlikely to solve it.

If G is a finitely generated profinite group, then (a) every subgroup of finite index is open and (b) every power subgroup G^m is open ([NS1], [NS2]; for better proofs see also [NS3]); here $G^m = \langle g^m \mid g \in G \rangle$ denotes the subgroup generated *algebraically* (not topologically) by all mth powers in G.

If (a) holds one says that G is *strongly complete*. If (b) holds I will say that G is *power-open*. It is clear that (b) implies (a).

We shall see below that every strongly complete group is small. A small group need be neither strongly complete nor power-open; we explore some connections between these various concepts, in particular, to what extent they can be 'algebraically defined'. Writing

$$\mathcal{F}(P) = \{P/N \mid N \lhd_o P\}$$

to denote the family of all continuous finite quotients of a profinite group P, I will say that a property of P is *algebraically defined* if it can be stated in terms of some purely group-theoretic property of the groups in $\mathcal{F}(P)$ – this is not very precise, but will be clear in the cases discussed below.

Significant contibutions are due to Nikolay Nikolov and John Wilson; thanks to both for allowing me to quote some unpublished results.

I will use the following notation. For subset X of a group,

$$X^{*n} = \{x_1 x_2 \dots x_n \mid x_1, x_2, \dots, x_n \in X\}.$$

For a group word w on k variables,

$$G_w = \{w(\mathbf{g})^{\pm 1} \mid \mathbf{g} \in G^{(k)}\}, \quad w(G) = \langle G_w \rangle\,;$$

and for $m \in \mathbb{N}$, $G_{\{m\}} = \{g^m \mid g \in G\}$, $G^m = \left\langle G_{\{m\}} \right\rangle$.

$\overline{X}$ denotes the closure of a subset X in a profinite group G. We write $N \lhd_o G$ to mean: N is an open normal subgroup of G.

The word w has *width* f in G if $w(G) = G_w^{*f}$, and infinite width if this holds for no finite f. We recall that in a profinite group G, the subgroup $w(G)$ is closed if and only if w has finite width in G; this holds if and only if w has bounded width in $\mathcal{F}(G)$ (see [S], Section 4.1). If $w(G)$ has countable index in G then $w(G)$ is open, hence has finite index ([SW], Lemma 2).

A finite group is *anabelian* if it has no abelian composition factors. A profinite group G is anabelian if G/N is anabelian for every open normal subgroup N of G.

2 Examples

In the proof of [N2], Theorem 4, Nikolov introduces a general method for constructing groups with large verbal width. The basic idea is summed up in the next lemma.

For a group B let $\mathcal{S}_n(B)$ denote the set of all n-generator subgroups of B.

Lemma 1 *Let w be a word in k variables and let $G = M \rtimes B$ be a semi-direct product with $w(M) = 1$. Suppose that for each $H \in \mathcal{S}_{km}(B)$ we have $M = A_H \times D_H$ with $[A_H, H] = 1$ and $[D_H, H] \leq D_H$. Then for any $\mathbf{g}_1, \dots, \mathbf{g}_m \in G^{(k)}$ there exists $H \in \mathcal{S}_{km}(B)$ such that*

$$\prod_1^m w(\mathbf{g}_i)^{\pm 1} \in D_H \cdot H. \tag{1}$$

This is clear: take $H = \langle b_{ij} \mid i = 1, \dots, m,\ j = 1, \dots, k \rangle$ where $g_{ij} \in M b_{ij}$, $b_{ij} \in B$, and observe that

$$w(\mathbf{g}_i) \in w(A_H \times (D_H \cdot H)).$$

Now suppose that

$$w(G) \supseteq M \neq \bigcup_{H \in \mathcal{S}_{km}(B)} D_H.$$

Then some element of M is not of the form (1), and it follows that w does not have width m in G.

Proposition 1 *Let π be a non-empty set of primes with infinite complement. There exists a metabelian small profinite group G such that $G/G'G^p$ is infinite iff $p \in \pi$. Also G is not strongly complete and G' is not closed.*

Proof. For distinct primes p and q we construct a finite group $G_{p,q}$ as follows. Set $B = B_q = C_q^{(4q)}$ (the elementary abelian group of order q^{4q}), and for $H \leq B$ let A_H be the $\mathbb{F}_p B$-module $(B-1)\mathbb{F}_p B/(H-1)\mathbb{F}_p B$. Note that $A_H(H-1) = 0$ and $A_H(B-1) = A_H$, since $p \neq q$ implies that $(B-1)\mathbb{F}_p B$ is an idempotent ideal.

Put

$$M_{p,q} = \bigoplus_{H \in \mathcal{S}_{3q}(B)} A_H$$
$$G_{p,q} = M_{p,q} \rtimes B_q.$$

Note that

$$G'_{p,q} = [M_{p,q}, G_{p,q}] = M_{p,q}.$$

Writing $D_H = \bigoplus_{H \neq L \in \mathcal{S}_{3q}(B)} A_L$ we see that Lemma 1 applies for the word $w_p = [x,y]z^p$, and infer that this word does not have width q in $G_{p,q}$.

Now partition π' (the set of primes complementary to π) into $|\pi|$ infinite subsets $\sigma(p)$ $(p \in \pi)$. Set

$$G = \prod_{p \in \pi, q \in \sigma(p)} G_{p,q}.$$

If $p \in \pi$ then w_p does not have width q in $G_{p,q}$, hence also not in G, for every $q \in \sigma(p)$. So w_p has infinite width in G. It follows that $w_p(G) = G'G^p$ is not closed, and therefore has uncountable index in G.

If $r \in \pi'$ then $G_{\{r\}}$ contains $\prod_{p \in \pi, r \neq q \in \sigma(p)} G_{p,q}$ so G^r is open and $G/G'G^r \cong B_r$ is finite.

Now let $m \in \mathbb{N}$. If $q \nmid m$ then $G_{p,q}^m \geq \left\langle B_q^{G_{p,q}} \right\rangle = G_{p,q}$. It follows that

$$\overline{G^m} \geq \prod_{p \in \pi, q \in \sigma(p), q \nmid m} G_{p,q}$$

and hence that $\overline{G^m}$ is open. It follows trivially (see Theorem 1 below) that G is small.

If $p \in \pi$ then the same argument shows that $\overline{G^p} = G$, while G has infinitely many normal subgroups of index p; none of these is open so G is not strongly complete. Finally, if G' were closed then $G'G^p = G'G_{\{p\}}$ would be closed, being the product of two compact subsets of G, whence $G = \overline{G^p} \leq G'G^p$. This is false for $p \in \pi$, so G' is not closed. (This may seem counter-intuitive since at first glance one expects G' to be the product of the $M_{p,q}$: the point is that an element of $M_{p,q}$ may be the product of about $4q$ commutators, and an infinite product of such elements may fail to be a product of finitely many commutators in G.) ∎

The next example is taken from [N2], Theorem 4. For any group S we denote by $\mathcal{V}_S$ the group variety generated by S (the class of all groups that satisfy all

laws of S). If S is finite then $\mathcal{V}_S$ is finitely based, by the Oates-Powell Theorem (see [HN], 52.12). It follows that $\mathcal{V}_S$ can be defined by a single word, w_S. Then for any group G, the corresponding verbal subgroup is $\mathcal{V}_S(G) = w_S(G)$.

Proposition 2 *Let S be a non-abelian finite simple group of exponent m. There exists an anabelian small profinite group G such that neither $\mathcal{V}_S(G)$ nor G^m is closed. G is not strongly complete.*

Proof. Say w_S is a word on k variables. Let $(T_n)_{n\in\mathbb{N}}$ be a sequence of finite non-abelian simple groups of strictly increasing exponents, all exceeding m (for example, large alternating groups). Since the free group F_{kn} has only finitely many normal subgroups of index $|T_n|$, there exists $r(n)$ such that $T_n^{(r(n))}$ cannot be generated by kn elements. Put $B_n = T_n^{(r(n))}$, for each $H \in \mathcal{S}_{kn}(B_n)$ let Ω_H be the B_n-set $H \setminus B_n$, and let $M_H = S^{\Omega_H}$, a B_n-group where B_n acts by permuting the factors.

Let $M_n = \prod_{H\in\mathcal{S}_{kn}(B_n)} M_H$ (direct product) and set

$$G_n = M_n \rtimes B_n = S \wr_\Omega B_n,$$

the permutational wreath product where Ω is the disjoint union of the transitive G-sets Ω_H.

Let $H \in \mathcal{S}_{kn}(B_n)$. Then $M_H = A_H \times C_H$ where $A_H \cong S$ is the factor corresponding to H in Ω_H and C_H is the product of the remaining factors, and the conditions of Lemma 1 are fulfilled on putting $D_H = C_H \times \prod_{L\neq H} M_L$, both for $w = w_S$ and for $w = x^m$. Also

$$w_S(G_n) \geq G_n^m \geq \left\langle (B_n^m)^{G_n} \right\rangle = \left\langle {B_n}^{G_n} \right\rangle = G_n$$

(the final equality holds because for each H we have $|\Omega_H| \geq 2$ and S is perfect).

We conclude that w_S does not have width n, and x^m does not have width kn, in G_n. Hence each of these words has infinite width in

$$G = \prod_{n=1}^{\infty} G_n,$$

and so neither $\mathcal{V}_S(G) = w_S(G)$ nor G^m is closed.

Let $q \in \mathbb{N}$. Then $T_n^q = T_n$ for all but finitely many n. As above it follows that $G_n^q = G_n$ for all but finitely many n, and hence (as above) that $\overline{G^q}$ is open in G, and finally that G is therefore small.

That G is not strongly complete follows from Theorem 4, below. ■

Different examples of small but not strongly complete groups were given in [N], Proposition 27.

3 Small groups

Write $s_n(G)$ to denote the number of (open) subgroups of index at most n in a (pro)finite group G. Thus a profinite group P is small if and only if $s_n(P)$ is finite for each n; this is equivalent to the statement: there is a function $f : \mathbb{N} \to \mathbb{N}$ such that $s_n(G) \leq f(n)$ for every $G \in \mathcal{F}(P)$ and all n.

Theorem 1 *A profinite group P is small if and only if $\overline{P^m} \lhd_o P$ for every $m \in \mathbb{N}$.*

Thus P is small if and only if for each $m \in \mathbb{N}$ there exists $k(m)$ such that

$$\forall Q \in \mathcal{F}(P) : |Q/Q^m| \leq k(m). \tag{2}$$

Equivalently: $\mathcal{F}(P)$ contains only finitely many groups of exponent m.

This has a curious number-theoretic interpretation: with Chebotarev's Theorem ([K], Theorem 1.116) it yields

Corollary 1 *Let S be a finite set of primes and let $m \in \mathbb{N}$. Then there are only finitely many finite Galois extensions K of $\mathbb{Q}$ such that* (1) *all primes ramified in K are in S and* (2) *almost all primes have residue degree at most m in K.*

In one direction, Theorem 1 is obvious: every open subgroup of index at most n contains $\overline{P^m}$ where $m = n!$, so $s_n(P) \leq s_n(P/\overline{P^m}) < \infty$.

The other direction lies deeper; it generalizes the positive solution to the Restricted Burnside Problem, which can be formulated as the statement: $\overline{F^m} \lhd_o F$ for every $m \in \mathbb{N}$ when F is a finitely generated free profinite group.

It is proved in much the same way, bearing in mind the slightly different hypothesis. Since $\overline{P^m}$ is the intersection of all $N \lhd_o P$ with $P^m \leq N$, it will follow from the next result, on taking $f(n) = s_n(P)$:

Theorem 2 *Let $f : \mathbb{N} \to \mathbb{N}$ be a function and let $m \in \mathbb{N}$. If G is a finite group such that $G^m = 1$ and $s_n(G) \leq f(n)$ for all n then $|G| \leq \nu(m, f)$, a number depending only on f and m.*

For the rest of this section all groups will be finite. For a group G let $h^*(G)$ denote the minimal length of a chain of normal subgroups $1 = G_0 \leq G_1 < \ldots < G_n = G$ such that each factor G_i/G_{i-1} is either nilpotent or semisimple (here, a *semisimple group* means a direct product of non-abelian simple groups). Classic results of Hall and Higman, recalled in Section 6 below, imply

Theorem 3 *If $G^m = 1$ then $h^*(G) \leq \eta(m)$, a number depending only on m.*

(Take $\eta(m) = 2\delta(m)$ in Theorem 10.)

Now let G be a group satisfying the hypotheses of Theorem 2.

Case 1. Suppose that $|G| = p^e$ for some prime p, and that $|G/G'G^p| = p^d$. Then $p^{d-1} \leq s_p(G) \leq f(p)$ so $d \leq \lambda(p) := \lceil 1 + \log_p f(p) \rceil$. Now G can be generated

by d elements, and then Zelmanov's theorem [Z1], [Z2] gives $|G| \leq \beta(\lambda(p), m)$, a number depending only on $f(p)$ and m.

Case 2. Suppose that G is nilpotent. Say $m = p_1^{e_1} \dots p_r^{e_r}$. Then from Case 1 we see that

$$|G| \leq \prod_{i=1}^{r} \beta(\lambda(p_i), m) := \nu_{\text{nil}}(m, f).$$

Case 3. Suppose that G is semisimple. The result of [J], with CFSG, shows that there are only finitely many non-abelian simple groups S such that $S^m = 1$; call them $S_1, \dots, S_k$ and put $t_i = |S_i|$. Now $G \cong \prod S_i^{(c_i)}$ for some $c_i \geq 0$. Clearly $c_i \leq s_{t_i}(G) \leq f(t_i)$ for each i, and so

$$|G| \leq \prod_{i=1}^{k} t_i^{f(t_i)} := \nu_{\text{ss}}(m, f).$$

So far, we have shown that if $h^*(G) = 1$ then

$$|G| \leq \max\{\nu_{\text{nil}}(m, f),\ \nu_{\text{ss}}(m, f)\} := \nu_1(m, f),$$

say. Now let $q > 1$ and suppose inductively that for each $h < q$, and every function g, we have found a number $\nu_h(m, g)$ such that for any group H satisfying $h^*(H) \leq h$, $H^m = 1$ and $s_n(H) \leq g(n)$ for all n we have $|H| \leq \nu_h(m, g)$.

Define

$$\nu_q(m, f) = \nu_1(m, f) \cdot \nu_{q-1}(m, g_{m,f})$$

where $g_{m,f}(n) = f(n.\nu_1(m, f))$. Suppose that G with $G^m = 1$ satifies $s_n(G) \leq f(n)$ for all n and that $h^*(G) \leq q$. Thus G has a normal subgroup H with $h^*(H) \leq q - 1$ such that G/H is either nilpotent or semisimple. Then $|G/H| \leq \nu_1(m, f)$, and so for each n we have

$$s_n(H) \leq s_{n.\nu_1(m,f)}(G) \leq g_{m,f}(n).$$

Therefore $|H| \leq \nu_{q-1}(m, g_{m,f})$, whence $|G| = |H|\,|G/H| \leq \nu_q(m, f)$.

Finally, set

$$\nu(m, f) = \nu_{\eta(m)}(m, f).$$

If G satisfies the hypotheses of Theorem 2 then $h^*(G) \leq \eta(m)$ by Theorem 3 and so $|G| \leq \nu(m, f)$ as required.

4 Strongly complete groups

The property of being small is inherently 'algebraically defined', in terms of the subgroup-growth functions $s_n(G)$, and more succinctly in the remark following Theorem 1. The definition of 'strongly complete', on the other hand, refers directly to non-open subgroups, which by their nature are undetectable in the

continuous finite quotients of a profinite group. The following characterization, due to Smith and Wilson, is therefore remarkable.

An *f-variety* is the group variety generated by a finite group. Each such variety is finitely based, by the Oates-Powell theorem (see [HN], Chapter 5), and can therefore be defined by a single group word.

Theorem 4 ([SW], Theorem 2) *A profinite group G is strongly complete if and only if $\mathcal{V}(G) \lhd_o G$ for every f-variety $\mathcal{V}$.*

If $N \leq G$ and $|G : N| = m$ then $N \geq \mathcal{V}(G)$ where $\mathcal{V} = \mathcal{V}_{\mathrm{Sym}(m)}$, so $s_m(G) = s_m(G/\mathcal{V}(G))$; thus we have

Corollary 2 *Every strongly complete profinite group is small.*

See also [P], Theorem 2.4, where this was first proved using an ultrafilter construction.

Now $\mathcal{V}(G)$ is open if and only it is both closed and has finite index in G. If $\mathcal{V} = \mathcal{V}_S$ for a finite group S, it is defined by a word w_S; let us call such a word an *f-word*. Then $\mathcal{V}(G)$ is closed in G if and only if w_S has finite width in G; in that case,

$$|G : \mathcal{V}(G)| = \left|G : \overline{\mathcal{V}(G)}\right| = \sup_{Q \in \mathcal{F}(G)} |Q : w_S(Q)| .$$

Thus we have the algebraic characterization: G is strongly complete if and only if for each f-word w there exists $k(w) \in \mathbb{N}$ such that

$$\forall Q \in \mathcal{F}(G) : |Q/w(Q)| \leq k(w) \text{ and } w \text{ has width } k(w) \text{ in } Q. \tag{3}$$

Smith and Wilson (loc.cit) establish another characterization, which is not algebraic in my sense but nicely clarifies the relation between 'strongly complete' and 'small': *G is strongly complete if and only if G has finitely many subgroups of each finite index, and this holds if and only if G has only countably many subgroups of finite index.*

Now (3) looks like a strengthening of (2), except that the power words x^m are not (usually) f-words, because infinite Burnside groups exist. Could we use power words instead of f-words here? The question has some plausibility because every *finitely generated* profinite group is indeed power-open (the power subgroups G^m are open, [NS2]). On the other hand, it is clear that every power-open profinite group is strongly complete.

Question 1. *Is every strongly complete profinite group power-open?*

If so, we can replace the f-words w in (3) by the power words x^m, $m \in \mathbb{N}$.

The following reduction was pointed out to me by John Wilson:

Proposition 3 (J. S. Wilson) *Suppose that G is strongly complete. If $H^q \lhd_o H$ for every $H \lhd_o G$ and every* prime-power *$q \mid m$ then $G^m \lhd_o G$.*

Proof. There are only finitely many finite simple groups of exponent dividing m, say $S_1, \ldots, S_t$ ([J]+CFSG). Let $\mathcal{V}$ denote the variety generated by $S_1 \times \cdots \times S_t$.

Let $\eta(m)$ be the number given by Theorem 3, so every finite group of exponent dividing m has a normal series of length $\eta(m)$ with each factor either semisimple or nilpotent. Let $k = \eta(m)s$, where m is divisible by s primes. Then every finite group of exponent dividing m has a normal series of length k with each factor either in $\mathcal{V}$ or of exponent q for some prime-power $q \mid m$. It follows by a standard inverse limit argument that every locally finite group of exponent dividing m has such a normal series. Now the main theorem of [NS2] implies that G/G^m is locally finite; hence there is a normal series

$$G = G_0 \geq G_1 \geq \cdots \geq G_k = G^m$$

such that for each i, either $\mathcal{V}(G_i) \leq G_{i+1}$ or $G_i^q \leq G_{i+1}$ for some prime-power $q \mid m$.

Let $i \in \{0, \ldots, k\}$ be maximal such that G_i is open in G. Suppose that $i < k$. Then G_i is again strongly complete, so if $\mathcal{V}(G_{i+1}) \leq G_i$ then $G_{i+1} \lhd_o G_i$ by Theorem 4, whence $G_{i+1} \lhd_o G$, contradiction. If G_i/G_{i+1} has exponent q for some prime-power $q \mid m$ then $G_{i+1} \lhd_o G_i$ by hypothesis, whence $G_{i+1} \lhd_o G$, again a contradiction. It follows that $i = k$ and so $G^m \lhd_o G$. ■

Thus it will suffice to answer Question 1 for normal subgroups of *prime power* index. In some cases this is feasible:

Theorem 5 (N. Nikolov) Let G *be an anabelian profinite group. Then* $G = G^q$ *for every prime-power* q.

Suppose that q is odd. Theorem 3 of [N2] says that the word x^q has bounded width $l(q)$ in every finite anabelian group. In unpublished work (personal communication), Nikolov proves the same statement for q any power of 2. It follows in either case that x^q has finite width $l(q)$ in G, whence G^q is closed. Now if $G^q \leq N \lhd_o G$ then G/N is a finite anabelian group of prime-power order, whence $N = G$. But G^q is the intersection of all such N, so $G^q = G$.

With Proposition 3 this gives

Theorem 6 *Let* G *be an anabelian profinite group. Then* G *is strongly complete if and only if* G *is power-open.*

At the other extreme we could consider prosoluble groups. Question 1 is still open in this case, but the following may be relevant:

Lemma 2 *Suppose that* G *is strongly complete and prosoluble. Let* $q = p^n$, p *a prime, and let* P *be a Sylow pro-*p *subgroup of* G. *If* G^q *is not closed then* $P_1 := P \cap \overline{G^q} \lhd_o P$ *and* P_1 *has an infinite perfect quotient* $P_1/(P \cap G^q)$.

Proof. $\overline{G^q} \lhd_o G$ by Theorem 1, so $P_1 \lhd_o P$. Now G has a Hall pro-p'-subgroup H, and $G^q P \geq HP = G$. So $\overline{G^q} = G^q P_1$ and so

$$\frac{P_1}{P \cap G^q} = \frac{P_1}{P_1 \cap G^q} \cong \frac{\overline{G^q}}{G^q}.$$

The latter is infinite and perfect, because $\overline{G^q}$ is strongly complete and an abelian group of finite exponent is residually finite. ■

Thus a negative answer to Question 1 would imply a positive answer to

Question 2. *Does there exist a pro-p group with a nontrivial perfect quotient*?

This is apparently unkown; the answer is probably 'yes', but it seems quite hard.

To summarize some of the above:

Theorem 7 *Let G be a profinite group. The following conditions are equivalent to G being strongly complete.*

i. *if G is a* pro-p *group: G is finitely generated; or, G is small; or, $\overline{G'G^p}$ is open; or, $G'G^p$ is open;*

ii. *if G is* pronilpotent*: G is small; or, each Sylow subgroup of G is finitely generated;*

iii. *if G is* prosoluble*: $H'H^p \lhd_o H$ for every $H \lhd_o G$ and every prime p;*

iv. *if G is* anabelian*: G^m is open for every $m \in \mathbb{N}$; or, $|G/G^m|$ is finite for every $m \in \mathbb{N}$.*

Proof. Most of this appears above, or follows easily. Let me sketch the argument for (iii), where G is prosoluble. Note that $H'H^p = w(H)$ where $w = [x, y]z^p$ defines the variety generated by C_p, so if G is strongly complete and $H \lhd_o G$ then H is strongly complete and $w(H)$ is open by Theorem 4. For the converse, suppose that G is not strongly complete and let N be a normal subgroup of G of minimal finite index such that N is not open. Then G/N is a finite soluble group, by Hall's characterization of finite soluble groups as those having a Hall p'-subgroup for every prime p: indeed, if Q is a Hall pro-p' subgroup of G then QN/N is a Hall p'-subgroup of G/N. Now let H/N be a minimal normal subgroup of G/N. Then $H \lhd_o G$ and $H'H^p \leq N < H$ for some prime p; so $H'H^p$ is not open in H. ■

Remark Theorem 4 does have a direct analogue for small groups:

Theorem 8 *A profinite group G is small if and only if $\overline{\mathcal{V}(G)} \lhd_o G$ for every f-variety $\mathcal{V}$.*

Of course this is an immediate corollary of Theorem 1, since if $\mathcal{V} = \mathcal{V}_Q$ where Q has exponent m then $G^m \leq \mathcal{V}(G)$. However it is worth mentioning because it is completely elementary. To prove it directly we argue exactly as in the proof of Theorem 1, quoting Proposition 4 (see Section 6 below) in place of Theorem 3.

5 The 'congruence kernel'

Let G be a profinite group. Considered as an abstract group, G has a profinite completion $\widehat{G}$, and the identity map on G induces a natural continuous epimorphism $\pi : \widehat{G} \to G$.

The 'congruence kernel' of G is $C(G) = \ker \pi$. Note that $C(G)$ is the projective limit

$$C(G) = \varprojlim \overline{N}/N$$

where N runs over normal subgroups of finite index in G. Thus G is strongly complete if and only if $C(G) = 1$.

Theorem 9 *If $C(G)$ is small then G is strongly complete.*

Thus a congruence kernel is either trivial or very large (in particular, not finitely generated as a profinite group).

Proof. Assume that $C = C(G)$ is small. First we prove that G is small.

Suppose for a contradiction that G has infinitely many open normal subgroups of index n. It is then easy to see that there exist an open normal subgroup H of G, a finite simple group Q of order $\leq n$ and a continuous epimorphism $\pi : H \to P = Q^{\mathbb{N}}$. For each non-principal ultrafilter $\mathcal{U}$ on $\mathbb{N}$ let $\psi_{\mathcal{U}} : H \to Q$ be the induced map onto the ultrapower $P/\mathcal{U} \cong Q$, and set $K_{\mathcal{U}} = \ker \psi_{\mathcal{U}}$. Note that $K_{\mathcal{U}}$ contains $\pi^{-1}(P_0)$ where P_0 is the restricted direct power of Q inside P; if S is any finite collection of non-principal ultrafilters, it follows that

$$K_S := \bigcap_{\mathcal{U} \in S} K_{\mathcal{U}}$$

is a dense normal subgroup of finite index in H. Thus K_S contains a normal subgroup N of finite index in G and $K_S\overline{N} = H$. Therefore $H/K_S \cong \overline{N}/(\overline{N} \cap K_S)$ is a continuous image of C; say $H/K_S \cong C/M$ where M is open and normal in C.

Let $\mathcal{V}$ be the variety generated by Q. Then $\overline{\mathcal{V}(C)} \lhd_o C$ by Theorem 8. Now $\mathcal{V}(H) \leq K_S$ so $\overline{\mathcal{V}(C)} \leq M$ and so $|H/K_S| \leq \left|C : \overline{\mathcal{V}(C)}\right| < \infty$. Choosing the set S so as to maximize $|H/K_S|$, we see that $K_{\mathcal{U}} \geq K_S$ for every non-principal ultrafilter $\mathcal{U}$. Thus there are only finitely many possibilities for $K_{\mathcal{U}}$.

Now it is easy to see that $K_{\mathcal{U}}$ determines $\mathcal{U}$; indeed, for $V \subseteq \mathbb{N}$ we have

$$V \in \mathcal{U} \iff K_{\mathcal{U}} \supseteq \pi^{-1}\left\{f : \mathbb{N} \to Q \mid f(V) = \{1\}\right\}.$$

But the number of non-principal ultrafilters is infinite, so we have our contradiction.

Now fix an f-variety $\mathcal{V}$ and put $W = \mathcal{V}(G)$. If $W \leq N \lhd_f G$ then $\overline{N}/N$ is a continuous image of C, and as above we may infer that $\left|\overline{N}/N\right| \leq \left|C : \overline{\mathcal{V}(C)}\right| < \infty$. We choose such an N so as to maximize $\left|\overline{N}/N\right|$.

Suppose that $W \leq M \lhd_f G$. Put $D = N \cap M$. Then $\overline{D}N = \overline{N}$ so $\left|\overline{D}/(N \cap \overline{D})\right| = \left|\overline{N}/N\right|$ and as $N \cap \overline{D} \geq D$ it follows that $N \cap \overline{D} = D$. There are countably many possibilities for $\overline{D}$, since G is small; and given D, there are finitely many possibilities for M. Thus there are countably many possibilities for M.

Since there are countably many f-varieties it follows that G has countably many normal subgroups of finite index. The result follows by [SW], Theorem 2. ■

6 Generalized Fitting height: a reminder

In this section all groups are finite. The *generalized Fitting subgroup* of a group G is $F^*(G) = FE$ where $F = F(G)$ is the Fitting subgroup and $E = E(G)$ is the largest quasi-semisimple normal subgroup of G (to say that E is *quasi-semisimple* means that E is perfect and $E/Z(E)$ is a product of simple groups); E is more usually defined as the subgroup generated by the components of G, the quasisimple subnormal subgroups (that this is equivalent is a small exercise). It is always the case that $F \cap E = \mathrm{Z}(E)$ and $E/\mathrm{Z}(E)$ is semisimple; see [A], Chapter 11. Thus F^*/F is semisimple.

The *generalized Fitting height* $h(G)$ of G is defined by:

$$h(1) = 0, \qquad h(G) = 1 + h(G/F^*(G)).$$

It is not hard to see that $h(G)$ is the minimal length of a series of normal subgroups from 1 to G such that each factor is the product of a nilpotent normal subgroup and a quasi-semisimple normal subgroup; it follows that h is sub-additive on group extensions.

The first result is elementary. For a group Q the variety generated by Q is denoted $\mathcal{V}_Q$.

Proposition 4 *For each finite group Q there is an integer $m(Q)$ such that $G \in \mathcal{V}_Q$ implies $h(G) \leq m(Q)$.*

Proof. We define $m(Q)$ recursively: set $m(1) = 0$ and suppose that $m(L)$ has been found for every group L with $|L| < |Q|$.

If G is a finite group in $\mathcal{V}_Q$ then G is a section of $Q^{(n)}$ for some finite n, so $h(G) \leq h(H)$ where $H \leq Q^{(n)}$. It will suffice to find an upper bound for $h(H)$.

Let M be a maximal normal subgroup of Q and put $X = H \cap M^{(n)}$. Then $X \in \mathcal{V}_M$ and $H/X \cong HM^{(n)}/M^{(n)} \in \mathcal{V}_{Q/M}$, so if $M > 1$ we have

$$h(H) \leq h(H/X) + h(X) \leq m(Q/M) + m(M).$$

Thus if Q is not simple we may define $m(Q)$ to be the infimum of $m(Q/M) + m(M)$ where M ranges over the maximal normal subgroups of Q.

Now suppose that Q is simple. Write $\pi_i : H \to Q$ for the projection to the ith factor in the product and set $L_i = \ker \pi_i$. Say $H\pi_i = Q$ for $1 \leq i \leq r$ and

$H\pi_i = T_i < Q$ for $r < i \leq n$ (here r may be 0 or n). Put $X = L_1 \cap \ldots \cap L_r$. Then $H/X \cong Q^{(t)}$ for some $t \leq r$ and $X \leq P := T_{r+1} \times \cdots \times T_n$.

Now let $a = \max\{h(T) \mid T < Q\}$. Then P has a series of normal subgroups $1 = A_0 \leq B_1 \leq A_1 \leq \cdots \leq B_a \leq A_a = P$ with B_i/A_{i-1} nilpotent and A_i/B_i semisimple. Say $S_1, \ldots, S_s$ are all the non-abelian composition factors of proper subgroups of Q. Then

$$B_i = B_{i0} \leq B_{i1} \leq \cdots \leq B_{is} = A_i$$

where each B_{ij} is normal in P and $B_{ij}/B_{i(j-1)} \cong S_j^{(n_{ij})}$. Intersecting with X we obtain a normal series

$$\ldots A_{i-1} \cap X \leq B_i \cap X = X_{i0} \leq X_{i1} \leq \cdots \leq X_{is} = A_i \cap X \ldots$$

such that $(B_i \cap X)/(A_{i-1} \cap X)$ is nilpotent and

$$\frac{X_{ij}}{X_{i(j-1)}} \cong \frac{B_{i(j-1)}(X \cap B_{ij})}{B_{i(j-1)}} \in \mathcal{V}(S_j),$$

for each i and j.

It follows that

$$h((A_i \cap X)/(A_{i-1} \cap X)) \leq 1 + m(S_1) + \cdots + m(S_s) = b$$

say, and hence that $h(X) \leq ab$. As H/X is semisimple we may therefore define $m(Q) = 1 + ab$. ■

The next result is not elementary: it depends on CFSG – more precisely, it needs the Schreier Conjecture and the Odd Order Theorem. It also depends on the Hall-Higman Theorem (which it more or less implies, in a weak sense).

Theorem 10 *For each $q \in \mathbb{N}$ there is an integer $\delta(q)$ such that $G^q = 1$ implies $h(G) \leq \delta(q)$.*

Proof. Setting $\delta(1) = 0$ we may suppose that $q > 1$ and that $\delta(q')$ has been defined for all $q' < q$. Let G be a group satisfying $G^q = 1$.

If q is a prime power then G is nilpotent and $h(G) \leq 1$. Otherwise, let p be an odd prime divisor of $q = p^e r$ where $p \nmid r$.

Suppose first that G is soluble. According to Theorem A of [HH], G has p-length $l \leq 2e + 1$; so G has a normal series

$$1 = P_0 \leq N_0 < P_1 < \cdots < P_l \leq N_l = G$$

with each P_i/N_{i-1} a p-group and $N_i^r \leq P_i$. It follows that

$$h(G) \leq l(1 + \delta(r)).$$

Next, suppose that $\mathrm{Fit}(G) = 1$ and let $M = F^*(G)$. Then $M = S_1 \times \cdots \times S_n$ is a product of non-abelian simple groups. Let L be the kernel of the induced

permutation action of G on the set $\{S_1, , \ldots, S_n\}$. Since $\mathrm{C}_G(M) = 1$ (because $\mathrm{Fit}(G) = 1$) we see that L/M embeds into $\mathrm{Out}(S_1) \times \cdots \times \mathrm{Out}(S_n)$, whence L/M is soluble by the Schreier Conjecture, [GLS] Theorem 7.1.1.

The Odd Order Theorem ensures that S_1 has even order, and hence that q is even [FT]. A simple argument, given below, shows that $G^{q/2} \leq L$. It follows that

$$h(G) \leq 1 + l(1 + \delta(r)) + \delta(q/2).$$

In general, let H be the soluble radical of G. Then $\mathrm{Fit}(G/H) = 1$. Applying the two previous cases we deduce that $h(G) \leq \delta(q)$ where

$$\delta(q) = 1 + 2l(1 + \delta(r)) + \delta(q/2).$$

Proof that $G^{q/2} \leq L$ (copied from the proof of [HH], Theorem 4.4.1). Suppose that the claim is false. Say $2^e = t$ exactly divides q. Then there exists $g \in G$ with $g^{2^e} = 1$ and $g^{2^{e-1}} \notin L$. Thus g has order t modulo L. Hence g in its conjugation action has a cycle of length t on $\{S_1, , \ldots, S_n\}$, say $(S_1, , \ldots, S_t)$. Let $x \in S_1$ be an element of order 2. Then $S_1^{(xg)^i} = S_{1+i}$ centralizes S_1 for $1 \leq i < t$, so for $h \in S_1$ we have

$$h^{(xg)^t} = h^{xg.g^{t-1}} = h^x.$$

Choosing $h \in S_1 \setminus \mathrm{C}_{S_1}(x)$ we infer that $(xg)^t \neq 1$. But $(xg)^t = (x, x^g, \ldots, x^{g^{t-1}}) \in S_1 \times \cdots \times S_t$ is an element of order 2, so the order of xg is exactly $2t$; this contradicts $x^q = 1$. ■

It is not known whether the generalized Fitting height of all finite groups in an arbitrary non-trivial variety is uniformly bounded; it would suffice to settle this for soluble groups: see [Kh], Problem 2, Theorem 6, Theorem 7.

References

[A] M. Aschbacher, *Finite group theory,* CUP , 1986.

[FT] W. Feit and J. G. Thompson, Solvability of groups of odd order, *Pacific J.Math.* **13** (1963), 775-1029.

[GLS] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups, no.3*, American Math. Soc., Providence, Rhode Island, 1998.

[HH] P. Hall and G. Higman, On the p-length of p-soluble groups and reduction theorems for Burnside's problem, Proc. London Math. Soc. (3) **6** (1956), 1-42.

[HN] Hanna Neumann, *Varieties of groups,* Springer-Verlag, Berlin -Heidelberg-New York, 1967.

[Kh] E. I. Khukhro, Problems of bounding the p-length and Fitting height of finite soluble groups, *Journal of Siberian Federal University. Mathematics & Physics* **2**(3) (2009), 258–270.

[K] H. Koch, *Algebraic Number Theory,* Springer-Verlag, Berlin Heidelberg 1997.

[LS] A. Lubotzky and D. Segal, *Subgroup growth*, Birkhäuser, Basel, 2003.

[J] G. A. Jones, Varieties and simple groups, *J. Austral. Math. Soc.* **17** (1974), 163–173.

[N] N. Nikolov, Algebraic properties of profinite groups, arXiv:1108.5130.

[N2] N. Nikolov, Verbal width in anabelian groups, *Israel J. Math.* **216** (2016), 847-876.

[NS1] N. Nikolov and D. Segal, On finitely generated profinite groups, I: strong completeness and uniform bounds, *Annals of Math.* **165** (2007), 171–238.

[NS2] N. Nikolov and D. Segal, Powers in finite groups, *Groups, Geometry and Dynamics* **5** (2011), 501-507.

[NS3] N. Nikolov and D. Segal, Generators and commutators in finite groups; abstract quotients of compact groups, *Invent. Math.* **190** (2012), 513-602.

[P] H. L. Peterson, Discontinuous characters and subgroups of finite index, *Pacific J. Math.* **44** (1973), 683-691.

[S] D. Segal, *Words: notes on verbal width in groups,* London Math. Soc. Lecture Notes Series **361**, Cambridge Univ. Press, Cambridge, 2009.

[SW] M. G. Smith and J. S. Wilson, On subgroups of finite index in compact Hausdorff groups, *Arch. Math.* **80** (2003), 123-129.

[Z1] E. I. Zelmanov, The solution of the restricted Burnside problem for groups of odd exponent, *Math. USSR Izv.* **36** (1991), 41–60.

[Z2] E. I. Zelmanov, The solution of the restricted Burnside problem for 2-groups, *Mat. Sb.* **182** (1991), 568–592.