Systems of Equations in Random Nilpotent Groups

Albert Garreta (joint results with Alexei Miasnikov and Denis Ovchinnikov)

Stevens Institute of Technology

Nilpotent groups

- Let G be a group. We define $[x, y] = x^{-1}y^{-1}xy$, and $\Gamma_1(G) = G$, $\Gamma_2(G) = [G, G]$, $\ldots$, $\Gamma_k(G) = [G, \Gamma_{k-1}(G)]$.
- G is *k-nilpotent* if $\Gamma_{k+1}(G) = 1$.
- G is 2-nilpotent iff $[G, G] \subseteq Z(G)$.
- A *τ_2-group* is a finitely generated, torsion-free, 2-nilpotent group. We write $G \in T_2$.

Diophantine problem in algebraic structures

- Let A be an algebraic structure (e.g. a group or a ring). $\mathscr{E}(A)$ is the problem of determining the solubility of systems of equations over A.
- $\mathscr{E}(A)$ is *decidable* if there exists an algorithm that, given a system of equations S over A, determines whether S admits a solution or not in A.
- *Hilbert's 10th Problem*. $\mathscr{E}(\mathbb{Z}, +, \cdot)$ is undecidable.

Question

Let $G \in T_2$. When is $\mathscr{E}(G)$ decidable? Is $\mathscr{E}(G)$ usually decidable or undecidable?

- What does 'usually' mean?

Equations in nilpotent groups

- There exists a 4-nilpotent group G such that $\mathscr{E}(G)$ is undecidable (Roman'kov, 1974).

Free nilpotent group

The *free k-nilpotent group* on generators S is

$$N = \langle\ S \mid \Gamma_{k+1}(N) = 1\ \rangle.$$

- $\mathscr{E}(G)$ is undecidable in any free nonabelian nilpotent group G. (Duchin, Liang, Shapiro, 2014).

Equations in nilpotent groups

Let $G \in T_2$, and let a, $b \in G$ be such that $[a, b] \neq 1$.

Theorem (G., Miasnikov, Ovchinnikov)

There exists a nontrivial integral domain $R_{a,b}$ such that $(R_{a,b}, +)$ is free abelian and such that if $\mathscr{E}(G)$ is decidable, then $\mathscr{E}(R_{a,b})$ is decidable.

If $R_{a,b} = (\mathbb{Z}, +, \cdot)$ then we say a and b are in *general position*. We write $a, b \in GP$.

Corollary

Suppose $a, b \in GP$ for some $a, b \in G$. Then $\mathscr{E}(G)$ is undecidable.

Integral elements

Let $g \in G$. Suppose

$$C(g) = \{x \in G \mid [x, g] = 1\} = \{g^t z \mid t \in \mathbb{Z},\ z \in Z(G)\}.$$

Then we say g is an *integral element*.

Lemma (GMO)

If $a, b \in G$ are integral and $[a, b] \neq 1$, then $a, b \in GP$.

Here is an outline of the proof:

- Let $[a, b] = c$. We have

$$[a, C(b)] = [C(a), b] = \{c^t \mid t \in \mathbb{Z}\}.$$

Let Z denote this set.

Outline of the proof

- We define $+$ and $\cdot$ in Z by letting $c^{t_1} + c^{t_2} = c^{t_1+t_2}$, and $c^{t_1} \cdot c^{t_2} = c^{t_1 t_2}$. Using that G is torsion-free, we have

$$(Z, +, \cdot) \cong (\mathbb{Z}, +, \cdot).$$

- $x \in Z$ can be expressed in terms of equations:

$$x = [a, x'], \quad [x', b] = 1.$$

- $\forall x, y, z \in Z$ we have
  - $z = x + y$ (since G is torsion free this has the form $c^{t_1} + c^{t_2} = c^{t_1+t_2}$) iff $z = xy$ in G.
  - $z = x \cdot y$ iff $x = [a, x']$, $[x', b] = 1$, $y = [y', b]$, $[y', a] = 1$, and $z = [y', x']$
- Hence Z, $+$, and $\cdot$ are *definable in G by equations*. $\square$

New question and random nilpotent groups

New question

Do groups $G \in T_2$ usually have a pair of non-commuting integral elements?
In other words, if we randomly pick a group G from T_2, how likely is G to have such elements?

- The study of random nilpotent groups started around 2015.
- Three models have been introduced so far.

T_2-presentations

- F.g. nilpotent groups are polycyclic. Such groups have a standard way to be presented: by means of polycyclic presentations.
- Polycyclic presentations look nice for $G \in T_2$.

Lemma (GMO)

A group G is free abelian or $G \in T_2$ if and only if G admits the following presentation:

$$G = \langle A, C \mid [a_i, a_j] = \prod_{t=1}^{m} c_t^{\lambda_t^{ij}}, \quad 1 \leq i < j \leq n,$$
$$[A, C] = 1, \quad [C, C] = 1 \rangle \tag{1}$$

for some $\lambda_t^{ij} \in \mathbb{Z}$, and $A = \{a_1, \ldots, a_n\}$, $C = \{c_1, \ldots, c_m\}$.

- We call such presentation a T_2-presentation.

Random nilpotent groups as random polycyclic groups

Model (GMO)

- We can randomly choose $G \in T_2$ by randomly selecting a T_2-presentation.[1]
- This can be done by fixing sets A, C, and then specifying integers λ_t^{ij} with $|\lambda_t^{ij}| \leq l$ for some large l.

- Let P be a property. We write $Pr(G \textit{ has property } P) = p$ to mean that the proportion of groups G with property P chosen this way tends to p as $l \to \infty$.
- If $p = 1$ then we say G *has property* P *asymptotically almost surely (a.a.s.)*.
- $|A| = n$ and $|C| = m$ act as parameters.

[1] Alternatively, this model can be understood as randomly selecting a Malcev basis and rules for writting the Malcev representation of xy in terms of x and y

Another model: nilpotent groups as members of a variety

Cordes, Duchin, Duong, Ho, and Sánchez model (2015)

A k-nilpotent group G can be randomly chosen by adding relations R of length $\leq l$ to some free k-nilpotent group N_k. I.e.

$$G = N_k/\langle\langle R \rangle\rangle.$$

- $|R|$ can be a constant (Olshanskii's model), or a function of l (Gromov's model).
- This model arises from looking at k-nilpotent groups as a variety.
- Mainly, the authors study the probability that G is trivial or abelian.

Another model: nilpotent groups as subgroups of $UT_n(\mathbb{Z})$

- A group G is f.g. torsion-free nilpotent iff it can be embedded in $UT_n(\mathbb{Z})$.

Delp, Dymarz, and Schaffer-Cohen model (2016)

- G can be randomly chosen by selecting matrices from $UT_n(\mathbb{Z})$ as the generators of G.
- This is done by specifying m words of length l on the set of standard generators of $UT_n(\mathbb{Z})$ (including inverses).

- l is taken to be a function of n, and $n \to \infty$.
- The authors study the probability that G is abelian (for $m = 2$).

Main results

- Fix n and m. Randomly choose $G \in T_2$ by selecting a T_2-presentation. I.e. fix A, C, and choose λ_t^{ij}'s.
- Roughly, $|A| = rank(G/Z(G))$, and $|C| = rank(Z(G))$.
- Recall that g is integral if $C(g) = \{g^t z \mid t \in \mathbb{Z},\ z \in Z(G)\}$. We write $a, b \in Int$ if $[a, b] \neq 1$ and a, b are integral.

Theorem (G., Miasnikov, Ovchinnikov)

- *If* $|C| \geq |A| - 1$, *then* G *has* $a, b \in Int$ *a.a.s. (as* $l \to \infty$*).*
- *If* $|C| \leq (|A| - 1)/2$, *then* G *does not have* $a, b \in Int$ *a.a.s.*

Corollary

If $|C| \geq |A| - 1$, *then* $\mathscr{E}(G)$ *is undecidable a.a.s.*

Thank you!

Bonus slides

First model: nilpotent groups as a variety

Theorem (Cordes, Duchin, Duong, Ho, Sánchez)

- *G is nonabelian a.a.s. if $|R| \leq m - 2$.*
- *If $|R| = m - 1$ or m, the probability that G is abelian approaches (descendingly) 44% and 85% as $m \to \infty$, respectively.*

A remark: G is a f.g. nilpotent group iff it is a quotient of some $N_{k,m}$. Equivalently, iff

$$[[x_1, x_2], x_3] = 1 \quad \forall\, x_1, x_2, x_3 \in G, \quad \text{case } k = 2.$$
$$[[[x_1, x_2], x_3], x_4] = 1 \quad \forall\, x_1, x_2, x_3, x_4 \in G, \quad \text{case } k = 3.$$

Hence k-nilpotent groups form a variety. This first model arises from looking at nilpotent groups as such.

First model: nilpotent groups as a variety

- Let P be a property. We write $Pr(G \textit{ has property } P) = p$ to mean that the proportion of choices of R such that G has property P tends to p as $l \to \infty$.
- If $p = 1$ then we say *G has property P asymptotically almost surely (a.a.s.)*

Theorem (Cordes, Duchin, Duong, Ho, Sánchez)

- *G is trivial a.a.s. if and only if $|R| \to \infty$ as a function of l.*
- *$G = [G, G]$ a.a.s. if and only if $|R| \to \infty$ as a function of l.*

Second model: nilpotent groups as subgroups of $UT_n(\mathbb{Z})$

Theorem (Delp, Dymarz, Schaffer-Cohen)

- *If* $l \in o(\sqrt{n})$, *then* G *is abelian a.a.s. (as* $n \to \infty$*).*
- *If* $l = c\sqrt{n}$, *then* G *is abelian with probability* e^{-2c^2}.
- *If* $l \in w(\sqrt{n})$, *then* G *is nonabelian a.a.s.*

Theorem

- *If* $l \in o(n^2)$, *then* G *is not* $(n-1)$*-nilpotent a.a.s.*
- *If* $l \in w(n^3)$, *then* G *is* $(n-1)$*-nilpotent a.a.s.*