The remarkable expressivity of first-order logic for profinite groups

André Nies

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

Joint with Dan Segal (Oxford) and Katrin Tent (Münster).

Algebra and Mathematical Logic
Conference in Honour of Marat Arslanov's Birthday
Kazan, 25 June 2019

Expressivity of first-order logic

A topological group is called profinite if it is

- compact and
- totally disconnected.

Equivalently, it is an inverse limit of finite groups with the discrete topology.

Question: How much can first-order logic express for such groups?

Caveat: The first-order language can directly only access the algebraic structure!

Answer: First-order logic can express an amazing lot of things for profinite groups. For instance, a lot of profinite groups can be determined by a single sentence within their class.

Main Definition

A profinite group G is called finitely axiomatisable (FA) if there is a first-order sentence ϕ in the language of groups such that for each profinite group H,

$$H \models \phi \iff H \cong G.$$

Here $\cong$ denotes topological isomorphism.

So the algebraic structure of such G determines the topological structure. Let p be a prime. $\mathbb{Z}_p$ denotes the ring of p-adic integers. The following unitriangular profinite group is FA:

$$\mathrm{UT}_3(\mathbb{Z}_p) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$$

The story started in 2003
with certain f.g. abstract groups:

the quasi-finitely axiomatizable groups

Definition (N., IJAC 2003)

An infinite f.g. group G is called quasi-finitely axiomatizable (QFA) if there is a first–order sentence ϕ such that for each f.g. group H,

$$H \models \phi \iff H \cong G.$$

- The "axiom" ϕ determines G among the f.g. groups.
- Abelian groups are not QFA, by the methods that showed quantifier elimination of the theory of abelian groups (Smielev, 1951).
- Being QFA has been studied for groups of many kinds: nilpotent (Oger and Sabbagh, 2006), metabelian (Khelif, 2007), particular types of permutation groups (Morozov and N., 2005), polycyclic (Lasserre, 2013), higher rank arithmetic groups (Avni, Meir, Lubotzky, 2019 and sequel paper).

Two examples of QFA groups

For groups G, A, R one writes $G = A \rtimes R$ (split extension) if

$$AR = G,\ A \triangleleft G, \text{ and } A \cap R = \{1\}.$$

We give examples of QFA groups that are split extensions $A \rtimes R$, where A is abelian, and $R = \langle d \rangle$ infinite cyclic. Let C_n denote the cyclic group of size n.

Theorem (N, 2005)

- For each $m \geq 2$, the following group is QFA:
$$H_m = \langle a, d \mid d^{-1}ad = a^m \rangle = \mathbb{Z}[\tfrac{1}{m}] \rtimes \mathbb{Z}.$$
- For each prime p, the restricted wreath product $C_p \wr \mathbb{Z}$ is QFA. (This group is not finitely presented.)

Structure of these groups

- H_m is a split extension of $A = \mathbb{Z}[1/m] = \{zm^{-i} : z \in \mathbb{Z}, i \in \mathbb{N}\}$ by $\langle d \rangle$, where the action of d is given by $u \mapsto um$.

- By its definition, $C_p \wr \mathbb{Z}$ is a split extension $A \rtimes C$, where
  - $A = \{f \mid \mathbb{Z} \to C_p \colon f \text{ has finite support}\}$
  - $C = \langle d \rangle$ with d of infinite order
  - d acts on A by "shifting": $(d^{-1}fd)(z) = f(z-1)$

QFA for nilpotent groups

Theorem (Oger and Sabbagh, 2006)

Let G be an infinite, f.g. nilpotent group.

$$G \text{ is QFA} \iff Z(G)/(Z(G) \cap G') \text{ is finite.}$$

- The condition says that the centre $Z(G)$ is almost contained in G'. It fails for infinite abelian G.
- The condition holds for $G = \mathrm{UT}_3(\mathbb{Z})$ because
$$Z(G) = G' = \begin{pmatrix} 1 & 0 & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
The first proof (N., 2003) that this group is QFA worked via an interpretation of arithmetic in $\mathrm{UT}_3(\mathbb{Z})$ due to Mal'cev.
- The implication $\Rightarrow$ holds for all f.g. groups, using ultrapowers.

A QFA criterion for polycyclic groups

Let $\Delta(G) = \{x : \exists m > 0\ x^m \in G'\}$.

Clement Lasserre has extended the Oger/Sabbagh criterion from f.g. nilpotent to a larger class. Recall that G is polycyclic if it has a subnormal series with cyclic quotients.

Theorem (Lasserre, 2013)

Let G be a polycyclic group. Then

G is QFA $\iff Z(H) \subseteq \Delta(H)$ for each subgroup H of finite index.

Complexity of the word problem for QFA groups

Theorem (Morozov and N., 2005)

Let $S \subseteq 3\mathbb{N}^+$ be an arithmetical singleton (e.g., the halting set). There is a QFA group G_S with WP of the same complexity as S.

- To say that S is an "arithmetical singleton" means that S can be described as a set within arithmetic.
- G_S is the subgroup of $\mathrm{Sym}(\mathbb{Z})$ generated by successor and the permutation p_S that has the cycles $(0, 1)$ and $(k, k+1, k+2)$ for each $k \in S$.

Complexity of the word problem for QFA groups

We also obtain an upper bound on the complexity of the word problem.

Theorem (Morozov and N., 2005)

If G is QFA then its word problem is hyperarithmetical.

The upper bound is sharp because each α-th jump $\emptyset^{(\alpha)}$, where α is a recursive ordinal, is an arithmetical singleton.

Finite groups

- For a finite group G, there is always a trivial first order description α_G.
- But α_G is unreasonably long.
- Is there a "short" first-order description?
- This question is usually interpreted asymptotically, in natural classes of finite groups.

Short descriptions for finite groups

Definition

Let $r \colon \mathbb{N}^+ \to \mathbb{R}$. A class $\mathcal{C}$ of finite groups is r-compressible if for any $G \in \mathcal{C}$, there exists a first-order sentence ψ_G in the language of groups such that $|\psi_G| = O(r(|G|))$, and for each group H,

$$H \models \psi_G \iff H \cong G.$$

Theorem (N. and Tent, Israel J. Math, 2017)

The class of finite simple groups is log-compressible.
The class of finite groups is $\log^3$-compressible.

Both results are near optimal for these classes.

Profinite groups

Definition, examples

A countably based compact (Hausdorff) topological group G is called profinite if one of the following equivalent conditions holds.

(a) G is totally disconnected (i.e., the closed and open sets form a basis of the topology.)

(b) G is the inverse limit of a system $\langle G_n \rangle_{n\in\mathbb{N}}$ of finite groups carrying the discrete topology, with surjective homomorphisms $p_n \colon G_{n+1} \to G_n$.

- The correspondence is not effective; the natural computable version of (b) is stronger than the one of (a) by Melnikov, TAMS, in press.
- Proof idea for (a)$\to$(b): open subgroups of a compact group have finite index, and $G = \varprojlim_{N \text{ open, normal}} G/N$.
- This inverse limit can be concretely defined as a closed subgroup of $\prod_N G/N$, consisting of those f such that $f(Ng) = Mg$ whenever $N \leq M$. Then make linear diagram.

Examples based on p-adic integers

- $(\mathbb{Z}_p, +)$ is the additive group of p-adic integers for a prime p. Addition works via carries but for infinite digit sequences. Say $p = 3$:

$$\begin{array}{cccccc} & \dots & 1 & 2 & 1 & 1 & 1 \\ + & \dots & 0 & 2 & 1 & 2 & 0 \\ \hline = & \dots & 2 & 2 & 0 & 0 & 1 \end{array}$$

- $\mathbb{Z}_p$ is in fact a ring: multiplication works like with the usual algorithm.
- This ring is profinite: $\mathbb{Z}_p = \varprojlim_n C_{p^n}$ as rings, with the maps $C_{p^{n+1}} \to C_{p^n}$ given by $x \mapsto x \mod p^n$.
- This implies that matrix groups such as $\mathrm{UT}_n(\mathbb{Z}_p)$ and $\mathrm{SL}_n(\mathbb{Z}_p)$, $n \geq 2$ are profinite:

$$\mathrm{SL}_n(\mathbb{Z}_p) = \varprojlim_n \mathrm{SL}_n(C_{p^n}).$$

Krull's Galois theory

An extension of fields K/k is Galois if it is algebraic, normal, and separable. Its Galois group $\mathrm{Gal}(K/k)$ consist of the automorphisms of K that fix k pointwise.

It has a natural topology that makes it profinite (Krull, 1928):

- Suppose we have $K = \bigcup_{i \in \mathbb{N}} L_i$, $L_i \leq L_{i+1}$ and the $|L_i/k|$ are normal finite extensions.
- A basis of neighbourhoods of the identity in $\mathrm{Gal}(K/k)$ is given by the open normal subgroups $\mathrm{Gal}(K/L_i)$.

Galois correspondence: to an intermediate field F corresponds a closed subgroup, the pointwise stabiliser of F. Every separable profinite group is realized as $\mathrm{Gal}(K/k)$ for a countable field k.

pro-$\mathcal{C}$-groups, pro-$\mathcal{C}$ completions

Let $\mathcal{C}$ be a class of finite groups with some nice properties (e.g. closed under isomorphism, taking quotients). A group is called pro-$\mathcal{C}$ if it is an inverse limit of a system of finite groups in $\mathcal{C}$.

The pro-$\mathcal{C}$-completion of a group G is the inverse limit

$$\widehat{G} = \varprojlim_{N} G/N,$$

where N ranges over the normal subgroups such that $G/N \in \mathcal{C}$.

- $\mathcal{C} =$ finite groups: profinite completion
- $\mathcal{C} =$ finite pro-p groups: pro-p completion.

If G is residually $\mathcal{C}$, then the natural map $G \to \widehat{G}$ is an embedding.

Finite axiomatizability

within classes of

profinite groups and rings

Main Definition, again

A profinite group G is called finitely axiomatisable (FA) if there is a first-order sentence ϕ in the language of groups such that for each profinite group H,

$$H \models \phi \iff H \cong G.$$

Here $\cong$ denotes topological isomorphism.

The definition can be adapted to other classes of profinite structures:

- profinite groups with constants,
- pro-$\mathcal{C}$ groups,
- profinite rings, etc.

The ring of p-adic integers is FA in profinite rings

Rings: commutative with 1. Sabbagh proved that $(\mathbb{Z}, +, \times)$ is QFA.

Proposition (with Scanlon, 2016; see Logic Blog 2017)

The ring $(\mathbb{Z}_p, +, \times)$ of p-adic integers is FA in the profinite rings.

The following argument of Segal is a bit simpler than Scanlon's. Let ϕ_p be the sentence of L_{ring} expressing for a ring R:

$$px = 0 \Longrightarrow x = 0$$

$$|R/pR| = p$$

$$x \in R \setminus pR \Longrightarrow xR = R.$$

Suppose that $R \models \phi_p$ where R is a profinite ring. Then $(R, +)$ is a pro-p group, since it is abelian and for each prime $q \neq p$ we have $qR = R$; the other conditions then imply that $(R, +)$ is also procyclic and torsion-free. It follows that $A \cong \mathbb{Z}_p$.

$\mathrm{UT}_3(\mathbb{Z}_p)$ is FA in the profinite groups

Recall the unitriangular group over $\mathbb{Z}_p$:

$$\mathrm{UT}_3(\mathbb{Z}_p) = \left\{ \begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} : \alpha, \beta, \gamma \in \mathbb{Z}_p \right\}.$$

This is the inverse limit of the finite groups $\mathrm{UT}_3(C_{p^n})$, so profinite. Its centre consists of the matrices of the form $\left(\begin{smallmatrix} 1 & 0 & \gamma \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$.

Theorem (N., Scanlon 2016; N., Segal and Tent, 2019)

$\mathrm{UT}_3(\mathbb{Z}_p)$ is finitely axiomatizable within the profinite groups.

In fact there is a formula $\phi(r, s)$ such that the structure $(\mathrm{UT}_3(\mathbb{Z}_p), a, b)$ is FA via ϕ, where a, b are the standard generators (defined below).

$(\mathrm{UT}_3(\mathbb{Z}_p), a, b)$ is FA within profinite structures

Proof. The standard generators are $a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

For any ring R, the Mal'cev formula $\mu(x, y, z; r, s)$ defines the ring operation $M_{r,s}$ on the centre $C(\mathrm{UT}(R)) \cong (R, +)$ when r, s are assigned to the standard generators a, b.

- A sentence α_1 expresses of a profinite group G that G is nilpotent of step 2, and that the centre $C = C(G)$ equals the set of commutators. In particular, $G_{\mathrm{ab}} = G/C$.
- A sentence α_2 expresses that pG/C has index p^2 in G/C.
- C is closed and the prof. ring $\mathbb{Z}_p$ is FA. So there is a formula $\gamma(r, s)$ expressing that $(C, +, M_{r,s})$ is isomorphic to $\mathbb{Z}_p$; in addition, γ expresses that $[r, s]$ is the neutral element 1 of this ring.

Let $\phi(r, s) \equiv \alpha_1 \wedge \alpha_2 \wedge \gamma(r, s)$. Using that $\mathrm{UT}_3(\mathbb{Z}_p)$ is free in its pro$-p$ variety, one shows ϕ is as required. See Logic Blog '17.

FA for pro-p nilpotent groups

Recall Oger/Sabbagh 2006: let G be an infinite, f.g. nilpotent group. Then G is QFA $\iff Z(G)/Z(G) \cap G'$ is periodic (the O/S condition).

- We show that there are uncountably many non-isomorphic nilpotent of step 2 pro$-p$ groups satisfying the O/S condition, so not all of them can be FA.
- We need to restrict to a countable class of groups that have a finite presentation. One special case is:

Theorem (N., Segal and Tent, 2019)

Let G be the pro-p completion of a f.g. nilpotent group.

G is FA in the profinite groups $\iff Z(G)/Z(G) \cap G'$ is periodic.

$\mathrm{UT}_3(\mathbb{Z}_p)$ is the pro$-p$ completion of $\mathrm{UT}_3(\mathbb{Z})$ and satisfies O/S condition, so we re-obtain the previous result in a purely algebraic

Some Chevalley groups over $\mathbb{Z}_p$

Theorem

Let p be an odd prime. Suppose p does not divide n.
The groups $\mathrm{SL}_n(\mathbb{Z}_p)$ and $\mathrm{PSL}_n(\mathbb{Z}_p)$ are FA within the profinite groups.

Examples: we can do $\mathrm{SL}_2(\mathbb{Z}_3)$, but not $\mathrm{SL}_6(\mathbb{Z}_3)$.

- The proof works by first considering the first congruence subgroup $G = \mathrm{SL}_n^1(\mathbb{Z}_p)$, the kernel of the natural map $\mathrm{SL}_n(\mathbb{Z}_p) \to \mathrm{SL}_n(C_p)$.
- In G we look at definable closed root subgroups (corresponding to Chevalley groups of type A_{n-1}).
- That way we reduce the problem to the finite axiomatizability of compact p-adic-analytic groups within the pro$-p$ groups.

Finite rank, and p-adic analytic groups

- The dimension of a profinite group is the minimal number of topological generators.
- The (Prüfer) rank of a profinite group is the supremum of the dimensions of all closed subgroups.

Lazard (1965) considered Lie groups over $\mathbb{Q}_p$, called p-adic analytic groups. He realized that they have an open pro-p subgroup H of finite rank.

His main theorem characterizes them as the groups with an open "uniformly powerful" pro-p subgroup, a particularly nice finite rank group. ('Uniformly powerful' is the subsequent terminology of Lubotzky and Segal.)

Finite rank pro-p groups and FA

Let L_p be the uncountable language extending L_{group} which has a symbol f_λ for each $\lambda \in \mathbb{Z}_p$, interpreted as exponentiation $x \to x^\lambda$ in a pro-p group. Here $x^\lambda = \lim_n x^{\lambda \restriction n}$.

Theorem (NST, 19)

(a) Each finite rank pro-p group G is finitely axiomatizable, with respect to L_p, within the pro-p groups. (I.e., we need finitely many exponentials to determine G.)

(b) If G is strictly finitely presented, then an axiom determining G can be chosen in the basic language L_{group}.

Here G is called strictly finitely presented if it is the pro-p completion of a f.p. group. For instance, $\mathbb{Z}_p$ is strictly finitely presented as the pro-p completion of $\mathbb{Z}$. So $\mathbb{Z}_p$ is FA within the pro-p groups. (This contrasts with the fact that $(\mathbb{Z}, +)$ is not QFA.)

Finitely generated pro−p groups of infinite rank

Examples:

- $F_{n,p}$=the pro-p completion of F_n, for $n \geq 2$
- $\widehat{C_p \wr \mathbb{Z}_p}$ the pro-p completion of $C_p \wr \mathbb{Z}$

An ad-hoc argument establishes an analog of the result that $C_p \wr \mathbb{Z}$ is QFA (N., 2003):

Theorem (NST 19, Prop 4.5)

$\widehat{C_p \wr \mathbb{Z}_p}$ is FA within the pro-p groups.

The abstract free groups F_n are not QFA. It is unknown at present whether $F_{n,p}$ is FA.

Separating classes of groups by their theories

The main object of study in N., 2003 was the first-order separation of isomorphism invariant classes of groups $\mathcal{C} \subset \mathcal{D}$. Can we distinguish them using first-order logic?

Definition. We say that $\mathcal{C}$ and $\mathcal{D}$ are first-order separable if some sentence holds in all groups in $\mathcal{C}$ but fails in some group in $\mathcal{D}$.

- This makes sense in particular when the classes are not axiomatizable (most aren't).
- One way to establish this is to find a witness: a group in $\mathcal{D} - \mathcal{C}$ that is FA within $\mathcal{D}$.

Witnesses for separations

We say that classes $\mathcal{C} \subset \mathcal{D}$ are first-order separable if some sentence holds in all groups of $\mathcal{C}$ but fails in some group in $\mathcal{D}$. Our results provide first-order separations of interesting classes of profinite groups.

Theorem

(a) The finite rank pro-p groups are f.o. separable from the (topologically) finitely generated pro-p groups.
(b) The f.g. profinite groups are f.o. separable from the class of all profinite groups. The same holds within the pro-p groups.

Proof. For (a), a witness (i.e., FA in the larger class, and not element of the smaller) is the above mentioned pro-p completion of $C_p \wr \mathbb{Z}$.
For (b) a witness is the affine group $\mathrm{Af}_1(R)$, where R is the profinite ring $F_p[[t]]$. This is the group of matrices over R of the form $\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$ where $b \in R^*$ (a unit). Equivalently, it is $R \rtimes R^*$.

Rings and groups that are not FA

Proposition (T. Scanlon, LB 2017)

Let S a set of primes and let R_S denote the profinite ring $\prod_{p \in S} \mathbb{Z}_p$. If S is infinite then R_S is not FA in the profinite rings.

The proof uses the Feferman-Vaught theorem from model theory, which determines the validity of sentences in a direct product from the validity of related sentences in the components.

Proposition

The group $\mathrm{UT}_3(R_S)$ is FA among profinite groups if and only if S is finite.

Questions

- Study complexity of FA profinite groups, analogous to the Morozov/N. results on QFA f.g. groups.
- Given a f.o. sentence ϕ, how complex is the class of concrete profinite groups satisfying it? (Trival upper bound: projective.)
- Extend the O/S criterion in order to characterise FA for the profinite analog of polycyclic groups: the solvable groups of finite rank. (Lasserre, 2013 has characterised QFA for polycyclic groups.)
- Which Chevalley groups over profinite rings are FA?

References:

- N., Describing Groups, BSL 2007
- N. and Tent, IJM 2017
- Logic Blog 2017, on arxiv
- N., Segal and Tent, Finite axiomatizability for profinite groups I: an algebraic approach, posted on arxiv shortly
- These slides on my web site