ALGEBRAIC PROPERTIES OF PROFINITE GROUPS

NIKOLAY NIKOLOV

ABSTRACT. Recently there has been a lot of research and progress in profinite groups. We survey some of the new results and discuss open problems. A central theme is decompositions of finite groups into bounded products of subsets of various kinds which give rise to algebraic properties of topological groups.

1. PROFINITE GROUPS

The classification of finite simple groups has transformed the study of finite groups and this in turn has brought a wealth of results about infinite groups with various finiteness conditions. One such obvious class is the residually finite groups. Frequently questions about such groups can be reduced to asymptotic properties of their finite images and a natural tool for studying these is the profinite groups.

A profinite group is a compact Hausdorff topological group G which is totally disconnected, i.e. any connected component of G is a singleton. It is a classical result due to van Dantzig [81] that the last condition is equivalent to the following: any open subset of G containing the identity contains an open normal subgroup. The diagonal embedding

$$i : G \to \prod_{N \lhd_o G} G/N$$

is a topological isomorphism and the image $i(G)$ is the inverse limit of the set $F(G) = \{G/N \mid N \lhd_o G\}$ of topological finite images of G.

Conversely the inverse limit $\varprojlim \Gamma_i$ of any inverse system of finite groups (Γ_i) is a profinite group. For details of these constructions and basic properties of profinite groups we refer the reader to [67], [77] or [83].

Profinite groups appeared first in number theory, in the first instance as a tool for studying congruences, namely the ring of p-adic integers $\mathbb{Z}_p$ and second as Galois groups of normal separable algebraic extensions. They form a part of the more general theories of compact groups and totally disconnected locally compact groups. For example the stabilizer of a vertex in the group of automorphisms of a locally finite tree is naturally a profinite group. Profinite groups feature in arithmetic geometry: the etale fundamental group $\pi(X)$ of a curve X of genus at least 2 defined over a number field k maps onto a $\mathrm{Gal}(k)$ and a famous conjecture of Grothendieck claims a bijection between the rational points $X(k)$ and the conjugacy classes of sections for this map, see [37].

Let us mention another important example, the compact p-adic analytic groups. For our purposes we can define them here as the closed subgroups of $GL_n(\mathbb{Z}_p)$. These groups were first studied by M. Lazard [43] as the non-archimedian equivalent of Lie groups, i.e. the compact topological groups which are analytic over $\mathbb{Z}_p$. This

was continued by Mann and Lubotzky, in particular they obtained the following group theoretic characterization of p-adic groups.

Theorem 1 ([16]). *A pro-p group G is p-adic analytic if and only if G has finite rank.*

Here and below by rank we mean Prüfer rank, i.e. the smallest integer d such that any subgroup of a finite topological quotient G/N of N is d-generated.

The applications of profinite groups in other branches of mathematics are often via profinite completions: Let Γ be a residually finite group. We can define the profinite topology on Γ by declaring the open sets to be the unions of cosets of subgroups of finite index of Γ. This makes Γ into a Hausdorff totally disconnected group and we can define $\hat{\Gamma}$ to be the completion of Γ with respect to this topology. A concrete way to construct $\hat{\Gamma}$ is as the closure of $i(\Gamma)$ in $\prod_N G/N$ where N ranges over all subgroups of finite index in G and i is the diagonal embedding of Γ. In this way Γ is a subgroup of its profinite completion $\hat{\Gamma}$ and properties of Γ can be deduced from those of $\hat{\Gamma}$. We can define the pro-p, pronilpotent or prosoluble completion of Γ in a similar way using the normal subgroups N of G such that G/N is a finite p-group, finite nilpotent or finite soluble group respectively.

A good illustration of the success of this approach is the Lubotzky's linearity condition (see [16], Interlude B).

Theorem 2. *A finitely generated group Γ is linear over a field of characteristic 0 if and only if there is a chain of normal subgroups $\Gamma > \Gamma_1 > \Gamma_2 \cdots$ of finite index in Γ with $\cap_i \Gamma_i = 1$ such that the inverse limit of the groups $\{\Gamma/\Gamma_i\}_i$ is a p-adic analytic group. Equivalently the family $\{\Gamma/\Gamma_i\}_i$ has bounded Prüfer rank.*

By contrast no such description is known for linear groups over fields of positive characteristic. Other applications of profinite groups include: the study of subgroup growth in residually finite groups [52], the congruence subgroup problem [51], the classification of p-groups of given coclass [44].

2. Profinite groups as profinite completions

We explained how a finitely generated residually finite group gives rise to a profinite group, namely its profinite completion. One may ask, conversely if every profinite group is the completion of some finitely generated residually finite abstract group. A moment's thought shows that the answer is no: The p-adic integers $\mathbb{Z}_p$ are not the profinite completion of any finitely generated group. We must change the question to: Which profinite groups are completions of finitely generated groups? Let us call such a profinite group a *profinite completion*. This is the same as asking: which collections of finite groups can be the images of some finitely generated residually finite group? The following example shows that we should not expect an easy answer:

Example: Let G be a profinite group with polynomial subgroup growth which is not virtually soluble. A discrete (respectively profinite) group G is said to have polynomial subgroup growth if there is some integer d such that G has at most n^d (open) subgroups of index n for each $n \in \mathbb{N}$.

Profinite groups with polynomial subgroup growth were characterised by Segal and Shalev, see Theorem 10.3 in [52]. For example we can take G to be a cartesian product $\prod_{i=1}^{\infty} PSL_2(p_i)$ for a fast increasing sequence of primes p_i. If G is the

completion of a residually finite finitely generated group Γ then Γ has polynomial subgroup growth as well. But then by a theorem of Mann, Lubotzky, Segal, (see [52] Theorem 5.1) Γ must be a virtually soluble group of finite rank and hence so is G, contradiction.

In fact a linearity criterion first proved by J. Wilson (see [52], Proposition 16.4.2 (ii)) shows that $\prod_{i=1}^{\infty} PSL_2(p_i)$ is not a profinite completion for any infinite sequence of primes p_i, see [73] for the full argument.

It is relaively easy to describe the nilpotent profinite groups which are profinite completions: These are the profinite groups commensurable with $\prod_p G(\mathbb{Z}_p)$ where G is a unipotent algebraic group defined over $\mathbb{Z}$.

There are only a few special classes of profinite groups which are known to be profinite completions, among them are iterated wreath products of finite simple groups and semisimple profinite groups. From now on we make the convention that a finite simple group means a *nonabelian* finite simple group.

Theorem 3 ([74]). *Let $S_1, S_2, \ldots$, be a sequence of nonabelian finite simple groups, each with a transitive action as a permutation group. Form the wreath product $W_k = S_1 \wr S_2 \wr \cdots \wr S_k$ and let G be the inverse limit of the groups W_k. Then G is a profinite completion.*

In [74] the proof assumes an extra condition on the actions of the S_i but this is unnecessary, see the remark in [52], page 266. In particular any collection of finite simple groups can be the composition factors of the finite images of some finitely generated residually finite group.

A profinite group G which is a Cartesian product of nonabelian finite simple group is called *semisimple*. The next example characterises the semisimple groups which are profinite completions.

Theorem 4 ([33]). *Let $G = \prod_{i=1}^{\infty} S_i$ be a semisimple profinite group which is topologically finitely generated. Then G is a profinite completion if and only if for each n only finitely many of the groups S_i are groups of Lie type of dimension n.*

The dimension of S_i is the dimension of the complex Lie algebra associated to the Lie type of S_i.

Another natural question is: Can two nonisomorphic residually finite groups have the same profinite completions? The answer is yes, even in the case of nilpotent groups, see [72], Chapter 11, Corollary 4. The following strong counterexample was constructed by Bridson and Grunewald [13] answering a question posed by Grothendieck:

Theorem 5. *There exist two finitely presented residually finite groups Γ_1, Γ_2 with an injection $i : \Gamma_1 \to \Gamma_2$ such that the induced map $\hat{i} : \hat{\Gamma}_1 \to \hat{\Gamma}_2$ is an isomorphism but Γ_1 and Γ_2 are not isomorphic.*

In [50] the authors show that counterexamples to Grothendieck's question as in Theorem 5 cannot exist within arithmetic hyperbolic 3-manifold groups and pose the following

Question 6. *Suppose that M_1 and M_2 are geometric 3-manifolds with infinite fundamental group for which the profinite completions $\widehat{\pi_1(M_1)}$ and $\widehat{\pi_1(M_2)}$ are isomorphic. Are M_1 and M_2 homeomorphic?*

It turns out that there exist uncountably many pairwise non-isomorphic finitely generated residually finite groups with the same profinite completion, see [62]. On the other hand it is a theorem of Grunewald, Pickel and Segal [22] that there are only finitely many polycyclic groups with a given profinite completion. Similar result has been proved by Aka [4] for simple arithmetic groups with the congruence subgroup property. However when we turn to more general classes of groups even the following is open, see [23]:

Question 7 (Remeslennikov). *A finitely generated residually finite group Γ has the same profinite completion as the free group on two generators F_2. Must Γ be isomorphic to F_2?*

If Γ is two generated then Γ must indeed be isomorphic to F_2: Any surjection $\pi : F_2 \to \Gamma$ gves rise to a surjection $\hat{\pi} : \hat{F}_2 \to \hat{\Gamma} \simeq \hat{F}_2$ of their profinite completions. Now a finitely generated profinite group G is non-Hopfian, i.e. any surjection from G to G is an isomorphisms. Therefore $\hat{\pi}$ is an isomorphism and hence so is π. So Question 7 is really about groups Γ which need more than 2 generators.

We remark that the analogous question for pro-p completions has a negative answer: There exist groups Γ which are not free but have the same set of nilpotent images as a free group. Such groups are called *parafree*, for examples see [9].

When we consider profinite completions of finitely presented groups there are a few more restrictions. First let us make two definitions. A group G is *large* if it has a subgroup of finite index H which maps homomorphically onto a nonabelian free group. Similarly G is said to be *p-large* for a prime p if H above can be taken to be a subnormal subgroup with $[G : H]$ a power of p. Clearly a large group G will have a lot of finite images, in particular any finite group will appear as an image of a finite index subgroup of G.

For a prime p a chain of subgroups (G_i) is called an abelian p-series of *rapid descent* if $G_i > G_{i+1} \geq G_i^p[G_i, G_i]$ for all $i \in \mathbb{N}$ and

$$\liminf_{i \to \infty} \frac{\dim_{\mathbb{F}_p} G_i/G_{i+1}}{[G : G_i]} > 0.$$

The following theorem has been proved by M. Lackenby in [40].

Theorem 8. *A finitely presented group G has an abelian p-series of rapid descent if and only if G is p-large.*

As a corollary if two finitely presented groups have isomorphic profinite completions then one of them is large if and only if the other is large.

3. Rigidity of profinite groups

Let G be a profinite group. What happens if we take the profinite completion of G itself? Since the open subgroups of G have finite index the profinite topology on G contains the original topology but could it be strictly stronger? In [77] Serre asked this question in the form: Assuming that G is (topologically) finitely generated is it true that every finite index subgroup of G open? Here and below we say that a profinite group is finitely generated if it contains a dense finitely generated subgroup.

Let us call a profinite group G *rigid* (or strongly complete) if every subgroup of finite index is open in G. It is easy to see that there exist non-rigid groups which

are not finitely generated. For example if $G = C_p^{\aleph_0}$ then G has $2^{2^{\aleph_0}}$ subgroups of index p of which only $\aleph_0$ are open. Even worse: the same abstract group can support two inequivalent topologies as a profinite group: The group $G = \prod_{i=1}^{\infty} C_{p^i}$ is abstractly isomorphic to $G_1 = G \times \mathbb{Z}_p$ but there is no continuous isomorphism between G and G_1. More generally in [35] J. Kiehlmann has classified all countably based abelian pro-p groups up to continuous and up to abstract isomorphisms.

When G is a finitely generated pro-p group then Serre himself proved in [77] that G is rigid. Increasing general cases were proved by Anderson [5], Hartley [26], Segal [71] until in 2003 the author and D. Segal answered Serre's question in the positive:

Theorem 9 ([56]). *Every finitely generated profinite group is rigid.*

In particular all homomorphisms between finitely generated profinite groups are automatically continuous and each such group is its own profinite completion.

4. WORD WIDTH IN FINITE AND PROFINITE GROUPS

The proof of Theorem 9 relies on *bounded width* of commutators and other words in finite groups.

It is a standart result observed by Brian Hartley that algebraic properties of a profinite group G are equivalent to asymptotic properties of the collection $F(G)$ of finite continuous images of G. For example G is topologically finitely generated if and only if there is some d such that any member of $F(G)$ is generated by d elements. For a subset X of G let us write

$$X^{*n} = \{x_1 \cdots x_n \mid x_i \in G\}$$

The following proposition is crucially used when proving that some subgroups of G are closed.

Proposition 10. *Let $X = X^{-1}$ be a closed subset of a profinite group G. The group $H = \langle X \rangle$ is closed in G if and only if there is some $n \in \mathbb{N}$ such that $H = X^{*n}$. In turn this condition is equivalent to $\bar{X}^{*n} = \bar{H}$ for the images $\bar{X}, \bar{H}$ of X and H in every $\bar{G} \in F(G)$.*

A typical application is where X is the set $G_q := \{x^q \mid x \in G\}$ of q-powers in G or the set of commutators $[x, y]$ in G. We can summarize the main results of [56] and [57] as follows.

Theorem 11. *Let $d, q \in \mathbb{N}$ and let Γ be a finite d-denerated group. There exist functions $f_1(d, q)$ and $f_2(d)$ such that*
    1. Every element of Γ^q is a product of at most f_1 powers x^q. i.e. $\Gamma^q = \Gamma_q^{*f_1}$.
    2. For a normal subgroup N of Γ the group $[N, \Gamma]$ generated by the set $Y = \{[n, g] \mid n \in N, g \in \Gamma\}$ is equal to Y^{*f_2}.

The proof of this theorem has recently been streamlined in [55] and we shall indicate some of the main ingredients in section 8 below. Proposition 10 now gives

Corollary 12. *Let G be a finitely generated profinite group. For any integer q and any closed normal subgroup N of G the algebraically defined subgroups G^q and $[N, G]$ are closed in G. In particular the terms of the lower central series $\{\gamma_i(G)\}_{i=1}^{\infty}$ of G are closed.*

Corollary 12 implies that G/G^q is a profinite group and therefore is an inverse limit of finite d-generated groups of exponent q. By the solution of the restricted Burnside problem by Zelmanov [85] the sizes of these finite groups are bounded, i.e. G/G^q is finite and therefore G^q is open. Theorem 9 is now an easy consequence:

Let H be a subgroup of index q in a finitely generated profinite group G. We want to prove that H is open. Without loss of generality we may assume that H is normal in G and hence $H \geq G^q$, which is open in G by the above argument. Hence H is open in G.

In fact the use of Zelmanov's theorem above was not strictly speaking necessary and it can be avoided if one just wants to prove Theorem 9. This was done in [56] (which was published before it was known that G^q is closed), and a simplified argument can be found in [55], section 5.1, using Theorem 36 below.

One might ask whether Corollary 12 extends to other algebraically defined subgroups of G, for example verbal subgroups. Let us make this more precise. Let $w = w(x_1, \ldots x_k)$ be an element of the free group on $x_1, \ldots, x_k$, we shall refer to w as a word in x_i. The set

$$G_w := \{w(g_1, \ldots, g_k)^{\pm 1} \mid g_i \in G\}$$

is called the set of values of w in G. It is clearly a closed subset of G when G is a profinite group. The verbal subgroup $w(G)$ is defined as $w(G) := \langle G_w \rangle$. The word w is said to have width at most n in a group G if $w(G) = G_w^{*n}$. Then the verbal subgroup $w(G)$ is closed in G if and only if there is some $n \in \mathbb{N}$ such that $w(\bar{G}) = \bar{G}_w^{*n}$ for all finite continuous images $\bar{G}$ in $F(G)$. If this is so we shall say that w has bounded width in the family $F(G)$.

Question 13. *For which words w it is true that $w(G)$ is closed in all finitely generated profinite groups G?*

This is equivalent to w having bounded width in all finite d-generated groups. Theorem 11 provides us with many such words:

Corollary 14. *Let $d \in \mathbb{N}$. Suppose that w is either a non-commutator word (i.e. $w \notin F'$) or the word $w = [x_1, x_2, \ldots, x_m]$. Then w has bounded width in all finite d-generated groups.*

Could the above corollary hold for all words? This is not true: Romankov [69] gave an example of 3-generated pro-p group G such that the second derived group G'' is not closed, i.e. the width of the word $[[x_1, x_2], [x_3, x_4]]$ is unbounded in d-generated finite p-groups. The most definitive description so far has been achieved by A. Jaikin-Zapirain [31] who has answered Question 13 for pro-p groups.

Theorem 15. *Let $w \neq 1$ be a word in a free group F. The following are equivalent:*
 1. $w(G)$ is closed in all finitely generated pro-p groups G.
 2. $w \notin F''(F')^p$.

Let us call a word w a J-word if $w \notin F''(F')^p$ for any prime p. It is clear that w must be a J-word for $w(G)$ to be closed in each finitely generated profinite group G. Is the converse true? No counterexample is known to this question. D. Segal [75] has proved that if w is a J-word then $w(G)$ is closed in all finitely generated soluble profinite groups G. Natural candidates to try next are the Engel words $[x_1, x_2, \ldots, x_2]$.

Could Question 13 have a positive answer for all words in some restricted class of groups? It turns out that this is the case if we consider only p-adic analytic groups:

Theorem 16. [31] *Let G be a compact p-adic analytic group and let w be any word. Then $w(G)$ is closed.*

L. Pyber has asked if this holds in greater generality for finitely generated adelic groups, i.e. closed subgroups of $\prod_p GL_n(\mathbb{Z}_p)$. Dan Segal [76] has answered this question in the positive for adelic groups which have the property FAb, i.e. every open subgroup has finite abelianization. A related question is:

Question 17. *Let w be a word and $r \in \mathbb{N}$. Is there $f = f(w, r)$ such that for any p-adic analytic group G of rank r the width of w in G is at most $f(w, r)$?*

The other extreme to p-groups is the family of finite simple groups. A finite simple group is generated by 2 elements, so Thereom 11 implies that the word width of any power word x_1^q or $[x_1, x_2]$ in the finite simple groups is bounded (a result proved in [53] and [70] earlier and in fact an essential ingredient in the proof of Theorem 11). Much better bounds are now known for *all* words.

Theorem 18 ([41]). *Let w be a word and S be a finite simple group. If the size of S is big enough as a function of w alone, then $S = S_w S_w$, i.e. w has width 2 in S.*

It follows that $w(G)$ is closed in all semisimple profinite groups G.

The obvious example $w = x_1^q$ with q dividing $|S|$ shows that 2 is the best possible bound in Theorem 18 in general. This is the essentially the only example we know where the word map is not surjective on finite simple groups. The following has been proved by Liebeck, Shalev, O'Brien and Tiep [47].

Theorem 19 (Ore Conjecture). *If S is a finite simple group then every element of S is a commutator.*

A. Shalev (private communication) has suggested the following problem: Let w be a word which is not a proper power. If S is a finite simple group of Lie type of large enough rank or a large alternating group then $S = S_w$.

4.1. **Word width in discrete groups.** Moving away from profinite groups let us say a few words about words in abstract groups. One of the first people to investigate word width was Philip Hall, who formulated a series of conjectures about verbal subgroups, see [68], Chapter 4.2. Hall's definition of elliptic words is the same as our definition of words of finite width we have adopted here. Hall's student P. Stroud [79] proved that any word has finite width in an abelian-by-nilpotent group. Independently Romankov [69] proved the same result for virtually polycyclic groups. D. Segal [75] recently extended this and proved that the word width in virtually soluble minimax groups is always finite.

One might expect that most words will have infinite width in a free group and this is indeed correct: A. Rhemtulla [65] showed that with the exception of trivial cases a word has infinite width in free products. This has recently been generalized to hyperbolic groups [54]. Some open problems remain:

Question 20. *Let Γ be a centre by metabelian group (i.e. $\Gamma/Z(\Gamma)$ is metabelian). Is it true that some word w has infinite width in Γ?*

Question 21. *Let Γ be a finitely generated soluble group. Is it true that the commutator word $[x_1, x_2]$ has finite width in Γ?*

This has been answered affirmatively by Rhemtulla [66] when Γ has derived length at most 3. It is open for the free soluble group on two generators of derived length 4.

5. Fibres of word maps

Let Γ be a finite or infinite group. We can consider a word $w \in F_k$ as a map $(g_1, \ldots, g_k) \to w(g_1, \ldots, g_k)$ from $\Gamma^{(k)} \to \Gamma$ and investigate the properties of this map.

For an element $g \in \Gamma$ let us write

$$P_\Gamma(w, g) = \frac{|\{\mathbf{x} \in \Gamma^{(k)} \mid w(\mathbf{x}) = g\}|}{|\Gamma|^k}$$

This is the probability of satisfying $w(\mathbf{x}) = g$ in Γ for a random k-tuple $x \in \Gamma^{(k)}$.

A word w is said to be *measure preserving* (in finite groups) if $P_\Gamma(w, g) = |\Gamma|^{-1}$ for all finite groups Γ and all $g \in \Gamma$. An example is any primitive word, i.e. an element of a free basis of the free group F_k. In fact a word w is measure preserving if and only if w is a primitive element in the free profinite group $\hat{F}_k$, see [61], Section 6.

T. Gelander has conjectured that conversely any measure preserving word must be primitive in F_k. D. Puder [61] proved this in the case of F_2. Very recently this has been extended by D. Puder and O. Parzanchevski to all words.

Theorem 22 ([60]). *Let $w \in F_k$. Then w is measure preserving in all finite groups if and only if w is primitive.*

Let us mention another intriguing open problem concerning the fibres of the word map. If Γ is abelian then the word map is a homomorphism and $P_\Gamma(w, e) = |w(\Gamma)|^{-1} \geq |\Gamma|^{-1}$, in particular $P_\Gamma(w, e)$ is bounded away from 0 for any word w. A. Amit (unpublished) asked whether this property characterizes all soluble groups. The combined results in [1] and [58] answer this affirmatively (without using the classification):

Theorem 23. *Let Γ be a finite group. Then Γ is soluble if and only if there exists $\epsilon > 0$ such that for any word $w \in F_k$ we have $P_\Gamma(w, e) \geq \epsilon$.*

Amit raised the following

Question 24. *Is it true that when Γ is a finite nilpotent group and $w \in F_k$ is a word then $P_\Gamma(w, e) \geq |\Gamma|^{-1}$?*

M. Levy [48] has answered this in the positive when Γ has nilpotency class 2. The general case remains open.

When we consider $P_\Gamma(w, g)$ for a finite simple group Γ, Larsen and Shalev [42]have proved the following with applications to subgroup growth and representation varieties.

Theorem 25. *Given a word w there is $\epsilon = \epsilon(w) > 0$ and $N = N(w)$ such that for any finite simple group S of size at least N and any $g \in S$ we have $P_S(w, g) < |S|^{-\epsilon}$.*

It turns out that some words are *almost measure preserving* in the finite simple groups. In order to define what this means, let us write for $X \subset G$ $P_G(w, X) = \sum_{g \in X} P_G(w, g)$.

Definition 26. *A word $w \in F_k$ is said to be almost measure preserving in a family $\mathcal{A}$ of finite groups if for any $\epsilon > 0$ there is $N = N(\epsilon)$ such that for any $G \in \mathcal{A}$ with $|G| > N$ and any subset $X \subset G$ we have*

$$|P_G(w, X) - \frac{|X|}{|G|}| < \epsilon.$$

In [19] S. Garion and A. Shalev show that the commutator word $[x_1, x_2]$ is almost measure preserving in all finite simple groups. This has diverse applications, in particular to Theorem 46 below. Similar result for the words $x_1^n x_2^m$ have been proved by M. Larsen and A. Shalev (work in preparation).

6. PROFINITE GROUPS OF TYPE IF

A finitely generated profinite group has only finitely many open subgroups of any given index. Let is call a profinite group with the latter property a group of type IF. Similarly let us define a profinite group to be of type AF if it has finitely many subgroup of any given finite index (which may or may not be open in G). Clearly AF implies IF and IF is equivalent to AF for rigid profinite groups.

A profinite group of type AF may not be finitely generated as the example $H = \prod_{n \geq 5} A_n^{(n!)^n}$ shows: It is clear that H has type IF while on the other hand from Theorem 18 it follows that H^q is open in H for any q which shows that H is rigid.

It is not too hard to show that a rigid profinite group G must have AF (and so also IF), a result first proved in [59]. Indeed otherwise G will maps topologically onto a Cartesian product $L = \prod_{i=1}^{\infty} S_i$ of isomorphic finite simple groups $S_i \simeq S$ (maybe abelian). Choose a non-principal ultrafilter $\mathcal{U}$ on $\mathbb{N}$ and consider the ultraproduct L/K where

$$K = \{(g_i) \in L \mid \text{ the set } \{i \mid g_i = e\} \in \mathcal{U}\}.$$

Then $L/K \simeq S$ and so K is a normal subgroup of finite index in L which is not open. Thus L is not rigid and neither is G. In fact [78] proves that a profinite group G is rigid if and only if it has type AF. One is led therefore to ask whether Theorem 9 can be generalized to all IF-groups, i.e. could it be that all IF-groups are rigid. However this is not true:

Proposition 27. *There exists a group of type IF which is not rigid.*

The idea of the proof is to use square width: Define $sw(G)$ to be the smallest integer k (if it exists) such that any element of G^2 is a product of k squares and set $sw(G) = \infty$ otherwise. We shall find a sequence of finite groups $\{\Gamma_n\}_{n=5}^{\infty}$ such that:
1. $\Gamma_n = \Gamma_n'$
2. Γ_n has a unique maximal normal subgroup K_n such that $\Gamma_n/K_n \simeq A_n$.
3. $sw(\Gamma_n) \geq n$.

If we then take $G = \prod_{n=5}^{\infty} \Gamma_n$ then condition 2 implies that G has type IF. On the other hand condition 3 and Proposition 10 imply that $G^2 \neq G$ hence G has a subgroup of index 2 which cannot be open by condition 1.

Let Q_n be a perfect finite group with $sw(Q_n) > 2n^2$. Such a group exists for any n by [30], Lemma 2.2. Put $\Gamma_n = Q_n \wr A_n = Q_n^{(n)} \rtimes A_n$. It is clear that Γ_n satisfies 1 and 2. As for the third condition I claim that $cw(\Gamma_n) \geq cw(Q_n)/2n \geq n$.

To prove this let $s = cw(\Gamma_n)$ and express the element $\mathbf{g} = (x, 1, 1, \cdots, 1) \in Q_n^{(n)}$ as a product of s squares in Γ_n:

$$\mathbf{g} = \prod_{i=1}^{s} (\mathbf{b}_i \pi_i)^2, \quad \mathbf{b}_i = (b_i(1), \ldots, b_i(n)) \in Q_n^{(n)}, \quad \pi_i \in A_n.$$

By collecting the elements of the base group to the left we reach the equation $\mathbf{g} = \prod_{i=1}^{s} \mathbf{b_i}^{\alpha_i} \mathbf{b_i}^{\beta_i}$ where α_i, β_i are some permutations from A_n. Now if we multiply together all the coordinates of the elements on both sides of this equation we reach the equation $x = U$ where U is product of elements $b_i(j) \in Q_n$ ($i = 1, \ldots, s$, $j = 1, \ldots, n$) in some order, each appearing exactly twice.

Now we only need to observe that by the proposition below U is a product of at most $2sn$ squares. Since $x \in Q_n$ was arbitrary this implies that $sw(Q_n) \leq 2ns = 2n \cdot sw(\Gamma_n)$ which was what we were after.

Proposition 28. *Let Γ be a group and let U be a product of length $2m$ of elements $c_1, \ldots, c_m$ in some order, each appearing exactly twice. Then U is a product of $2m - 1$ squares.*

Proof: Suppose that $U = c_r V_1 c_r V_2$, where $V_1 V_2$ does not involve c_r. Then

$$U = (c_r V_1)^2 V_1^{-2} V_1 V_2$$

and by induction we may assume that $V_1 V_2$ is a product of $2m - 3$ squares. $\square$

7. Presentations and cohomology

Let Γ be a finite group with generating set of minimal size equal to d. Then $\Gamma = F_d/N$ is a quotient of the free group F_d on the set $X = \{x_1, \ldots, x_d\}$ by a normal subgroup N. By a minimal presentation for Γ we mean a presentation $\langle X| \ R \rangle$ where R is a set of relators with $|R|$ as small as possible and we define $r(\Gamma) = |R|$.

At the same time Γ is a quotient of the free profinite group on X, $\hat{F}_d$. By a profinite presentation of Γ we mean a pair $\langle X|R_1 \rangle$ where $R_1 \subset \hat{F}_d$ such that $\Gamma \simeq \hat{F}_d/U$, with $U := \overline{\langle R_1^{\hat{F}_d} \rangle}$, the closed normal subgroup of $\hat{F}_d$ generated by R_1. Again a minimal profinite presentation is one where $|R_1|$ is as small as possible and we set $\hat{r}(\Gamma) = |R_1|$. We can view every abstract presentation of Γ as profinite presentation and this shows that $\hat{r}(\Gamma) \leq r(\Gamma)$. It is a well-known problem whether this is always an equality.

Question 29. *Is there a finite group Γ with $\hat{r}(\Gamma) < r(\Gamma)$?*

The motivation for this question is that unlike $r(\Gamma)$ the quantity $\hat{r}(\Gamma)$ can in theory be computed from the representation theory of Γ, a classic result of Gruenberg, for the formula see Proposition 16.4.7 of [52]. In particular for a finite p-group P $\hat{r}(P) = H^2(P, \mathbb{F}_p)$.

A case of interest is when Γ is a finite simple group: In [24] the authors show that $\hat{r}(\Gamma) \leq 18$ and $\hat{r}(A_n) \leq 4$. As for abstract presentation of finite simple groups in another paper [25] the same authors prove that $r(\Gamma) \leq 80$ with $r(A_n) \leq 8$.

Let us return to Serre's result that any finite index subgroup in a finitely generated pro-p group is open. It can be restated in the following way: any homomorphism from G to $(\mathbb{F}_p, +)$ is continuous.

For a profinite group G and a finite topological G-module M (which just means that $C_G(M)$ is open in G) define $H_c^n(G, M)$ to be usual cohomology group defined as the quotient $Z_c^n(G, M)/B_c^n(G, M)$ of the groups of continuous n-cocycles and n-coboundaries from G to M. Similarly, let $H_a^n(G, M)$ be the analogue defined without requiring continuity of the cocycles or coboundaries. It is easy to see that $H_c^n(G, M)$ embeds in $H_a^n(G, M)$. For example when M is a trivial module $H_c^1(G, M)$ is the additive group of continuous homomorphisms from G to $(M, +)$, while $H_a^1(G, M)$ is the group of all abstract homomorphisms.

Serre's result can now be restated as $H_c^1(G, F_p) = H_a^1(G, F_p)$ provided $H_c^1(G, F_p)$ is finite. It is natural to ask if the higher dimensional analogue of this holds.

Question 30. *Let G be a finitely presented pro-p group (i.e. $H_c^1(G, F_p)$ and $H_c^2(G, F_2)$ are finite). Is it true that $H_a^2(G, F_p) = H_c^2(G, F_p)$?*

It is not too hard to see that the condition thet G is finitely presented is necessary, see [17]. A case of special interest is when G is a p-adic analytic group, which has been answered affirmatively for Chevalley and soluble p-adic groups by [80]. Sury's result concerns non-compact Chevalley groups over $\mathbb{Q}_p$ and his methods have been extended to cover the compact Chevalley group $SL_2(\mathbb{Z}_p)$ as well by Barnea, Jaikin-Zapirain and Klopsch (work in preparation). Another of their results is that a positive answer to Question 30 for free pro-p groups implies a positive answer in general for all finitely presented pro-p groups.

The groups $H^2(G, \mathbb{F}_p)$ (abstract or continuous) parametrize the equivalence classes of (abstract or continuous) extensions of F_p by G. Thus the following are equivalent for a pro-p group G:

1. $H_a^2(G, F_p) = H_c^2(G, F_p)$.
2. Any central extension of C_p by G (i.e. a group K with a normal central subgroup C of order p such that $K/C \simeq G$) is isomorphic to a pro-p group.
3. Any central extension of C_p by G is residually finite.

Using this now it is immediate that $H_a^2(G, F_p) \neq H_c^2(G, F_p)$ when G is not finitely presented: Let $G = F/N$ where F is a finitely generated free pro-p group and N is a closed normal subgroup. If G is not finitely presented then $N/[N, F]N^p$ is infinite elementary abelian pro-p group and hence it has a subgroup $N > K > [N, F]N^p$ of index p in N which is not closed. This F/K is an extension of $C_p = N/K$ by $G = F/N$ which is not residually finite.

Similarly one can prove the following:

Proposition 31. *Let G be a pro-p group which is an extension of finitely generated pro-p group N by a finitely generated profinite group $H = G/N$. Suppose that $H_a^2(N, F_p) = H_c^2(N, F_p)$ and $H_a^2(U, F_p) = H_c^2(U, F_p)$, for any open subgroup U of H. Then $H_a^2(G, F_p) = H_c^2(G, F_p)$.*

Proof: First note that the condition on H implies that any extension E of a finite p-group P by H is residually finite and so topological. This is proved by induction on $|P|$ the case when $P = C_p$ being part of the assumptions. For the induction step let Z be the centre of P. Then $H = E/P$ acts on the finite group Z, so by replacing H by an open subgroup (and E by a finite index subgroup) we may assume that

$Z \leq Z(E)$. Let C be a subgroup of order p in Z, then by considering E/C and the induction hypothesis we may assume that E/C is residually finite and in particular E has a finite index subgroup E_1 with $E_1 \cap P = C$. Then $E_1/C \simeq E_1 P/P$ is isomorphic to an open subgroup of H, so by assumption E_1 is a redisually finite extension, so there is a finite index subgroup K of E_1 with $C \cap K = 1$. This implies that E itself is residually finite.

Now we can easily finish the proof: Let $C_p \lhd J \lhd K$ be an extension of $C_p \leq Z(K)$ by $G \simeq K/C_p$ where $K/J \simeq H$ and $J/C_p \simeq N$. Since G is residually finite it is enough to find a subgroup M of finite index in K with $C_p \cap M = 1$. From the assumption on N we know that J is residually finite and finitely generated topologically, thus we may find a subgroup $S \leq J$ with $[J : S] < \infty$, such that $S \lhd K$ and $S \cap C_p = 1$. Consider now K/S which is an extension of the finite p-group J/S by $H \simeq K/J$ and so by the argument above there is some finite index subgroup M/S in K/S with $1 = M/S \cap (C_p S)/S = (M \cap C_p S)/S$, this $C_p \cap M = 1$. $\square$

Proposition 31 shows that Question 30 for p-adic analytic groups reduces to the case when G is a simple p-adic analytic group i.e. whose Lie algebra is simple. A first test case will be $G = SD^1(\Delta_p)$, the group of norm 1 elements in the quaternion division algebra over $\mathbb{Z}_p$. For definition of this group see Exercise 9.3 in Chapter I of [36].

8. STRANGE IMAGES OF PROFINITE GROUPS

In this section we present some recent results of D. Segal and the author in [55]. Let G be a finitely generated profinite group. We can interpret Theorem 9 as saying that every finite quotient of G is topological. What can we say about other quotients? Suppose first that G/N is a residually finite quotient, then it must be a profinite group. Indeed N is an intersection of finite index subgroups each of which is open and hence closed in G. Therefore N is a closed subgroup of G i.e. the induced topology on G/N makes it into a profinite group. As a consequence G cannot have a countably infinite residually finite quotient.

Could it be that G has a countably infinite quotient? The answer is perhaps surprisingly yes. For example let $G = \prod_{p \in P} \mathbb{F}_p$ (product over the set P of all primes p). Take a non-principal ultrafilter on P and let G/K be the ultraproduct. Then G/K is an field of characteristic 0, which maps onto $\mathbb{Q}$ as an additive group. Therefore $(\mathbb{Q}, +)$ is an image of G. Similar argument shows that $\mathbb{Z}_p$ maps onto $\mathbb{Q}$ (use that $\mathbb{Q}_p$ is a vector space over $\mathbb{Q}$). More generally any infinite abelian profinite group has a countable infinite image.

Let us then put a further restriction on the image: Could a profinite group have a finitely generated infinite image? The answer is no, even more generally for compact Hausdorff groups:

Theorem 32. [55] *Let G be a compact group and N a normal subgroup of (the underlying abstract group) G such that G/N is finitely generated. Then G/N is finite.*

We can in addition provide some information about possible countable images:

Theorem 33. *Let G be a finitely generated profinite group. Let N be a normal subgroup of (the underlying abstract group) G. If G/N is countably infinite then G/N has an infinite virtually-abelian quotient.*

The last condition implies that G has an open subgroup K such that K/K' is infinite. This is also easily seen to be sufficient for the existence of countable infinite quotients:

Corollary 34. *Let G be a finitely generated profinite group. Then G has a countably infinite quotient if and only if some open subgroup of G has infinite abelianization.*

Note that if G/N is countable then $\bar{N}$ is open in G. We say that a normal subgroup N is *virtually dense* in G if $[G : N]$ is infinite and the closure of N is open in G. For example, when G is abelian or semisimple then G has a dense normal subgroup. In the latter case we can take $N = \oplus_i S_i$ in $G = \prod_i S_i$. In fact the existence of virtually dense normal subgroups is described by these examples.

Corollary 35. *A finitely generated profinite group has a virtually dense normal subgroup if and only if it has an open normal subgroup H which has an infinite abelian quotient or an infinite semisimple quotient.*

The key to proving the above results is the following result about finite groups proved in [55]. For a finite group Γ we denote the derived group by Γ' and write Γ_0 for the intersection of the centralizers of the non-abelian simple chief factors of Γ.

Theorem 36. [55] *Let Γ be a finite group, $H \leq \Gamma_0$ a normal subgroup of Γ, and $\{y_1, \ldots, y_r\}$ a symmetric subset of Γ. If $H \langle y_1, \ldots, y_r \rangle = \Gamma' \langle y_1, \ldots, y_r \rangle = \Gamma$ then*

$$[H, \Gamma] = \left(\prod_{i=1}^{r} [H, y_i] \right)^{*f}$$

where $f = f(r, \mathrm{d}(\Gamma)) = O(r^6 \mathrm{d}(\Gamma)^6)$.

If $\{y_1, \ldots, y_r\}$ actually generates Γ then the above equality holds for every H (not necessarily inside Γ_0).

Now Γ/Γ_0 is semisimple-by-(soluble of derived length ≤ 3), while Γ/Γ' is abelian: so the theorem reduces certain problems to the case of semisimple groups and abelian groups.

As an application let us indicate how to deduce Theorem 11 from Theorem 36. Part (2) of Theorem 11 follows just by setting $H = N$ and $y_1, \ldots y_d$ to be a symmetric generating set of Γ. Part (1) of Theorem 11 needs a little more work. For a finite d-generated group Δ we set $\Gamma := \Delta^q$. The index of Γ in Δ is bounded in terms of d and q and so Γ can be generated by some $f_1(d, q)$ elements. Moreover we can choose a symmetric set $y_1, \ldots, y_r$ with r bounded in terms of d, q such that each $y_i = x_i^q$ for some $x_i \in \Delta$ and $y_1, \ldots, y_r$ generates Γ modulo Γ' and modulo Γ_0. (Using a version of Theorem 11 for finite semisimple and finite soluble groups which were proved earlier) Then Theorem 36 with $H = \Gamma_0$ implies that every element of $[\Gamma_0, \Gamma]$ is a product of boundedly many copies of $[\Gamma_0, y_i]$. Since $[x, y_i] = y_i^{-x} y_i$ is a product of two q-th powers it follows that $[\Gamma_0, \Gamma]$ is a product of boundedly many q-th powers. It remains to deal with $\Gamma/[\Gamma_0, \Gamma]$ which is easy. The full details can be found in [55] Theorem ??.

An easy consequence of Theorem 36 is

Corollary 37. *Let G be a finitely generated profinite group and N a normal subgroup of G. If $NG' = NG_0 = G$ then $N = G$. Here G_0 is the intersection of all open normal subgroups M such that G/M is almost simple.*

Indeed, we may choose elements $y_1, \ldots, y_{2d}$ from N such that $\overline{\langle y_1, \ldots, y_{2d} \rangle}$ projects onto G/G' and G/G_0. The profinite analogue of Theorem 36 now implies that for the integer f defined there we have

$$[G_0, G] = (\prod_i [G_0, y_i])^{*f}$$

In particular $[G_0, G] \leq N$ since $y_i \in N$. Therefore

$$G' = [G, NG_0] \leq [G, N][G, G_0] \leq N$$

hence $G = NG' = N$.

Corollary 37 shows that if G has a 'strange' normal subgroup, then either G/G' or G/G_0 has one: and these groups are not so hard to understand. Let us illustrate

this by proving Theorem 32 at least for profinite groups G. The general case is obtained by observing that if a compact group G has a finitely generated infinite image then either G/G^0 of G^0 has such image, where G^0 denotes the connected component of the identity in G. Now G/G^0 is a profinite group, while G^0 is a pro-Lie group [29]; in the latter case an analogue of Proposition 38 below for Lie groups suffices to complete the proof.

So let us assume that G is a profinite group with infinite finitely generated image I. By considering the closed subgroup of G containing preimages of the generators of I we reduce to the case when G is topologically finitely generated. Let I_1 be the intersection of all subgroups of finite index in I. Then I/I_1 is a residually finite countable image of G and therefore finite by the argument at the beginning of this section. Thus by replacing I with I_1 and G with the preimage of I_1 we may further assume that I has no finite images.

In order to apply Corollary 37 we need to be able to understand the countable images of G/G_0, which is a semisimple by soluble profinite group.

Proposition 38. *Let $G = \prod_{i \in X} S_i$ be a finitely generated semisimple profinite group. Then any infinite image of G is uncountable.*

Assuming this we can complete the proof of Theorem 32. Let N be a normal subgroup of G such that $G/N \simeq I$ is a finitely generated countable group without finite images. Then $I = I'$ and hence $G'N = G$. Suppose that $NG_0 < G$, then G/G_0 maps onto a nontrivial factors of I which must be infinite. It follows that the group $\bar{G} = G/G_0$ has an infinite finitely generated perfect quotient. Let V be the semisimple normal subgroup of $\bar{G}$ such that $\bar{G}/V$ is soluble of derived length 3. Clearly G/V cannot have a nontrivial perfect quotient, therefore V must have an infinite finitely generated quotient. This contradicts Proposition 38 and Theorem 32 follows.

Finally let us indicate a proof of Proposition 38. This proceeds by describing the maximal normal subgroups of a semisimple profinite group $G = \prod_{i \in X} S_i$. For this we need the following result of Liebeck and Shalev:

Theorem 39 ([46]). *There is a constant c with the following property: If S is a nonabelian finite simple group and C is a nontrivial conjugacy class of S then $C^n = S$ for some integer $n \leq c \log |S| / \log |C|$.*

Now let $\mathcal{U}$ be an ultrafilter on the index set X. We define a normal subgroup $N_{\mathcal{U}}$ of G as follows: first define a function $h : G \to [0,1]$ by

$$h((g_i)) = \lim_{\mathcal{U}} \frac{\log |g_i^{S_i}|}{\log |S_i|}$$

where $\lim_{\mathcal{U}}$ denotes the ultralimit with respect to $\mathcal{U}$, then set $N_{\mathcal{U}} = h_{\mathcal{U}}^{-1}(0)$. Using Theorem 39, one shows that the subgroups $N_{\mathcal{U}}$ are precisely the maximal proper normal subgroups of G. Proposition 38 is then deduced by eliminating the possibility $H \leq N_{\mathcal{U}}$ when G/H is countably infinite.

9. AN APPLICATION: LOCALLY COMPACT TOTALLY DISCONNECTED GROUPS

Profinite groups appear as open subgroup of locally compact totally disconnected (abbreviated lctd) groups. By contrast with profinite groups Corollary 12 does not hold even for very 'nice' lctd groups as the following example noticed by D. Segal shows. Let G be the group

$$G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a,b \in \mathbb{Z}, c \in \mathbb{Z}_p \right\}$$

where $\mathbb{Z}$ has the discrete topology while $\mathbb{Z}_p$ has the p-adic topology. Then G and its compact open subgroup $\mathbb{Z}_p$ are both finitely generated topologically, however $G' = \mathbb{Z} < \mathbb{Z}_p$ is not closed in G.

However the situation may be different for topologically simple tdlc groups (i.e. groups which do not have a nontrivial normal *closed* subgroups). Perhaps the most natural question to ask is whether these groups are abstractly simple. Note that any non-trivial normal subgroup of a topologically simple group must be dense. In [14] Caprace and Monod pose the following

Question 40. *Is there a compactly generated, topologically simple locally compact group which has a proper dense normal subgroup?*

The methods from the previous section provide some information in the case when the topologically simple group is compactly generated and locally finitely generated (i.e its open compact subgroups are finitely generated).

Proposition 41. *Let L be a compactly generated, locally finitely generated tdlc group without compact normal subgroups. Let G be a compact open subgroup of L and let N be a dense normal subgroup of L. Then $N \geq G'$. In particular L is abstracly simple if and only if L is abstractly perfect.*

Proof: Suppose that L is generated by a compact set K. Without loss of generality we may assume that $K = K^{-1} = GKG$. Let $\mathcal{G}$ be the Schreier graph of L with respect to K and U. The vertices of $\mathcal{G}$ are $\{Ga \mid a \in L\}$ and the edges are the pairs (Ga, Gka) for $k \in K$. Our group L acts transitively on the vertices of $\mathcal{G}$ with stablizer of the vertex $v_0 = G$ equal to G. By assumption L has no non-trivial compact normal subgroups hence the action of L on G is faithful. The valency at every vertex of $\mathcal{G}$ is $|K : U| < \infty$, in particular there are only finitely possibilities for the upper composition factors of G (that is the composition factors of G/N for open normal subgroups N of G). We conclude that G/G_0 is finite while G/G' has only finitely many nontrivial Sylow subgroups. It follows that there is a finite index

subgroup $G > F > G'$ such that for a closed subgroup M of G $G = MF$ implies $G = MG'$.

Suppose N is a dense normal subgroup of L and put $H = G \cap N$, then H is a dense normal subgroup of G. Since F and G_0 are open subgroups of G we have that $G = G_0 H = FH$. Thus we can find finitely many elements $y_1, \ldots y_r \in H$ such that

$$\overline{\langle y_1, \ldots y_r \rangle} G_0 = G = \overline{\langle y_1, \ldots y_r \rangle} F$$

and the last equality implies that $\overline{\langle y_1, \ldots y_r \rangle} G' = G$. We can now deduce as in the proof of Corollary 37 that $H > [G_0, G]$. Finally $G' = [G, HG_0] \le H[G, G_0] \le H$ as before. Since N is dense in L we have that $L/N = GN/N = G/H$ is abelian. $\square$

In [8] the authors study commensurators of profinite groups and one aspect of this is the following question: Which profinite groups can be the compact open subgroups of topologically simple tdlc groups? By the proof of Proposition 41 such a profinite group G has only finitely many different upper composition factors. In particular G cannot be a free profinite group. It is shown in [8] that the above question has a positive answer for the Grigorchuk group and negative for the Nottingham group. Another negative answer was proved by G. Willis [82]: a soluble profinite group cannot be an open subgroup of a compactly generated simple tdlc group, moreover the condition of being compactly generated is necessary. The following concrete question is asked in [8].

Question 42. *Let G be the free pro-p on 2 generators. Can G be an open subgroup in a topologically simple lctd group?*

Next we discuss some of the main ingredients in the proof of Theorem 36.

10. Elements of the proof of Theorem 36

The most natural approach is to use induction on $|\Gamma|$. Suppose for example that H in Theorem 36 is an minimal normal subgroup of Γ, with the property that $H = [H, \Gamma]$.

Then a necessary condition on the y_i is that at least one of the sets $[H, y_i]$ is not too small, i.e. y_i does not centralize a subgroup of H of big Hausdorff dimension. Now either H is elementary abelian and then each y_i acts on H as a linear transformation, or H is a direct product of isomorphic simple groups and y_i acts by permuting the factors and twisting them with some automorphisms. This motivates the following definition:

Let the group $\langle Y \rangle$ generated by a set Y act on either

(1) a set Ω, or
(2) a vector space V.

In situation (1) we say that Y has (ϵ, k) *fixed point property* on Ω if at least k of the elements of Y fix at most $(1 - \epsilon)|\Omega|$ of the points in Ω. Similarly in situation (2) Y has the (ϵ, k) *fixed space property* on V if at least k of the elements of Y have centralizer of dimension at most $(1 - \epsilon) \dim V$.

One of the main new ingredients is a result which guarantees that a set $Y \subset \Gamma$ has the (ϵ, k)-fixed point and fixed space property on the non-central chief factors of Γ provided Y generates Γ modulo Γ' and modulo Γ_0:

Theorem 43. *Let Γ be a finite group with a subset Y such that $\Gamma = \Gamma' \langle Y \rangle = \Gamma_0 \langle Y \rangle$. Then Y has the $\varepsilon/2$-fsp on every non-central abelian chief factor of Γ and the ε-fgp on every non-abelian chief factor of Γ inside Γ_0, where*

$$\varepsilon = \min \left\{ \frac{1}{1 + 6\delta}, \frac{1}{|Y|} \right\}.$$

This allows to prove the following.

Theorem 44. *Let G be a group and $K \leq G_0$ a normal subgroup of G. Suppose that $G = K \langle y_1, , \ldots, y_r \rangle = G' \langle y_1, , \ldots, y_r \rangle$. Then there exist elements $x_{ij} \in K$ such that*

$$G = \left\langle y_i^{x_{ij}} \mid i = 1, \ldots, r, \; j = 1, \ldots, f_0 \right\rangle$$

where $f_0 = f_0(r, \mathrm{d}(G)) = O(r\mathrm{d}(G)^2)$.

Let us now consider the situtation where H in Theorem 36 has a minimal elementary abelian subgroup $M \lhd \Gamma$ with $[M, \Gamma] = M$. Suppose $h \in H$. By induction and considering the smaller group Γ/M we may assume that we have found elements $a_{i,j} \in H$ such that for some $m \in M$ we have

$$hm = \prod_{i=1}^{f} \prod_{j=1}^{r} [a_{i,j}, y_j]$$

Let us replace $a_{i,j}$ by $a_{i,j} x_{i,j}$ with some $x_{i,j} \in M$. By collecting the terms involving $a_{i,j}$ to the left we reach the equation

(1) $$m = \prod_{i=1}^{f} \prod_{j=1}^{r} [x'_{i,j}, z_{i,j}]$$

where each $z_{i,j}$ is specific conjugates of y_j depending on $x_{i,j}$ and $a_{i,j}$ and similarly for $x'_{i,j}$. In order to be able to solve this equation in terms of $x'_{i,j}$ we assume that the elements $y_{i,j}$ generate G/M and put this condition in the induction hypothesis for Γ, see Key Theorem in [55] Theorem 3.10. But then when solving (1) for M we need to ensure that the extra condition that $z_{i,j}$ generate Γ is satisfiied. We do this by counting the solutions of (1) and comparing this with the number of conjuagtes of y_i whcih fail to generated Γ. The counting is relatively straightforward when M is a minimal normal subgroup as above (i.e. M is abelian and $M = [M, \Gamma]$) but if $[M, \Gamma] = 1$ or when M is semisimple it gets much more complicated. To deal with the situation when $M \leq Z(\Gamma)$ the methods developed earlier in [56] suffice. When M is semisimple we need better lower estimates for the number of solutions to the equation (1) than the ones in [56].

This leads us to the subject of growth in finite simple groups and the following generalization of the 'Gowers trick' by Babai, Nikolov and Pyber in [6]:

Theorem 45. *For a finite group G let $l = l(G)$ denote the minimal degree of a nontrivial real representation of G. Suppose now that $k \geq 3$ and $A_1, \ldots, A_k$ are subsets of G with the property that $\prod_{i=1}^{k} |A_i| \geq |G|^k / l^{k-2}$. Then $\prod_{i=1}^{k} A_i = G$.*

This is a key ingredient in the proof of Theorem 47 below. To make sure that the conditions of the Gowers trick are met we prove the following result concerning twisted commutators of finite simple groups:

For automorphisms α, β of a group G and $x, y \in S$ we write

$$T_{\alpha,\beta}(x,y) = x^{-1}y^{-1}x^\alpha y^\beta.$$

Theorem 46. *There exist $\varepsilon > 0$ and $D \in \mathbb{N}$ such that if S is a finite quasisimple group with $l = l(S) > 2$, $\alpha, \beta \in \mathrm{Aut}(S)^{(D)}$, and $X \subseteq S^{(2D)}$ has size at least $(1 - \varepsilon) \left| S^{(2D)} \right|$, then*

$$|\mathbf{T}_{\alpha,\beta}(X)| \geq l^{-3/5}|S|$$

Note that there are only finitely many quasisimple groups with $l(S) \leq 2$.

The last two theorems combined with some further work give

Theorem 47. *Let D and ϵ be the constants introduced in Theorem 46. Let N be a finite quasisemisimple group with at least 3 non-abelian composition factors. Let $\mathbf{y}_1, \ldots, \mathbf{y}_{10}$ be m-tuples of automorphisms of N. Assume that for each i, the group $\langle \mathbf{y}_i \rangle$ permutes the set Ω of quasisimple factors of N transitively and that $\mathbf{y}_i$ has the (k, η)-fpp on Ω, where $k\eta \geq 4 + 2D$. For each i let $W(i) \subseteq N^{(m)}$ be a subset with $|W(i)| \geq (1 - \varepsilon/6) |N|^m$. Then*

$$\prod_{i=1}^{10} W(i)\phi(i) = N$$

where $\phi(i) : N^{(m)} \to N$ is given by

$$(x_1, \ldots, x_m)\phi(i) = \prod_{i=1}^{m} [x_i, y_{ij}].$$

This last theorem provides the induction step in the proof of Theorem 36 in the case when $M \leq H$ is a nonabelian minimal normal subgroup of G.

11. Growth in finite simple groups

A common theme in this survey has been product decompositions of finite and profinite groups, and how these relate to algebraic properties of infinite groups. Most useful are results of the following kind:

Suppose that Γ is a finite group and $X_1, \ldots X_n$ are subsets of Γ. If

$$\sum_{i=1}^{n} \log |X_i| > C \log |\Gamma|$$

for some constant C and X_i generate G we want to deduce that $X_1 \cdots X_n = \Gamma$. Of course this result in not true in all finite groups, the cyclic abelian groups being a counterexample.

However when we turn to the other extreme, finite simple groups then we expect positive answers. For example if X_i are all equal to a conjugacy class in Γ and Γ is a finite simple group this is the content of Theorem 39.

A very influential problem in the area is the Babai Conjecture [7]:

Conjecture 48. *There is a constant $C > 0$ such that if S is a finite simple group and $X = X^{-1}$ is a generating set for S then the diameter of the Cayley graph $Cay(S, X)$ is at most $(\log |S|)^C$.*

Note that when $1 \in X$ the Babai conjecture is equivalent to $S = X^{*n}$ for some integer $n < (\log |S|)^C$.

The conjecture was proved in the positive by Helfgott [27] for $PSL_2(\mathbb{F}_p)$ and subsequently extented in [28] to PSL_3 and other non-prime fields by Dinai [15]. Recently Breuillard, Green and Tao [11] and at the same time Pyber and Szabo [63] have proved the Babai Conjecture for all finite simple group of bounded Lie rank. Both papers prove a *Helfgott type* estimate on the growth of subsets in simple groups. Rather than define what we mean by this we give a statement of one of the main theorem in [63], or equivalently Corollary 2.4 in [11].

Theorem 49. *Let S be a finite simple group of Lie type of rank r and A a generating set of L. Then either $AAA = L$ or $|AAA| > \delta |A|^{1+\epsilon}$ where ϵ, δ depend only on r.*

Results of this type together with sieve methods developed by Bourgain, Gamburd and Sarnak [10] play an important role in the construction of expanders as Cayley graphs in finite simple groups of bounded Lie rank. For example this was how the Suzuki finite simple groups were shown to be a family of expanders in [12]. For details about this fascinating and rapidly evolving subject we point the reader to the survey by B. Green [21].

Expressing a finite simple group as a product of few of its subgroups has been used to construct expanders in large rank as well, see [32] and the references therein. Let us mention a very general conjecture made in [45].

Conjecture 50. *There exists an absolute constant c such that if S is a finite simple group and A is any subset of S of size at least two, then S is a product of N conjugates of A for some $N < c \log |S| / \log |A|$.*

This conjecture can be viewed as a direct generalization of Theorem 39 from conjugacy classes to subsets. Some special cases are known, for example it holds for specific subgroups A of G, or when $|A|$ is bounded. Most notably its validity has recently been proved for simple groups of bounded rank in [20].

12. Rank gradient

We saw that some properties of Γ cannot be deduced from its profinite completion $\hat{\Gamma}$, for example $\hat{\Gamma}$ does not determine Γ up to an isomorphism. Another such example is $d(\Gamma)$, the minimal number of generators of Γ, which cannot be found from knowledge of $d(\hat{\Gamma})$ alone: For any integer n there exists a residually finite group Γ such that $d(\Gamma) = n$ but $\hat{\Gamma}$ (equivalently every finite image of Γ) is 3-generated, see [84]. It is thus surprising that the growth of $d(H)$ for subgroups of finite index in Γ can be recovered from the knowledge of $\hat{\Gamma}$ plus some extra information: the action of Γ on its profinite completion. Let us make this precise.

Let Γ be a finitely generated group and (Γ_i) a chain of subgroups in Γ. The *rank gradient* of Γ with respect to (Γ_i) is defined as

$$\mathrm{RG}(\Gamma, (\Gamma_i)) = \lim_{i \to \infty} \frac{d(\Gamma_i) - 1}{[\Gamma : \Gamma_i]}$$

where $d(\Gamma)$ denotes the minimal number of generators of Γ. This notion has been introduced by Marc Lackenby [39] in the study of hyperbolic 3-manifolds and the virtually Haken conjecture. A natural question is whether the rank gradient depends on the choice of the normal chain in Γ.

Conjecture 51. *If* (Γ_i) *and* (Δ_i) *are two normal chains in* Γ *with trivial intersection then* $\mathrm{RG}(\Gamma, (\Gamma_i)) = \mathrm{RG}(\Gamma, (\Delta_i))$.

Conjecture 51 is relevant the following well-known problem in 3-dimensional topology which dates back to Waldhausen: *Is there a closed hyperbolic* 3-*manifold* M *such that* $d(\pi_1(M)) \neq g(M)$*? (where* $\pi_1(M)$ *is the fundamental group of* M *and* $g(M)$ *is the Heegaard genus of* M*)* This has recently been solved by T. Li:

Theorem 52 ([49])**.** *For any fiven* $n \in \mathbb{N}$ *there exists a closed orientable hyperbolic* 3-*manifold* M *such that* $g(M) - d(\pi_1(M)) > n$.

As explained in [3] the truth of Conjecture 51 together with results of M. Lackenby [38] and A. Reid [64] implies an even stronger result: the ratio $d(\pi_1(M))/g(M)$ can be arbitrarily small for closed hyperbolic 3-manifolds M. For this application it will be enough to prove Conjecture 1 for free-by-cyclic groups.

Conjecture 51 is closely related to the subject of measurable group actions and in particular the notion of *cost* as introduced by Levitt and developed by Gaboriau in [18]. Let X be a probability measure space. Let Γ be a group acting on X by measure preserving transformations. Assume that the action of Γ on X is ergodic and essentially free. As explained in [18] and also in [34] one can define an invariant $\mathrm{cost}(\Gamma, X)$, the cost of the action of Γ on X. This invariant has been used by Gaboriau to prove that two finitely generated free groups have measure equivalent actions if and only if they are isomorphic. It turns out that rank gradient is connected to cost via the following result from [3]:

Theorem 53. *Suppose* (Γ_i) *is a normal chain with trivial intersection in a finitely generated group* Γ*. Let* $\widehat{\Gamma} = \varprojlim_i \Gamma/\Gamma_i$ *be the completion of* Γ *with respect to* (Γ_i) *and let* Γ *act on* $\widehat{\Gamma}$ *by left translations. Then*

$$\mathrm{RG}(\Gamma, (\Gamma_i)) = \mathrm{cost}(\Gamma, \widehat{\Gamma}) - 1.$$

There is not a single group known which has two (essentially free) measurable actions with different cost. This is the content of the

Fixed Price Conjecture *Every countable group has the same cost in each of its measurable essentially free actions on probability spaces.*

It is known [18] (see also [34]) that the collection of groups with fixed price, includes free groups, amenable groups, groups with infinite centre and is closed under free products. In view of Theorem 53 the validity of the Fixed Price Conjecture will imply Conjecture 51.

Department of Mathematics,
Imperial College London,
SW7 2AZ, UK.
n.nikolov@imperial.ac.uk

References

[1] M. Abert, On the probability of satisfying a word in a group, *J. Group Theory. Vol. 9 (5), pp. 685-694.*

[2] M. Abert, A. Jaikin-Zapirain, N. Nikolov, Rank gradient from combinatorial viewpoint *Groups, Geometry and Dynamics 2011, Vol. 5, 213-230.*

[3] M. Abert, N. Nikolov, Rank gradient, cost of groups and rank vs Heegaard genus problem, *J. Europ. Math. Soc. to appear.*

[4] M. Aka, Arithmetic groups with isomorphic finite quotients, *preprint* http://arxiv.org/abs/1107.4147

[5] M. Anderson, Subgroups of finite index in profinite groups. *Pacific J. Math. 62 (1976), no. 1, 19-28.*

[6] L. Babai, N. Nikolov, L. Pyber, Product Growth and Mixing in Finite Groups, *19th ACM-SIAM Symposium on Discrete Algorithms, SIAM, 2008, pp. 248-257.*

[7] L. Babai, A. Seress, On the diameter of permutation groups, *European J. Comb. 13(1992), 231-243.*

[8] Y. Barnea, M. Ershov, T. Weigel, Abstract commensurators of profinite groups,*Trans. Amer. Math. Soc. 363 (2011), no. 10, 5381–5417.*

[9] G. Baumslag, Groups with the same lower central sequence as a relatively free group I, the groups, *Trans. Amer. Math. Soc. 129 (1967), 308-321.*

[10] J. Bourgain, A. Gamburd, P. Sarnak, Affine linear sieve, expanders, and sum-product. *Invent. Math. 179 (2010), no. 3, 559644.*

[11] E. Breuillard, B. Green, T. Tao, Approximate subgroups of linear groups, *preprint* http://arxiv.org/abs/1005.1881

[12] E. Breuillard, B. Green, T. Tao, Suzuki groups as expanders, http://arxiv.org/abs/1005.0782

[13] M. Bridson, F. Grunewald, Grothendieck's problems concerning profinite completions and representations of groups. *Ann. of Math. (2) 160 (2004), no. 1, 359–373.*

[14] P.E. Caprace, N. Monod, Decomposing locally compact groups into simple pieces, *preprint* http://arxiv.org/abs/0811.4101

[15] O. Dinai, Expansion properties of finite simple groups, *preprint,* arXiv:1001.5069.

[16] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, D. Segal, *Analytic pro-p groups,* Cambridge University Press, 2003.

[17] G. Fernandez-Alcober, I. Kazachkov, V. Remeslennikov, P. Symonds, Comparison of the discrete and continuous cohomology groups of a pro-p group. *preprint* http://arxiv.org/abs/math/0701737

[18] D. Gaboriau, Coût des relations d'équivalence et des groupes. (French) [Cost of equivalence relations and of groups] *Invent. Math. 139 (2000), no. 1, 41–98.*

[19] S. Garion, A. Shalev, Commutator maps, measure preservation, and T -systems, *Trans. Amer. Math. Soc. 361 (2009), no. 9, 4631-4651.*

[20] N. Gill, I. Short, L. Pyber, E. Szab, On the product decomposition conjecture for finite simple groups, *preprint* arXiv: 1111.3497.

[21] B. J. Green, Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak, *preprint,* arXiv:0911.3354.

[22] F. Grunewald, P. Pickel, D. Segal, Polycyclic groups with isomorphic finite quotients, *Annals of Math. 111, 155-195.*

[23] F. Grunewald, P. Zaleskii, Genus for groups, *J. Algebra, 326 (2011), 130-168.*

[24] R. M. Guralnick, W. M. Kantor, M. Kassabov, A. Lubotzky Presentations of finite simple groups: profinite and cohomological approaches, *Groups Geom. Dynamics, Vol. 1, Issue 4, 2007, pp. 469 - 523.*

[25] R. M. Guralnick, W. M. Kantor, M. Kassabov, A. Lubotzky, Presentations of finite simple groups: a computational approach, *preprint* http://arxiv.org/abs/0804.1396

[26] B. Hartley, Subgroups of finite index in profinite groups. *Math. Z. 168 (1979), no. 1, 71-76.*

[27] H. A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, *Annals of Math. 167 (2008), no. 2, pp. 601-623.*

[28] H. A. Helfgott, Growth in $SL_3(\mathbb{Z}/p\mathbb{Z})$, *J. European Math. Soc. to appear.*

[29] K. Hofmann, S. Morris, *The structure of compact groups,* de Gruyter Studies in Mathematics Vol. 25, 1998.

[30] D. Holt, Enumerating perfect groups, *J. London Math. Soc.* (2) **39** (1989), 67-78.

[31] A. Jaikin-Zapirain, On the verbal width of finitely generated pro-p groups, *Revista Math. Iberoamericana 24 (2008), 617-630.*

[32] M. Kassabov, A. Lubotzky, N. Nikolov, Finite simple groups as expanders, *Proc. Natl. Acad. Sci. USA, 2006, Vol. 103, 6116-6119.*

[33] M. Kassabov, N. Nikolov, Cartesian products as profinite completions, *Int. Math. Research Notices, 2006, ISSN: 1073-7928*

[34] A. Kechris, B. Miller, *Topics in orbit equivalence*, Lecture Notes in Mathematics, 1852. Springer-Verlag, Berlin, 2004.

[35] J. Kiehlmann, PhD thesis, Imperial College London 2012.

[36] B. Klopsch, N. Nikolov, C. Voll, *Lectures on profinite topics in group theory,* LMS student texts 77, Cambridge University Press, 2011.

[37] J. Königsmann, On the 'section conjecture' in anabelian geometry. *J. Reine Angew. Math. 588 (2005), 221-235.*

[38] M. Lackenby, Heegaard splittings, the virtually Haken conjecture and property τ, *Invent. Math. 164 (2006), no. 2, 317–359.*

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

[40] M. Lackenby, Detecting large groups, *J. Algebra 324 (2010), 2636-2657.*

[41] M. Larsen, A. Shalev, and P.H. Tiep: Waring problem for finite simple groups, *to appear in Annals of Math.*

[42] M. Larsen, A. Shalev, Fibers of word maps and applications *preprint.*

[43] M. Lazard. Groupes analytiques p-adiques, *Publ. Math. IHES 26 (1965), 389-603.*

[44] C. R. Leedham-Green, S. McKay, *The structure of groups of prime power order*, London Mathematical Society Monographs. New Series, 27. Oxford University Press, Oxford, 2002.

[45] M. W. Liebeck, N. Nikolov, A. Shalev, Product decompositions in finite simple groups, *preprint* http://arxiv.org/abs/1107.1528

[46] M. W. Liebeck, A. Shalev, Diameters of simple groups: sharp bounds and applications, *Annals of Math. 154 (2001), 383-406.*

[47] M.W. Liebeck, E.A. O'Brien, A. Shalev, and P.H. Tiep: The Ore conjecture, *J. Europ. Math. Soc. 12 (2010), 939-1008.*

[48] M. Levy, On the probability of satisfying a word in nilpotent groups of class 2, *preprint* http://arxiv.org/abs/1101.4286

[49] Tao Li, Rank and genus of 3-manifolds, *preprint* http://arxiv.org/abs/1106.6302

[50] D.D. Long, A. Reid, Grothendieck's problem for 3-manifold groups, *Groups, Geometry and Dynamics, Vol. 5 (2011), 479-499.*

[51] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math. 119 (1995), 267-295.*

[52] A. Lubotzky, D. Segal, *Subgroup growth*, Birkhauser, Basel, 2003.

[53] C. Martinez and E. Zelmanov, Products of powers in finite simple groups, *Israel J. Math. 96 (1996), 469-479.*

[54] A. Myasnikov, A. Nikolaev, Verbal subgroups of hyperbolic groups have infinite width, *preprint* http://arxiv.org/abs/1107.3719

[55] N. Nikolov, D. Segal, Generators and commutators in finite groups; abstract quotients of compact groups, *preprint* http://arxiv.org/abs/1102.3037

[56] N. Nikolov, D. Segal, On finitely generated profinite groups, I: strong completeness and uniform bounds, *Annals of Math., Vol. 165 (2006), 171-238.*

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

[58] N. Nikolov, D. Segal, A characterization of finite soluble groups, *Bull. London Math. Soc., 2007, Vol. 39, 209-213.*

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

[60] O. Parzanchevski, D. Puder, Measure preserving words are primitive, *in preparation.*

[61] D. Puder, On primitive words II: measure preservation, *preprint* http://arxiv.org/abs/1104.3991

[62] L. Pyber, Groups of intermediate subgroup growth and a problem of Grothendieck. *Duke Math. J. 121 (2004), no. 1, 169-188.*

[63] L. Pyber, E. Szabo, Growth in finite simple groups of Lie type of bounded rank *preprint* http://arxiv.org/abs/1005.1858

[64] A. Reid, A non-Haken hyperbolic 3-manifold covered by a surface bundle, *Pacific J. Math. 167, No. 1, (1995), 163-182.*

[65] A. Rhemtulla, A problem of bounded expressibility in free products, *Proc. Cambridge Philos. Soc. 64 (1968), 573-584.)*

[66] A. Rhemtulla, Commutators in certain finitely generated soluble groups, *Canad. J. Math. 21 (1969), 1160-1164.*

[67] L. Ribes, P. Zalesskii, *Profinite groups*, Springer, 2000.

[68] D. J. S. Robinson, *Finiteness conditions and generalized soluble groups, Part 1*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 62. Springer-Verlag, 1972.

[69] V. Romankov, Width of verbal subgroups in soluble groups, *Algebra and Logic 21 (1982), 41-49.*

[70] J. Saxl and J. S. Wilson, A note on powers in simple groups. *Math. Proc. Camb. Phil. Soc. 122 (1997), 91-94.*

[71] D. Segal, Closed subgroups of profinite groups. *Proc. London Math. Soc. (3) 81 (2000), no. 1, 29-54.*

[72] D. Segal, *Polycyclic groups*, 2-nd ed. Cambridge University press, 2005.

[73] D. Segal, Some aspects of profinite group theory. *Essays in geometric group theory, Ramanujan Math. Soc. Lect. Notes Ser., 9, Ramanujan Math. Soc., Mysore, 2009, 27-60.*

[74] D. Segal, The finite images of finitely generated groups. *Proc. London Math. Soc. (3), 82(3) (2001), 597-613.*

[75] D. Segal, *Words: Notes on verbal width in groups*, LMS lecture notes series 361 (2009).

[76] D. Segal, On verbal width of adelic groups, *J. Algebra Vol. 326, 1, pp. 227-237.*

[77] J. P. Serre, *Galois Cohomology*, New Ed. Springer, 2002.

[78] M. G. Smith, J. S. Wilson, On subgroups of finite index in compact Hausdorff groups. *Arch. Math. (Basel) 80 (2003), no. 2, 123-129.*

[79] P. Stroud, *Topics in the theory of verbal subgroups*, PhD thesis, University of Cambridge, 1966,

[80] B. Sury, Central extensions of p-adic groups: a theorem of Tate, *Comm. Algebra 21 (1993) 1203-1213.*

[81] D. van Dantzig, Ueber topologisch homogene Kontunua, *Fund. Math. 15 (1930), 102-125.*

[82] G. Willis, Compact open subgroups in simple totally disconnected groups, *J. Algebra 312 (2007), 405-417.*

[83] J. Wilson, *Profinite groups*, Oxford University Press, 1999.

[84] D. T. Wise, A residually finite version of Rips's construction, *Bull. London Math. Soc. 35 (2003), no. 1, 23-29.*

[85] E. I. Zel'manov, 'Solution of the restricted Burnside problem for groups of odd exponent', *Izv. Akad. Nauk. USSR* **54**(1990), 42-59*; 'Solution of the restricted Burnside problem for 2-groups', *Mat. Sb.* **182** (1991), 568–592 *(Russian); Math. USSR-Sb.* **72** (1992), 543–565 *(English).*