Describing a group by a first-order sentence

André Nies

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

New Methods in Group Actions on Manifolds

KIAS, Seoul, Aug 2024

First–order language for a functional signature

A functional "signature" $\mathcal{S}$ consists of finitely many function symbols and constants.

To build the first-order language for $\mathcal{S}$,

- start with equations

$$s(x_1, \ldots, x_k) = t(x_1, \ldots, x_k),$$

  where the x_i are variables, and s and t are terms containing these variables and the symbols in the signature;
- build formulas from equations using $\neg, \wedge, \vee, \rightarrow, \exists x, \forall x$.

A (first-order) sentence ϕ is a formula in which all the variables are bound. $M \models \phi$, for an $\mathcal{S}$-structure M, denotes that ϕ holds in M. (This doesn't depend on any objects external to M.)

Examples of first-order sentences for groups

- Let ϕ be the sentence $\forall x \forall y \; [x, y] = e$. For a group G, $G \models \phi$ expresses that G is abelian.
- The following sentence expresses that every commutator is a product of three squares:

$$\forall u \forall v \exists r \exists s \exists t \; [u, v] = r^2 s^2 t^2$$

Strictly speaking, the signature for groups has a constant e, unary function symbol f, and a binary function symbol g.

$[x, y]$ denotes the term $ggfxfygxy$, and the expression above is shorthand for $\forall u \forall v \exists r \exists s \exists t \; ggfxfygxy = gggrrgssgtt$.

$\mathtt{Th}(G)$ is the set of all sentences that hold in G.
Does it know whether G is torsion free? periodic? finitely generated?

First-order definability

Given an $\mathcal{S}$-structure M, one says that a relation $R \subseteq M^k$ is definable in M if there is a formula $\phi(x_1, \ldots, x_k)$ such that

$$R = \{(a_1, \ldots, a_k) \colon M \models \phi(a_1, \ldots, a_k)\}.$$

Example:
the ordering relation $\leq$ is definable in the ring $\mathbb{Z}$ via the formula

$$\phi(x, y) \equiv \exists z_1 \exists z_2 \exists z_3 \exists z_4 (x + z_1 z_1 + z_2 z_2 + z_3 z_3 + z_4 z_4 = y).$$

Finitely axiomatisable in the f.g. groups

Question (N., 2003)

Which infinite, f.g. groups can it be described (up to isomorphism) by a finite axiom system in first-order logic,

within the class of f.g. groups?

Such a group is called quasi finitely axiomatisable (QFA). Taking the conjunction of a finite axiom system, the formal definition is:

Definition (N., 2003)

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

- ϕ holds in G;
- if H is a f.g. group such that ϕ holds in H, then $G \cong H$.

Finitely axiomatisable in the f.g. groups

Many interesting groups are QFA.

- N., 2003:
  Baumslag-Solitär groups $B(1,m)$ for $m \geq 2$,
  restricted wreath product $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}$ for p a prime (not f.p.)
  Heisenberg group $\mathrm{UT}_3(\mathbb{Z})$.
- Lasserre, 2014: Thompson groups F and T; note T is simple.
- Avni and Meiri, 2023: Certain higher rank arithmetic lattices, such as $\mathrm{SL}_3(\mathbb{Z})$. Also $\mathrm{PSL}_n(\mathbb{Z})$ for $n \geq 3$.

In contrast, the free groups F_n ($n \geq 1$) are not QFA:
For $n = 1$ one uses quantifier elimination for the theory of abelian groups. For $n \geq 2$ we have $F_n \equiv F_2$ (Khar., Myasnikov; Sela).

Algebraic methods and logical methods

- The groups in N. 2003 where shown to be QFA using algebraic methods. One exploits the structure: for instance both $B(1, m)$ and $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}$ are split extensions $A \rtimes \mathbb{Z}$ with definable components, and commutators form a subgroup.
- Lasserre 2014 (Thompson groups) and Avni and Meiri 2023 (arithmetic lattices) show bi-interpretability in parameters with the ring $\mathbb{Z}$, which implies being QFA.
- $\mathrm{UT}_3(\mathbb{Z})$ is QFA, but Khelif (2007) has shown that $\mathrm{UT}_3(\mathbb{Z})$ is not bi-interpretable with $\mathbb{Z}$.

For a survey of results up to 2007 see

N., Describing Groups, Bull. Symb. Logic, the last two sections.

Algebraic method: axioms for $B(1,m) = \mathbb{Z}[1/m] \rtimes \mathbb{Z}$

Write a conjunction $\psi(d)$ of first-order properties of an element d in a group G so that $B(1,m)$ is QFA via the sentence $\exists d\, \psi(d)$. We have $B(1,m) = A \rtimes \langle d \rangle$ where $A = \mathbb{Z}[1/m]$.

Given a group G, as first axiom require that the commutators are closed under product. Then G' and hence $A = \{g : g^{m-1} \in G'\}$ are definable. Let u, v range over elements of A and x, y over elements of $C := C(d)$.

Further conditions involving d:

- A and C abelian, $|A : A^q| = q$, $|C : C^2| = 2$, and $G = A \rtimes C$,
- Conjugation action of $C - \{1\}$ on $A - \{1\}$ has no fixed points.
- $\forall u\, [d^{-1} u d = u^m]$;
- The map $u \mapsto u^q$ is 1-1, for a fixed prime q not dividing m;

Bi-interpretability of structure M with the ring $\mathbb{Z}$

Bi-interpretability of structures M, N is a property from logic, implying that the structures are model-theoretically equivalent.

Bi-interpretability of M with the ring $\mathbb{Z}$ is equivalent to:

- M is interpretable in $\mathbb{Z}$ as a ring (usually easy to show).
- There is a copy R of $\mathbb{Z}$ defined in M, together with a definable injection $\alpha\colon M \to R$ (the main work).

Mnemonic for this definition: M is a house, R its architectural plan stored inside, $\alpha(g)$ is the piece of the plan that encodes g.

Often we can define R as a subset of M. But sometimes it's necessary to represent the elements of R by equivalence classes of k-tuples for fixes k. See again N., Bull. Symb. Logic, 2007.

Examples of bi-interpretability with $\mathbb{Z}$

Definition of bi-interpretability with the ring $\mathbb{Z}$ (recall)

M is bi-interpretable with $\mathbb{Z}$ if M is interpretable in $\mathbb{Z}$ as a ring and there is a copy R of $\mathbb{Z}$ defined in M, together with a definable injection $\alpha \colon M \to R$.

- Let $M = \mathbb{Q}$. The copy R of $\mathbb{Z}$ is the natural one, f.o. definable in $\mathbb{Q}$ (J. Robinson). Now let

$$\alpha(q) = \langle r, s \rangle \text{ iff } s > 0 \wedge (r, s) = 1 \wedge qs = r.$$

- Let $M = (\mathbb{N}, +, \times)$.
  The additive group of the copy R of $\mathbb{Z}$ is the difference group, defined on equivalence classes of pairs: $\langle a, b \rangle \sim \langle c, d \rangle$ iff $a + d = b + c$. Can also define $\times$. Let $\alpha(n) = \langle n, 0 \rangle / \sim$.

Bi-interpretability in params with $\mathbb{Z}$

Definition

We say that a structure M is BI in parameters with $\mathbb{Z}$ if $(M, \overline{a})$ is BI with $\mathbb{Z}$, for some tuple of constants $\overline{a} \in M^n$.

Example:

- The ring $\mathbb{Z}[X]$ is BI with $\mathbb{Z}$ using parameter X.
  The internal copy R of $\mathbb{Z}$ is the natural one, the set of polynomials of degree 0 (Khelif, see N. 2007).
- We need a parameter, because the ring $\mathbb{Z}[X]$ has nontrivial automorphisms, so it's no BI with $\mathbb{Z}$.

Bi-interpretability in params with $\mathbb{Z}$ implies QFA

Theorem (Khelif, N.)

Let M be a finitely generated $\mathcal{S}$ structure such that M is bi-interpretable in parameters with $\mathbb{Z}$.

Then M is FA in the finitely generated $\mathcal{S}$-structures.

- Via the finite axiom system, the ring R interpreted in $(N, \overline{a})$ is required to satisfy basic axioms of arithmetic.
- Finite generation of M implies that R is "standard".
- So it must be isomorphic to $\mathbb{Z}$, whence $N \cong M$.

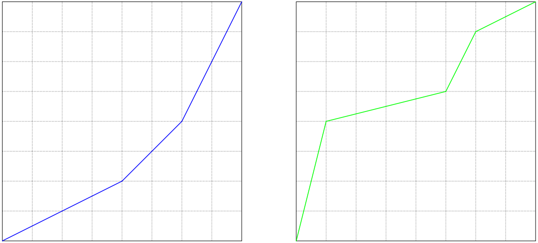
Khelif in a 2-page announcement (C. R. Math. Acad. Sci. Paris 345, 59-61, 2007) stated this result.

A full proof of a more general result is in N. 2007, Th 7.15.

Thompson groups F and T

$F \leq T$, and T is simple. Both F and T are f.p. F is the group of continuous bijections of $[0, 1]$ that are piecewise linear, and

- nondifferentiable only at dyadic rationals
- all slopes are of the form $2^z, z \in \mathbb{Z}$.



T: same conditions, except that the functions are merely continuous when $0, 1$ are identified. (Can jump from 1 to 0.)

F is BI in parameters with $\mathbb{Z}$: Step 1

Lasserre (2014) proved that F is BI in parameters with $\mathbb{Z}$.
The proof has three steps. Below all f.o. definitions can involve parameters.

Step 1: defined copies of $\mathbb{Z} \wr \mathbb{Z}$.

- For any $f \in F$ such that the bicentraliser $CC(f) = \langle f \rangle$, there is $g \in F$ such that $\langle g, f \rangle$ is naturally isomorphic to the restricted wreath product $\langle g \rangle \wr \langle f \rangle$.
- This enables us to parameter-define a copy of the ring $\mathbb{Z}$ on $\langle f \rangle$ via sum and also product of exponents.

F is BI in parameters with $\mathbb{Z}$: Step 2

For $f \in F$ let $\mathrm{Supp}(f) = \{x \in [0,1] \colon f(x) \neq x\}$.
Interpret inside F the action of F on $\mathbb{Z}[\frac{1}{2}] \cap [0,1]$.

- Represent a dyadic rational q by any pair of functions $(f,g) \in F^2$ such that $\mathrm{Supp}(f) \subset \mathrm{Supp}(g)$, both supports are open intervals, and q is their common extreme point.
- Can f.o.-define in F this set D of pairs, as well as the equivalence relation $\sim$ that two pairs represent the same dyadic rational, and the linear ordering on $D/\sim$.
- Can also f.o.-define the action $F \curvearrowright D/\sim$.
- Let a be the first standard generator of F.
- Use a f.o. defined copy of $\mathbb{Z} \wr \langle a \rangle$ to define a $1-1$ map $\tau \colon (D/\sim) \to \langle a \rangle$ such that $\tau(q) = \langle k, n \rangle$ (Cantor pairing function) where q is the rational $k2^{-n}$, k odd.

F is BI in parameters with $\mathbb{Z}$: Step 3

- Any $f \in F$ can be described by a fixed number of integers, and the breakpoints of f.
- Within the ring $\mathbb{Z}$, tuples can be definably encoded by single integers.
- This gives the 1-1 map $\alpha \colon F \to \langle a \rangle$.

To show that the simple Thompson group T is BI in params with $\mathbb{Z}$, Lasserre gives a f.o. definition of F in T, and then extends some of the definability arguments above to T.

Finite axiomatizability

within classes of

profinite groups and rings

Reference classes other than f.g.

We now look at finite axiomatisability for other reference classes $\mathcal{C}$. Is $G \in \mathcal{C}$ uniquely described by a f.o. sentence?

- For instance, let $\mathcal{C}$ be the class of homeomorphism groups of compact, connected manifolds M.
- Kim, Koberda and de la Nuez Gonzalez (2023) show that each $G \in \mathcal{C}$ is FA with respect to $\mathcal{C}$.
- For each such M they construct sentence ϕ_M in the language of groups such that $G = \text{Homeo}(L) \models \phi_M$ iff $M \cong L$, for each compact connected manifold L.
- In fact ϕ_M works for each group G such that $\text{Homeo}_0(L) \leq G \leq \text{Homeo}(L)$.

Definition of profinite group

A countably based topological group G is called profinite if G is the inverse limit of a system $\langle G_n \rangle_{n \in \mathbb{N}}$ of finite groups carrying the discrete topology.

The profinite groups coincide with the compact groups such that the clopen sets form a basis.

A similar definition works for other structures, such as rings. For instance, $\mathbb{Z}_p = \varprojlim_n C_{p^n}$ 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 $\mathrm{UT}_k(\mathbb{Z}_p)$ and $\mathrm{SL}_k(\mathbb{Z}_p)$, $k \geq 2$ are profinite: $\mathrm{SL}_k(\mathbb{Z}_p) = \varprojlim_n \mathrm{SL}_k(C_{p^n})$.

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 discrete group G is the topological 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 axiomatisability within profinite groups

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

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

Here $\cong$ denotes topological isomorphism.

$UT_3(\mathbb{Z}_p)$ is perhaps the easiest example of a profinite FA group.

Other classes of profinite structures where being FA is interesting:

- pro-p groups (should be easier than for all profinite groups),
- profinite rings, etc.

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

Proof: Write px for $\underbrace{x + \ldots + x}_{p \text{ times}}$.

Let ϕ_p be the sentence of L_{ring} expressing for a ring R:

$$px = 0 \Rightarrow x = 0$$
$$\forall x [\exists y \, py = x \vee \exists z \, xz = 1]$$
$$|R/pR| = p.$$

Clearly $\mathbb{Z}_p \models \phi_p$. 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.

FA for nilpotent groups

Theorem (Oger/Sabbagh 2006)

For an infinite, f.g. nilpotent group G,

$$G \text{ is FA in the f.g. groups} \iff Z(G)/(Z(G) \cap G') \text{ is finite.}$$

One can replace "finite" by "torsion" because any f.g. nilpotent torsion group is finite. So the condition says that each central element has a power in G'.

We prove a profinite version of this result. Special case:

Theorem (N., Segal and Tent, Proc. LMS 2021)

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

$$G \text{ is FA in the profinite groups} \iff Z(G)/(Z(G) \cap G') \text{ is torsion.}$$

Theorem (N., Segal and Tent 21, recall)

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 torsion.

Example: $\mathrm{UT}_3(\mathbb{Z}_p)$ is the pro$-p$ completion of $\mathrm{UT}_3(\mathbb{Z})$ and satisfies the O/S condition, so it is FA in the profinite groups.

- There are uncountably many non-isomorphic nilpotent of class 2 pro$-p$ groups satisfying the condition of Oger and Sabbagh (NST, 21). So not all of them can be FA.
- For general nilpotent pro-p groups G, the equivalence above holds for being finitely axiomatisable in an extended language:
- it includes finitely many unary functions f_λ, $\lambda \in \mathbb{Z}_p$, where $f_\lambda(x) = \lim_n x^{\lambda \restriction n}$. These λ's depend on G.

Examples of profinite objects that are not FA

N., Segal and Tent, 2021:

- 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.
- The group $\mathrm{UT}_3(R_S)$ is FA iff S is finite.

Finite rank, and p-adic analytic groups

- For a profinite group G, by $d(G)$ one denotes the minimal number of topological generators.
- The (Prüfer) rank is $r(G) = \sup\{d(H) \colon H \leq_c G\}$.

Lazard (1965) studied p-adic analytic groups, the analog of Lie groups in the totally disconnected setting:

- A pro-p group is p-adic analytic iff it has finite rank.
- A topological group G is p-adic analytic iff it has an open subgroup P that is pro-p and has finite rank.
- P has a "uniformly powerful" normal open subgroup U. This means that U is torsion-free, and U/U^p is abelian.

Note: Charts are defined via open subsets of $\mathbb{Z}_p^d$.
Analytic means described by power series over $\mathbb{Q}_p$.

Finite rank pro-p groups and finite axiomatisation

Let L_p be the uncountable language extending L_{group} by a unary function symbol f_λ for each $\lambda \in \mathbb{Z}_p$, interpreted as $x \to x^\lambda$.

Theorem (NST, 21)

(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 exponential operations 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.

Theorem (Recall)

Each finite rank pro-p group G is finitely axiomatizable within the pro-p groups using the language L_p.

Two ideas in the proof:

1. For each $d \geq 1$ there is a formula $\beta_d(x_1, \ldots, x_n)$ that, given a pro-p group G, expresses that n elements topologically generate G.
This uses that $\mathrm{Frat}(G)$ is definable from generators $a_1, \ldots, a_d$ of G (if they exists), and then $\mathrm{Frat}(G)$ has finite index in G. (See Prop 5.3 in NST '21.)

2. Let d be least number of generators (same as dimension of a p-adic manifold G lives on). Then any proper quotient has smaller dimension.

Now we describe G as (a) a group of dimension d, that is (b) generated by elements $x_1, \ldots, x_d$ which (c) satisfy a certain presentation of G. (See Th. 5.15 in NST '21.)

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

Let p be an odd prime. Suppose p does not divide $n \geq 2$. The groups $\mathrm{SL}_n(\mathbb{Z}_p)$ and $\mathrm{PSL}_n(\mathbb{Z}_p)$ are FA within the profinite groups.

- The proof uses the first congruence subgroup $G = \mathrm{SL}^1_n(\mathbb{Z}_p)$. This is the kernel of the natural map $\mathrm{SL}_n(\mathbb{Z}_p) \to \mathrm{SL}_n(C_p)$, where C_p is the cyclic group of order p.
- In G we look at definable closed root subgroups U, V.

  For $n \geq 3$, they are nilpotent and satisfy the Oger-Sabbagh condition, and hence can be f.o. described among all profinite groups. (For $n = 2$ describe them as $(\mathbb{Z}_p, +)$ in the context.)
- Next write some axioms that hold in G, and if profinite group H also satisfies them it is pro-p.
- Now we can use that strictly finitely presented pro-p groups of finite rank are FA within the pro$-p$ groups.

Finitely generated pro−p groups of infinite rank

Examples:

- $F_{n,p}$, the pro-p completion of the free group 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 (N., 2003) that $C_p \wr \mathbb{Z}$ is FA in the f.g. groups:

Theorem (N. Segal and Tent '21, Prop 4.5)

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

The abstract free groups F_n are not FA in the f.g. groups. It is unknown at present whether the $F_{n,p}$ are FA in pro-p groups.

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 (N., Segal and Tent, 21)

(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 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 $\mathbb{F}_p[[t]]$.
$\mathrm{Af}_1(R)$ is $R \rtimes R^\times$ with $(R^\times, \cdot)$ acting on $(R, +)$ by multiplication.

Some open questions

- Are profinite free groups of finite dimension FA? Same for free pro-p groups.
  (Segal has recent results showing FA in the profinite group for free metabelian pro p groups.)
- Complexity questions in the sense of descriptive set theory. For instance, given a f.o. sentence ϕ, how complex is the class of concrete profinite groups satisfying it? (Trival upper bound: projective.)

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.
- Lasserre, C. RJ Thompson's groups F and T are bi-interpretable with the ring of the integers. The Journal of Symbolic Logic, 79(2014), 693-711.
- N., Segal and Tent, Finite axiomatizability for profinite groups, Proc. LMS, 2021
- Avni, Nir, and Chen Meiri. On the model theory of higher rank arithmetic groups. Duke Mathematical Journal 172.13 (2023): 2537-2590.