# 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).

CARMA seminar

Newcastle, Feb 2020

A topological group is called profinite if it is

- compact
- totally disconnected.

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

How much can first-order logic express about a profinite group?

Answer: A lot.

- Each topologically f.g. profinite group is given by its first-order theory within the class of profinite groups (Jarden/Lubotzky)
- Many a profinite group can be determined by a single sentence within its class.

# First–order language for groups

- The basic formulas are the equations
$$s(x_1, \dots, x_k) = t(x_1, \dots, x_k),$$
where $s$ and $t$ are group terms.
One builds more complex formulas using the symbols $\neg, \wedge, \vee, \to, \exists x, \forall x$, adhering to the usual syntactical rules.

- A (first-order) sentence is a formula which has only bound variables.

# First-order logic and groups

Let $[x, y]$ denote the commutator $x^{-1}y^{-1}xy$.

- The first-order sentence $\forall x \forall y \; [x, y] = 1$ expresses that the group is abelian.
- The following first-order sentence expressed that every commutator is a product of three squares:

$$\forall u \forall v \exists r \exists s \exists t \; [u, v] = rrsstt.$$

- We can express that a group is torsion free using infinitely many sentences.
- By the compactness theorem we can not express that a group is periodic. (We can't quantify over natural number exponents.)

# Main Definition

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

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

In this case, the algebraic structure of such $G$ determines the topological structure.

# Unitriangular groups

There are no “obvious” examples of FA profinite groups.

Let $p$ be a prime. $\mathbb{Z}_p$ denotes the ring of $p$-adic integers.
The following profinite group was the first to be shown FA (Scanlon and N., on Logic Blog 2017):

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

# Quasi-finitely axiomatizable groups

The idea to enhance the power of first order logic by also prescribing a reference class has been around for at least 20 years. I introduced this in the context of finitely generated discrete groups.

# Quasi-finitely axiomatizable groups

## Definition (N., Int. J. Algebra Computation 2003)

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

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

- The "axiom" $\phi$ determines $G$ among the f.g. groups.
- Being QFA has since 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 such as $\mathrm{SL}_3(\mathbb{Z})$ (Avni, Meir, Lubotzky, 2019 and its forthcoming sequel paper).

# Two examples of QFA groups

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

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

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:
$$H_m = \langle a, d \,|\, d^{-1}ad = a^m \rangle = \mathbb{Z}[\tfrac{1}{m}] \rtimes \mathbb{Z}.$$
- 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

  - $A = \{f \mid \mathbb{Z} \to C_p \colon f$ has finite support$\}$

  - $C = \langle d \rangle$ with $d$ of infinite order

  - $d$ acts on $A$ by "shifting": $(d^{-1} f d)(z) = f(z-1)$

# Proof that these groups are QFA

Each group has the form $G = A \rtimes C$. The group $A$ will be given as the set of elements satisfying a first-order formula.
One writes a conjunction $\psi(d)$ of first-order properties of an element $d$ in a group $G$ so that the sentence $\exists d\, \psi(d)$ implies that $G$ is QFA.

Let $C$ be the centralizer of $d$, namely $C = \{x : [x, d] = 1\}$. In the following, $u, v$ denote elements of $A$ and $x, y$ elements of $C$.

- The commutators form a subgroup (so $G'$ is definable)
- $A$ and $C$ are abelian, and $G = A \rtimes C$
- The conjugation action of $C - \{1\}$ on $A - \{1\}$ has no fixed points. That is, $c^{-1}ac \neq a$ for each $a \in A - \{1\}$, $c \in C - \{1\}$.
- $|C : C^2| = 2$

To specify $H_m = \mathbb{Z}[\frac{1}{m}] \rtimes \mathbb{Z}$ one uses the f.o. definition $A = \{g : \; g^{m-1} \in G'\}$, and requires in addition that

- $\forall u \, [d^{-1}ud = u^m]$;
- The map $u \mapsto u^q$ is 1-1, for a fixed prime $q$ not dividing $m$;
- $x^{-1}ux \neq u^{-1}$ for $u \neq 1$;
- $|A : A^q| = q$.

The information that $G$ is f.g. yields that $A$, when viewed as a torsion-free module over the principal entire ring $\mathbb{Z}[1/m]$, is finitely generated; hence $A$ is a free module. By the properties above, its rank is 1, and so we know its structure.

To specify $C_p \wr \mathbb{Z}$,

- one uses the f.o. definition $A = \{g : \; g^p = 1\}$,
- requires that $|A : G'| = p$ and
- no element in $C - \{1\}$ has order $< p$.

# 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 the derived subgroup $G'$. 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

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

**Theorem (Lasserre, 2013)**

Let $G$ be a polycyclic group. Then $G$ is QFA $\iff$

$Z(H)/(Z(H) \cap H')$ is finite for each subgroup $H$ of finite index.

# Finite groups

- For a finite group $G$, there is always a trivial first order description $\alpha_G$, obtained from the whole group operation table.
- But $\alpha_G$ is unreasonably long.
- Is there a "short" first-order description?
- While it would be interesting to design a very short f.o. description of the monster, this question is best interpreted asymptotically, in natural classes of finite groups.

# Short first-order descriptions of 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 $\psi_G$ 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. This is proved by counting the number of nonisomorphic groups of each size in the class. For the second case, one uses the Higman result that the number of groups of order $p^m$ is at least $p^{\frac{2}{27}m^2(m-6)}$.

# 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 algorithmic version of (b) is stronger than the one of (a) by Melnikov, TAMS, 2019.

Recall: 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 $p_n \colon G_{n+1} \to G_n$.

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 $N \leq M$. From this one can make a linear diagram.

# Examples based on the $p$-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.
- $\mathbb{Z}_p$ is in fact a ring: multiplication works with the usual algorithm extended to infinite sequences.
- 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 $G/N \in \mathcal{C}$.

- If $\mathcal{C} =$ finite groups, we have the profinite completion
- If $\mathcal{C} =$ finite pro-$p$ groups, we have the 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

An infinite, profinite group $G$ is called finitely axiomatisable (FA) within the profinite groups if there is a first-order sentence $\phi$ in the language of groups such that for each profinite group $H$,

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

Here $\cong$ denotes topological isomorphism.

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

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

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

Rings are commutative with 1.
Sabbagh (2005) proved that $(\mathbb{Z}, +, \times)$ is QFA as a ring.

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

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

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

The following argument of Segal is a bit simpler than Scanlon's.

Let $\phi_p$ 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 $R \cong \mathbb{Z}_p$ as topological rings.

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

Recall the following 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 $\begin{pmatrix} 1 & 0 & \gamma \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

**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 $\phi$, 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 $\alpha_1$ expresses of a profinite group $G$ that $G$ is nilpotent of class 2, and that the centre $C = C(G)$ equals the set of commutators.
- A sentence $\alpha_2$ expresses that $pG/C$ has index $p^2$ in $G/C$.
- $C$ is closed and the profinite 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, $\gamma$ 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 $\phi$ is as required. See Logic Blog '17.

# FA for pro-$p$ nilpotent groups

Result of Oger/Sabbagh 2006: let $G$ be an infinite, f.g. nilpotent group. Then

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

Note we can replace finite by periodic as the two things are equivalent for f.g. nilpotent groups.

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

One special case of our result 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 the O/S condition, so we re-obtain the previous result in an algebraic way.

# Rings and groups that are not FA

**Proposition (T. Scanlon, see Logic Blog 2017)**

Let $S$ be 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.

## Theorem (Chevalley groups over $\mathbb{Z}_p$ that are FA)

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.

- The proof works by considering the first congruence subgroup $G = \mathrm{SL}_n^1(\mathbb{Z}_p)$, that is, 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 $U, V$. They are nilpotent and pro-$p$, and hence can be described among all profinite groups.
- Using this provide sentences that ensure a profinite group sufficiently similar to $G$ is pro-$p$.
- In this 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. (This is the subsequent terminology of Lubotzky and Segal.)

# Finite rank pro-$p$ groups and FA

Exponentiation $x \to x^\lambda$ in a pro-$p$ group is given by $x^\lambda = \lim_n x^{\lambda \upharpoonright n}$. Let $L_p$ be the uncountable language extending $L_{group}$ which has a symbol $f_\lambda$ for each $\lambda \in \mathbb{Z}_p$, interpreted as $x \to x^\lambda$.

## Theorem (NST, 19)

(a) Each finite rank pro-$p$ group $G$ is finitely axiomatizable using the language $L_p$, within the pro-$p$ groups. (I.e., we need finitely many exponentials in the language 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:

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

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

### Theorem (NST 19, Prop 4.5)

$\widehat{C_p \wr \mathbb{Z}_p}$ is FA within the profinite 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 the "QFA paper" [N., 2003] was in fact the first-order separation of isomorphism invariant classes of groups $\mathcal{C} \subset \mathcal{D}$. Can one distinguish such classes 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 is interesting when the classes are not axiomatizable.
- One way to separate the classes is to find an FA witness: a group in $\mathcal{D} - \mathcal{C}$ that is FA within $\mathcal{D}$.

# First-order separations

**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. (a) a witness (i.e., FA in the larger class, and not element of the smaller) is the above mentioned pro-$p$ completion of $C_p \wr \mathbb{Z}$.

(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 $R \rtimes R^*$ with $R^*$ acting on $(R, +)$ by multiplication.

# Some open questions

- Extend the O/S criterion in order to characterise being FA for the profinite analog of polycyclic groups: the solvable groups of finite rank.
- FA for profinite free groups of finite dimension.
- Which t.d.l.c. groups are FA in their class?
  $UT_3(\mathbb{Q}_p)$, $p \neq 2$, is a first example. How about $\mathrm{Aut}(T_d)$?
- Which $p$-adic analytic groups are FA in this class?

**References:**


- N. Separating classes of groups by first order sentences. Intern. J. of Algebra and Computation 13, No 3 (2003), 287-302.
- N., Describing Groups, Bull. Symb. Logic. 13 no 3 (2007), 305-339.
- N. and Tent. Describing finite groups by short first-order sentences. Israel J. Mathematics 221 (2017), 85-115.
- N. and Scanlon, Describing a profinite structure by a single first-order sentence, Section 10 of Logic Blog 2017, arxiv.org/abs/1804.05331
- N., Segal and Tent, Finite axiomatizability for profinite groups I: group theory, arxiv.org/abs/1907.02262