Problems that stumped me

Dan Segal

October 9, 2007

Everyone knows about the great problems of mathematics. So instead of trying to emulate Hilbert, I want to discuss here a few quite humble questions that I've come across over the years; ones that I wasn't smart enough to answer myself, but which look reasonably approachable.

1 The genus of polycyclic groups

Let's say that two groups G and H lie in the same *genus* if their profinite completions $\widehat{G}$ and $\widehat{H}$ are isomorphic (topologically); this is equivalent to saying that $\mathcal{F}(G) = \mathcal{F}(H)$ where $\mathcal{F}(G)$ denotes the set of finite images of G. The main result of [GPS] states that *each genus of virtually polycyclic groups consists of finitely many isomorphism classes.* The proof is in two stages:

(a) reduction to stage (b)

(b) a sort of 'relative' version: *if* Γ *is an arithmetic group, then each congruential conjugacy class of virtually soluble subgroups of* Γ *consists of finitely many conjugacy classes of subgroups.*

Here, subgroups of $\Gamma = \mathfrak{G}(\mathbb{Z})$ are called *congruentially conjugate* if their images in $\mathfrak{G}(\mathbb{Z}/m\mathbb{Z})$ are conjugate for each $m \in \mathbb{N}$ (where $\mathfrak{G}$ is a linear algebraic group defined over $\mathbb{Q}$). The result (b) is proved in [GS] using respectable mainstream mathematics (finiteness properties of arithmetic groups, due to Borel and Serre). **Problem 1** is to find a natural and attractive way to do (a); the existing proof is messy and technical, involving several non-canonical reduction steps. A more suggestive way to state the result is as follows:

Let P *be a profinite group and* $\mathcal{X}$ *the family of all dense virtually polycyclic subgroups* G *of* P *that have the congruence subgroup property* (i.e. the natural mapping from $\widehat{G}$ to P is an isomorphism). *Then* $\mathrm{Aut}(P)$ *has finitely many orbits on* $\mathcal{X}$.

In this formulation the result sounds not too different from (b). The recent paper of Baues and Grunewald [BG] demonstrates intimate connections between automorphism groups of polycyclic groups and algebraic groups over $\mathbb{Q}$; this may point the way to a sufficiently good description of $\mathrm{Aut}(P)$ and of its action on $\mathcal{X}$. (Actually, it can be shown that if P is the profinite completion of a virtually

polycyclic group then every finitely generated group having profinite completion P is already virtually polycyclic; but this is a bit of a red herring here.)

An outline of the (original) proof is given in Chapters 9 and 10 of [PG].

References

[GPS] F. J. Grunewald and P.F. Pickel and D. Segal: Polycyclic groups with isomorphic finite quotients. *Annals of Math.* **111** (1980), 155-195.

[GS] F. J. Grunewald and D. Segal: Conjugacy of subgroups in arithmetic groups. *Proc. London Math. Soc.* (3) **44** (1982), 47-70.

[BG] O. Baues and F. Grunewald: Automorphism groups of polycyclic-by-finite groups and arithmetic groups. *IHES Publ. Math.* **104** (2006), 213-368.

[PG] D. Segal: *Polycyclic groups,* CUP, Cambridge, 1983 (*Excellent value paperback reprint:* 2005).

2 Generators of virtually polycyclic groups

The minimal size of a generating set for a group G is denoted $\mathrm{d}(G)$.

Problem 2a. *Give an algorithm to determine* $\mathrm{d}(G)$ *for virtually polycyclic groups* G, or: *prove that the problem is undecidable.*

It is amazing, to me, that this is (apparently) not known, *even for the special case of finitely generated abelian-by-finite groups.* All of the 'traditional' decision problems have a positive solution in virtually polycyclic groups ([DP]). In the case of the word problem and the conjugacy problem this follows from suitable 'local-global' theorems (residual finiteness and conjugacy separability); regarding the number of generators, there is an 'almost' local-global theorem due to Linnell and Warhurst:

Theorem [LW] *If* G *is virtually polycyclic then* $\mathrm{d}(\widehat{G}) \leq \mathrm{d}(G) \leq 1 + \mathrm{d}(\widehat{G})$.

Here $\mathrm{d}(\widehat{G})$ denotes the number of *topological* generators of $\widehat{G}$, namely the supremum of $\mathrm{d}(Q)$ over all finite quotients Q of G. This provides an algorithm which determines $\mathrm{d}(G)$ up to a possible error of 1. It goes as follows. Enumerate (a) finite generating sets X for G and (b) minimal-size generating sets Y for finite quotients of G; then

$$|Y| \leq \mathrm{d}(\widehat{G}) \leq \mathrm{d}(G) \leq |X|$$

for each such X and Y, and eventually we will find a pair X, Y such that $|X| - |Y| \leq 1$. If in fact $|X| = |Y| = n$ we may conclude that $\mathrm{d}(G) = \mathrm{d}(\widehat{G}) = n$; but if $|X| = n = 1 + |Y|$ we can only infer that $n \leq \mathrm{d}(\widehat{G}) \leq \mathrm{d}(G) \leq n + 1$.

The indeterminacy could be removed by solving

Problem 2b. *Characterize those virtually polycyclic groups G such that* $\mathrm{d}(G) = \mathrm{d}(\widehat{G})$.

This seems to be a very delicate matter. A basic example is

$$G = A \rtimes \langle \zeta \rangle$$

where ζ is a root of unity and A is a non-zero ideal of $\mathbb{Z}[\zeta]$. Here $\mathrm{d}(\widehat{G}) = 2$, while $\mathrm{d}(G) = 2$ if A is principal, $\mathrm{d}(G) = 3$ if not. Of course, this is decidable by algebraic number theory in this case, but polycyclic groups are usually much more complicated!

References

[LW] P. A. Linnell and D. Warhurst: Bounding the number of generators of a polycyclic group. *Arch. der Math.* **37** (1981), 7-17.

[DP] D. Segal: Decidable properties of polycyclic groups. *Proc. London Math. Soc.* (3) **61** (1990), 497-528.

3 Upper rank

I will use "rank" in the sense of Prüfer rank, that is

$$\mathrm{rk}(G) = \sup \{ \mathrm{d}(H) \mid H \leq G, \quad \mathrm{d}(H) < \infty \}.$$

The *upper rank* of a group G is

$$\begin{aligned} \mathrm{ur}(G) &= \sup \{ \mathrm{rk}(Q) \mid Q \in \mathcal{F}(G) \} \\ &= \mathrm{rk}(\widehat{G}). \end{aligned}$$

I am interested in finitely generated residually finite (fgR$\mathfrak{F}$) groups. Avinoam Mann and I (and independently John Wilson) established the following

Theorem [MS] *Let G be a* fgR$\mathfrak{F}$ *group. Then G has finite upper rank if and only G is virtually soluble of finite rank (hence a virtually soluble minimax group).*

(See [SG], Section 5.5). Not long after, we showed with Alex Lubotzky that the same class of groups is characterized by the condition of *polynomial subgroup growth* (*loc. cit.,* Chapter 5), and Alex asked me if one could weaken this hypothesis: *is there a function f which grows (a little) faster than polynomially and such that every* fgR$\mathfrak{F}$ *group with subgroup growth at most f is virtually soluble minimax?* In other words, is there a "subgroup growth gap"? The answer turned out to be "no"; see [SG], Chapter 13. However, there is such a gap for groups in certain classes, such as linear groups, and more generally for groups that are virtually residually nilpotent (see [SG], Chapter 8). The following is still open:

Problem 3a. *Is there a subgroup growth gap for finitely generated soluble groups?*

Now, what our original proof did establish was the following

Proposition. *Let G be a finitely generated soluble group. If*

$$\log s_n(G) = o\left(\frac{\log n}{\log\log n}\right)^2 \qquad (*)$$

then G has finite upper p-rank for every prime p.

Here $s_n(G)$ denotes the number of subgroups of index at most n in G, and the *upper p-rank of G* is defined by

$$\mathrm{ur}_p(G) = \sup\left\{\mathrm{r}_p(Q) \mid Q \in \mathcal{F}(G)\right\},$$

where $\mathrm{r}_p(Q)$ for a finite group Q denotes the rank of a Sylow p-subgroup of Q. (Thus $\mathrm{ur}_p(G)$ is the rank of a Sylow pro-p subgroup of $\widehat{G}$). A theorem of Guralnick and Lucchini (first proved for soluble groups by Kovács) implies that for every finite group Q,

$$\mathrm{rk}(Q) \leq 1 + \sup_p \mathrm{r}_p(Q);$$

it follows that for any group G we have

$$\mathrm{ur}(G) \leq 1 + \sup_p \mathrm{ur}_p(G).$$

Hence G has finite upper rank if and only if the numbers $\mathrm{ur}_p(G)$ are *bounded* as p ranges over all primes. Thus a positive answer to Problem 3a would follow if one were to prove

Conjecture 3b. *Let G be a finitely generated soluble group. If the numbers $\mathrm{ur}_p(G)$ are finite for every prime p then they are bounded (hence $\mathrm{ur}(G)$ is finite, and modulo its finite residual G is a minimax group).*

It is worth remarking that any group G with $\mathrm{ur}_2(G)$ finite has $\widehat{G}$ virtually prosoluble (this is due to Lubotzky and Mann; see [SG], Section 5.5). So removing solubility from the hypothesis of the conjecture is not a very big step. Still, the conjecture is not inconsistent with a positive solution to the following slightly more general problem:

Problem 3c. *Does there exist a finitely generated group G of infinite upper rank such that the numbers $\mathrm{ur}_p(G)$ are finite for every prime p?*

In any case, to prove the conjecture it would suffice to assume that the group G is abelian-by-minimax (arguing by induction on the derived length). Such groups are in particular abelian-by-nilpotent-by-polycyclic. Recently, in joint work with Laci Pyber [PS], I have been able to establish the conjecture for the special case of groups that are nilpotent-by-abelian-by-polycyclic (so for finitely generated groups in this class there is indeed a subgroup growth gap, between polynomial and the type indicated in (*).

For more discussion of these problems, see [UR] and [FI].

References

[L] A Lucchini: A bound on the number of generators of a finite group. *Arch. der Math.* **53** (1989), 313-317.

[MS] A. Mann and D. Segal: Uniform finiteness conditions in residually finite groups. *Proc. London Math. Soc.* (3) **61** (1990), 529-545.

[UR] D. Segal: On modules of finite upper rank. *Trans. Amer. Math. Soc.* **353** (2000), 391-410.

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

[FI] D. Segal: On the finite images of infinite groups. In '*Groups: Topological, Combinatorial and Arithmetic Aspects*', ed. T. W. Müller, LMS Lect. Notes Ser. **311**, CUP, Cambridge, 2004.

[PS] L. Pyber and D. Segal: Finitely generated groups with polynomial index growth. *J. reine angew. Math.* **612** (2007), 173-211.

4 Verbal width, I

Let us say that a group word w has *width* m in a group G if every element of the verbal subgroup $w(G)$ is equal to a product of m values of w or their inverses. The following observation was made by Brian Hartley in 1979:

Proposition. *The following are equivalent for a profinite group G and a word w:*
(a) *the (algebraically defined) verbal subgroup $w(G)$ is closed in G;*
(b) *w has finite width in G;*
(c) *there is a uniform finite bound for the width of w in every finite (continuous) quotient of G.*

Using the (easy) implication (c) $\Longrightarrow$ (a), Serre had shown in the 1970s that in any finitely generated pro-p group, every subgroup of finite index is open: he deduced it from the fact that the commutator word $[x, y]$ has width d in every d-generator nilpotent group. In an attempt to generalize Serre's result, Nikolay Nikolov and I proved

Theorem. [NS] *For each $d \in \mathbb{N}$ there exists $g_1(d) \in \mathbb{N}$ such that $[x, y]$ has width $g_1(d)$ in every d-generator finite group. Similarly for each $c > 1$ there exists $g_c(d)$ such that the word $[x_1, x_2, \ldots, x_{c+1}]$ has width $g_c(d)$ in every d-generator finite group.*

(Actually our proof, rather surprisingly, gives an explicit bound of the form $g_1(d) = 12d^3 + O(d^2)$.) It follows that the derived group, and the other terms of the lower central series, are closed in every finitely generated profinite group. Interesting though this is, it doesn't help much towards generalizing Serre's

result beyond prosoluble groups. To this end, we had to consider other kinds of words:

Theorem. [NS] *Let $d \in \mathbb{N}$ and let w be a d-locally finite word. Then there exists $f = f(w, d)$ such that w has width f in every d-generator finite group.*

(The word w is *d-locally finite* if every d-generator group G satisfying $w(G) = 1$ is finite.) From this, it is not hard to deduce that the finite-index subgroups are open in every finitely generated profinite group.

This is a satisfactory conclusion to one story, but a successful blockbuster should leave the audience wanting a sequel. The glaring question is: what is it that the lower-central (iterated commutator) words and the locally finite words have in common? Let us say that the word w is *uniformly elliptic in finite groups* if there is a function $f : \mathbb{N} \to \mathbb{N}$ such that w has width $f(d)$ in in every d-generator finite group. This is equivalent to saying that $w(G)$ is closed in every finitely generated profinite group G.

Problem 4a. *Characterize the group words that are uniformly elliptic in finite groups.*

What we have shown is that all lower central words and all locally finite words are uniformly elliptic; in 1982 V. A. Roman'kov [R] showed that the second commutator word $[[x, y], [z, t]]$ is *not*, even in the restricted class of finite p-groups. Recently, Andrei Jaikin has established the definitive answer for this subclass of finite groups:

Theorem. [J] *Let p be a prime. A non-trivial word w is uniformly elliptic in finite p-groups* (equivalently, $w(G)$ is closed in G for every finitely generated pro-p group G) *if and only if $w \notin F''(F')^p$ where F is the free group on the variables of w.*

(Here F' denotes the derived group and F'' the second derived group of F.) In a sense, this 'explains' the distinction between the various kinds of word mentioned in the preceding paragraph. I am tempted to make the

Conjecture 4b. *A non-trivial word w is uniformly elliptic in finite groups if and only if $w \notin F''(F')^p$ for every prime p.*

Perhaps I should resist the temptation, however. I can show that this is true for words w that satisfy a rather special extra hypothesis: $F_\infty/w(F_\infty)$ is residually virtually-soluble (here F_∞ is the free group on $\aleph_0$ generators); and for arbitrary words if we restrict to finite groups that are nilpotent (this was already proved in [J]) or soluble of bounded derived length. But there is a hard 'test case' that has stubbornly resisted all our efforts: namely the 'Burnside words' $w = x^q$ (where q is a large-ish positive integer). So let me single out

Problem 4c. Prove or disprove: *if G is a finitely generated profinite group then every 'power subgroup' G^q is closed in G.*

A special case was actually proved in [NS]: when the group G is *non-universal*, which means that $\mathrm{Alt}(k)$ is not an upper section of G for some k. So while

slightly doubtful about Conjecture 4b in general, I am fairly confident that it is correct when restricted to finite groups not involving $\mathrm{Alt}(k)$ for some fixed k (and in particular for finite soluble groups).

When Nikolay and I were working on Serre's problem we spent a long time trying to prove that the Burnside words are uniformly elliptic in all finite groups; in the end, we had to settle on locally finite words instead. Now there is a plausible metamathematical argument which seems to get round the problem; it goes like this. According to the positive solution of the Restricted Burnside Problem, every finitely generated residually finite group of exponent q is finite; hence the finitely generated *infinite* Burnside groups should be *invisible* within the universe of finite groups and profinite groups. In other words, in this universe the word x^q should behave just like a locally finite word. To understand why this won't wash, we have to isolate the particular feature of a locally finite word w that our proof relies on; here it is: *if w is d-locally finite and G is a finite d-generator group then $w(G)$ is generated by h w-values, where h depends only on d and w*. In particular, this holds for $w = x^q$ if the Burnside group $B(d, q)$ is finite, but I don't know if it does or not when $B(d, q)$ is infinite. If it does *not*, we have found a way to detect the infinitude of $B(d, q)$ within the universe of finite groups! On the other hand, if it *does*, then our original proof will yield a positive solution to Problem 4c. So let me formulate

Problem 4d. *Does there exists a function $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that in every finite d-generator group G the subgroup G^q is generated by $h(d, q)$ q*th *powers*?

References

[NS] N. Nikolov and D. Segal: On finitely generated profinite groups, I: strong completeness and uniform bounds; II: products in quasisimple groups. *Annals of Math.* **165** (2007), 171-238, 239-273.

[J] A. Jaikin-Zapirain: On the verbal width of finitely generated pro-p groups. *Revista Mat. Iberoamericana*, to appear.

[R] V. A. Roman'kov: Width of verbal subgroups in solvable groups, *Algebra and logic* **21** (1982), 41-49 (*English translation*).

5 Verbal width, II

In the paper [J] cited above Andrei Jaikin also proves

Theorem. *In a compact p-adic analytic group every word has finite width* (equivalently*, every verbal subgroup is closed*).

Andrei's beautiful proof is analytic, resting ultimately on an application of the inverse function theorem for p-adic analytic functions. In particular, it is non-effective: one cannot extract from it a bound for the width of a particular word. My student Nick Simons gives in his thesis a different, algebraic proof,

modelled on Roman'kov's proof that polycyclic groups are verbally elliptic [R]; but this also appears to be ineffective. Now Andrei's theorem applies in particular to pro-p groups of finite rank. If G is such a group, of rank r, say, then w has finite width in G if and only if w has *bounded* width in all the finite quotients of G; in other words, *w is uniformly elliptic in $\mathcal{F}(G)$*. The only obvious feature that all groups in $\mathcal{F}(G)$ have in common is that their ranks are at most r. The maxim "a qualitative result about profinite groups is equivalent to a quantitative result about a family of finite groups" leads one to suggest

Problem 5a. *Let w be a word and p a prime. Prove: for each $r \in \mathbb{N}$ there exists $k = k(w, p, r)$ such that w has width k in every finite p-group of rank r.*

This would be the 'finite' version of Jaikin's theorem. If the claim is not true, we are left with the following fundamental question:

Problem 5b. *Let $\mathcal{X}$ be a family of finite p-groups of bounded rank. What conditions on $\mathcal{X}$ are sufficient to imply that $\mathcal{X} \subseteq \mathcal{F}(G)$ for some pro-p group G of finite rank?*