Groups and first-order logic

André Nies

Algebra and Combinatorics Seminar

UWA

Describing groups

- We want to describe finitely generated, infinite groups by a finite amount of information.
- A finite presentation in terms of generators and relators provides such a description
- I will discuss another way to describe f.g. groups, which is based on first-order logic.
- I will also ask: If the group is finite, can we describe it by a small amount of information?
  Small = polylogarithmic in the size of the group.

First–order logic

- The first–order language of groups consists of formulas built up from equations $t(x_1, \ldots, x_k) = 1$, using $\neg, \wedge, \vee, \rightarrow, \exists x, \forall x$.
- A (first-order) sentence is a formula which has only bound variables.

Examples of first-order sentences for groups

Let $[x, y]$ denote the commutator $x^{-1}y^{-1}xy$. This is a term $t(x, y)$.

- The sentence $\forall x \forall y\ [x, y] = 1$ expresses that the group is abelian.
- The sentence "every commutator is a product of three squares", i.e.

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

holds for all groups. (Let $r = u^{-1}v^{-1}$, $s = vuv^{-1}$, and $t = v$.)

Examples of first-order sentences in real life

Consider the real-life example of a first-order language with unary predicates M, F, and a binary predicate L. Variables range over all people in Coronation Street. We interpret

- Mx as "x is a man",
- Wx as "x is a woman" and
- Lxy as "x likes y".

What does the following sentence say?

$$\forall x\,(Mx \to \exists y\ (Wy \wedge (Lxy \wedge \neg Lyx))).$$

Now add a unary function symbol g. We interpret $g(x)$ as "the mother of x". What does the following sentence say?

$$\forall y\,(Wy \to \exists x\ (Mx \wedge (Lyx \wedge \neg Lg(x)y))).$$

Expressiveness of the first-order theory

For a group G, by

$$\mathrm{Th}(G)$$

one denotes the set of sentences that hold in G. This is called the first-order theory of G.
The first-order theory of a group G contains the information whether G is

- nilpotent
- torsion-free.

Expressiveness of the first-order theory

On the other hand, many properties of infinite groups cannot be expressed by the first–order theory. For instance:

- being finitely generated: this would naively be expressed by an infinite disjunction, which is not allowed,
- the maximum condition, i.e., every subgroup is finitely generate: this would naively be second order, namely, quantification over subgroups
- simplicity: this would be another expression involving infinite disjunction

To show that the first-order theory is insufficient, we rely on the compactness theorem from logic. E.g., for the first two, every theory with an infinite model has an uncountable model.

Why first–order logic?

- A first-order property of a structure G is the most intrinsic. One does not have to go "beyond G" to verify it.
- There is a toolbox for first–order logic: compactness theorem, etc. There are fewer tools for more expressive languages.
- the first-order theory of a group is an interesting "invariant": it only depends on the group up to isomorphism.

Theory of finitely generated groups

Let G be a finitely generated (f.g.) infinite group. To what extent is G determined by $\mathtt{Th}(G)$?
Using basic results of model theory, one can prove:

- As we have seen, there is some uncountable model of $\mathtt{Th}(G)$. So besides $\mathtt{Th}(G)$, we certainly need to require that G be countable in order to determine G.
- There is in fact a a countable model not isomorphic to G. To see this, let n be the rank of G. Then $\mathtt{Th}(G)$ has infinitely many "$n+1$–types" and thus has more than one countable model.

Can it happen that G is the only finitely generated model of $\mathtt{Th}(G)$?

Quasi-axiomatizable groups

Definition

An infinite f.g. group G is called quasi-axiomatizable if, whenever H is a f.g. group with the same theory as G, then $G \cong H$.

All f.g. abelian groups G are quasi-axiomatizable. For instance, if $G = \mathbb{Z}^n$, then G is the only f.g. group such that

- G abelian and torsion-free
- $|G/2G| = 2^n$.

These properties can be captured by an infinite axiom system.

Free groups

Let F_n be the free group of rank n. The following answered a long-open questions of Tarski (1945)

Theorem (Kharlampovich/Myasnikov; Sela)

For each $n > 2$, $\mathtt{Th}(F_n) = \mathtt{Th}(F_2)$.
$\mathtt{Th}(F_2)$ *is a decidable set of sentences.*

In fact, they showed that the natural embedding $F_n \to F_k$ $(2 \leq n < k)$ preserves validity of first-order properties in both directions.

We know that $F_n \ncong F_k$ for $n \neq k$.
So, the theorem implies that F_n, $n \geq 2$, is not quasi-axiomatizable.

Nilpotent groups

Let $Z(G)$ denote the center of G, that is

$$\{g \colon \forall x\, gx = xg\}.$$

Definition

- G is nilpotent of class 1 $:\Longleftrightarrow$ G is abelian
- G is nilpotent of class $c+1 \iff$ $G/Z(G)$ is nilpotent of class c.

For each fixed c, this can be expressed by a first-order sentence.

(For finite groups, nilpotent is the same as being a direct product of p-groups for various primes p.)

Quasi-axiomatizable nilpotent groups

Theorem (Hirshon, 1977 together with Oger, 1990)

- *Each f.g. torsion-free nilpotent group of class 2 is quasi-axiomatizable.*
- *There are f.g. torsion-free nilpotent groups* G, H *of class 3 such that* $\mathtt{Th}(G) = \mathtt{Th}(H)$*, but* $G \ncong H$*.*

Proof that class-2 $\Rightarrow$ QA but class-3 $\not\Rightarrow$ QA

Hirshon (1977) studied the following question: for which groups A can $\mathbb{Z}$ be 'cancelled' from a direct product $A \oplus \mathbb{Z}$? That is,

$$A \oplus \mathbb{Z} \cong B \oplus \mathbb{Z} \Rightarrow A \cong B.$$

- It can always be cancelled when A is f.g. torsion free nilpotent of class 2.
- It can not always be cancelled when A is is f.g. torsion free nilpotent of class 3.

Oger (1990) showed: for f.g. nilpotent G, H,

$$\mathtt{Th}(G) = \mathtt{Th}(H) \iff G \oplus \mathbb{Z} \cong H \oplus \mathbb{Z}.$$

The direction $\Leftarrow$ is actually true for any groups G, H.

Quasi-finitely axiomatizable groups

We now consider groups that are characterized by a single first-order sentence, together with the information that the group is finitely generated (f.g.)

Definition

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 $G \cong H$.

Example: Fix $m \geq 2$. Then $\langle a, d \,|\, d^{-1}ad = a^m \rangle$ is QFA.

We study the property of being QFA for various classes of groups:

- abelian
- nilpotent
- metabelian

Abelian groups are never QFA

- By 'quantifier elimination' for the theory of abelian groups (Smielev, 1951), each ϕ which holds in an abelian group G also holds in

$$G \oplus \mathbb{Z}_p,$$

  for almost all primes p.
- If G is f.g. then $G \ncong G \oplus \mathbb{Z}_p$, so G is not QFA.

Thus one needs an infinite axiom system to describe G even within the f.g. groups.

QFAness for nilpotent groups

The following definitions are NOT first-order.

For a group G, let

- $G' = \langle [x, y] : x, y \in G \rangle$ the commutator subgroup.
- $\Delta(G) = \{x : \exists m > 0 \; x^m \in G'\}$. This is the least normal subgroup N such that G/N is torsion free abelian.

Sabbagh and Oger gave an algebraic characterization of QFAness for infinite nilpotent f.g. groups G.

Theorem (Oger and Sabbagh, J. Group Theory, 2006)

G is QFA $\iff Z(G) \subseteq \Delta(G)$.

Informally, G is QFA iff G is far from abelian. The implication $\Rightarrow$ holds for all f.g. groups.

The Heisenberg group if QFA

$\mathrm{UT}_3^3(\mathbb{Z}) = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$ is torsion free, and

$$Z(G) = G' = \begin{pmatrix} 1 & 0 & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

So $\mathrm{UT}_3^3(\mathbb{Z})$ is QFA by Oger/Sabbagh.

The first proof (N., 2003) was entirely different: it worked via an interpretation of arithmetic in $\mathrm{UT}_3^3(\mathbb{Z})$ due to Mal'cev.

O/S criterion for abelian, and polycyclic groups

Recall

- $G' = \langle [x, y] : x, y \in G \rangle$
- $\Delta(G) = \{x : \exists m > 0 \; x^m \in G'\}$.

For abelian G, $Z(G) = G$ and $\Delta(G)$ is the (finite) torsion subgroup. So $Z(G) \not\subseteq \Delta(G)$ (we assumed G is infinite).

Clement Lasserre in his 2011 Thesis (Univ. Paris 7) has extended the Oger/Sabbagh criterion from f.g. nilpotent to a much larger class:

Let G be a polycyclic group. Then

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

Metabelian QFA groups

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

$$AC = G,\ A \triangleleft G, \text{ and } A \cap C = \{1\}.$$

We give examples of QFA groups that are split extensions $A \rtimes C$, where A is abelian, and $C = \langle d \rangle$ infinite cyclic.

Theorem (N, 2005)

- *For each $m \geq 2$, the group*

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

  is QFA. Note that this group is finitely presented.
- *For each prime p, the restricted wreath product $\mathbb{Z}_p \wr \mathbb{Z}$ 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 $u \mapsto um$.
- By the definition, $\mathbb{Z}_p \wr \mathbb{Z}$ is a split extension $A \rtimes C$, where
  - $A = \bigoplus_{r \in \mathbb{Z}} \mathbb{Z}_p^{(r)}$, $\mathbb{Z}_p^{(r)}$ is a copy of $\mathbb{Z}_p$
  - $C = \langle d \rangle$ with d of infinite order
  - d acts on A by "shifting".

Proving that a group is QFA

The proofs that these groups of the form $G = A \rtimes C$ are QFA follow the same scheme. The group A is given by a first-order definition. 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 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 $\mathbb{Z}_p \wr \mathbb{Z}$, one uses the definition $A = \{g : g^p = 1\}$, and requires in addition that $|A : G'| = p$ and no element in $C - \{1\}$ has order $< p$.

Can a QFA group be simple?

The foregoing proofs relied on a lot of structure in order to show the group is QFA. In particular, we used several normal subgroups. For this reason I asked (2007) whether a QFA group can be simple.

Theorem (Lasserre, 2011)

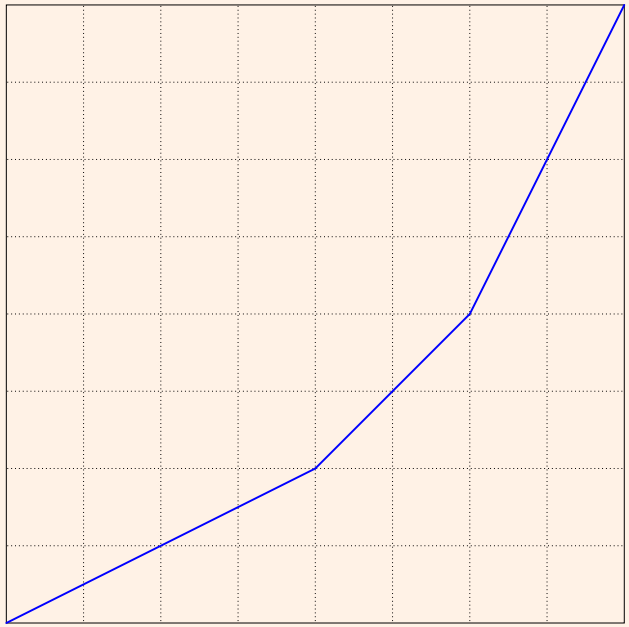
The Thompson groups F and T are QFA.

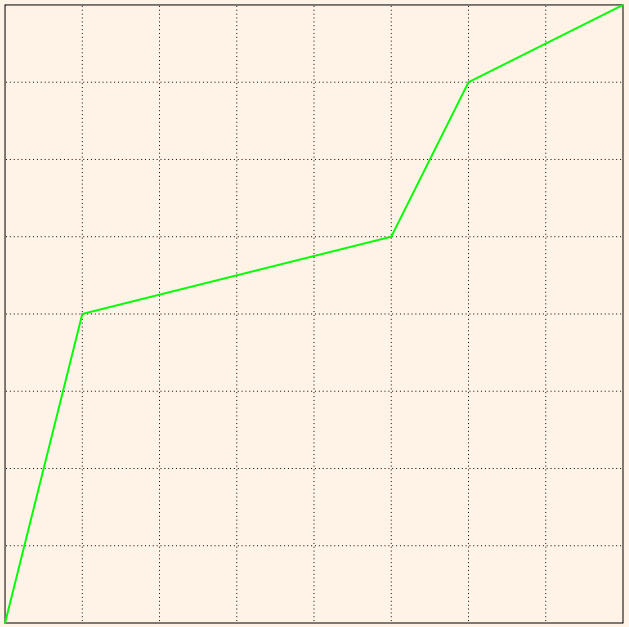
Lasserre showed bi-interpretability with $(\mathbb{Z}, +\times)$, which is known to be QFA as a ring (Sabbagh).

Thompson groups

F consists of the piecewise linear increasing bijections of $[0,1]$ with

- dyadic rational breakpoints
- all slopes of form $2^z, z \in \mathbb{Z}$





T: the same for the circle topology where $0, 1$ are identified.

$F \leq T$, and T is simple. Both F and T are finitely presented.

Homogeneity of F_2

Theorem (N., J. Algebra 2003)

F_2 is $\exists$-homogeneous. That is, if two k-tuples $\overline{g}, \overline{h}$ satisfy the same existential formulas, then they are automorphic.

This used a fact specific to F_2:
elements u, v generate a free subgroup of rank 2 iff they don't commute.

I then asked whether F_n, $n > 2$ is also homogeneous, and at which level of quantifiers.

Homogeneity of F_n

Theorem (Perrin and Sklinos, Duke Math. J., 2014; Ould Houcine, Confluentes Mathematicae, 2011)

F_n is $\forall\exists$-homogeneous. That is, if two k-tuples $\overline{g}, \overline{h}$ satisfy the same $\forall\exists$ formulas, then they are automorphic.

This used deep methods, such as JSJ decompositions (out of the solutions to Tarski's problem)

Question

If F_n $\exists$-homogeneous?

Finite groups

Reference:
Report by Yuki Maehara under Nies' supervision,
`http://arxiv.org/abs/1305.0080`

Definition

A class $\mathcal{C}$ of finite groups is polylogarithmically compressible (PLC) if for any $G \in \mathcal{C}$, there exists a first-order sentence ψ_G such that

- $|\psi_G| = O(\log^k |G|)$ for some fixed k,
- $G \models \psi_G$, and
- if $H \models \psi_G$ then $G \cong H$.

We say $\mathcal{C}$ is logarithmically-compressible (LC) if $k = 1$.

Examples of PLC classes due to Maehara/N

Theorem (Maehara/N)

Let $\mathcal{C}$ be the class of finite simple groups, with exception of the Ree groups. This class is PLC.

Theorem

The class of finite symmetric groups is LC.

Theorem

The class of finite abelian groups is LC.

Question

Is the class of all finite groups polylogarithmically compressible?

A good test case would be the p-groups.