Dehn Monsters

Alexei Miasnikov
(Stevens Institute)

WEBINAR, Group Theory International,
January, 2011

Abstract

I will discuss new types of finitely generated recursively presented groups with undecidable Word Problem, called Dehn monsters.

In fact, the Word Problem is so bad in these groups that there is no any algorithmic way to produce an infinite set of pairwise distinct elements of G.

We use Golod-Shafarevich construction and immune sets from the classical recursion theory to build Dehn monsters.

Outline

- Finitely generated groups
- The Word Problem in groups.
- Algorithmically finite groups.
- Golod-Shafarevich and Dehn Monsters

Finitely generated groups

Let X be a finite set.

$F(X)$ a free group with basis X (viewed as the set of reduced words in $X \cup X^{-1}$).

$R \subseteq F(X)$ and $\langle\langle R \rangle\rangle$ the normal closure of R in $F(X)$.

$G = \langle X \mid R \rangle \iff G = F(X)/\langle\langle R \rangle\rangle$.

G is finitely presented iff $G = \langle X \mid R \rangle$ for some finite X and R.

Beyond finitely presented groups

There interesting examples of finitely generated not finitely presented groups:

- wreath products of abelian groups;
- free solvable groups;
- The Grigorchuk group.

Of course, most of the finitely generated groups are not finitely presented.

A general theory of "tractable" finitely generated groups?

Beyond finitely presented groups

There interesting examples of finitely generated not finitely presented groups:

- wreath products of abelian groups;
- free solvable groups;
- The Grigorchuk group.

Of course, most of the finitely generated groups are not finitely presented.

A general theory of "tractable" finitely generated groups?

Computably enumerable sets

A subset $W \subseteq F(X)$ is computably enumerable (c.e.) if there exists an algorithm A that computes a function $f : \mathbb{N} \to F(X)$ whose image is W.

In this case $W = \{w_1, w_2, \ldots, \}$, where $w_i = f(i)$.

Recursively presented groups

A group G is recursively presented if it has a presentation $G = \langle X \mid R \rangle$, where X is finite and the set of relators R is a c.e. subset of $F(X)$.

Notice, that if R is c.e., then the normal subgroup $\langle\langle R \rangle\rangle$ generated by R is also c.e.

In particular, G is recursively presented iff the set $WP(G) = \{w \in F(X) \mid w = 1 \text{ } in \text{ } G\}$ is c.e.

Higman's Embedding Theorem

Recursively presented groups = finitely generated subgroups of finitely presented groups.

Non-recursively presented groups in general seem beyond our reach.

We are lacking general methods to construct such groups.

Forcing, priority methods, ..

Recursively presented groups

Non-recursively presented groups in general seem beyond our reach.

We are lacking general methods to construct such groups.

Forcing, priority methods, ..

The Word Problem

The original Word Problem (WP) for groups was formulated by M.Dehn in 1910/1912 (and two years later by A. Thue for semigroups in a similar fashion) in the following way:

> *Construct an algorithm to determine for an arbitrary finitely presented group $G = \langle X \mid R \rangle$ and any two words u and v in the alphabet $X \cup X^{-1}$ whether or not u and v represent the same element of G.*

Certainly, Dehn and Thue believed that such an algorithm should exist.

Notice, that not only they asked to find a decision algorithm they were actually asking to find a uniform decision algorithm that would work for all such groups (and semigroups).

The original Word Problem (WP) for groups was formulated by M.Dehn in 1910/1912 (and two years later by A. Thue for semigroups in a similar fashion) in the following way:

> *Construct an algorithm to determine for an arbitrary finitely presented group $G = \langle X \mid R \rangle$ and any two words u and v in the alphabet $X \cup X^{-1}$ whether or not u and v represent the same element of G.*

Certainly, Dehn and Thue believed that such an algorithm should exist.

Notice, that not only they asked to find a decision algorithm they were actually asking to find a uniform decision algorithm that would work for all such groups (and semigroups).

The original Word Problem (WP) for groups was formulated by M.Dehn in 1910/1912 (and two years later by A. Thue for semigroups in a similar fashion) in the following way:

> *Construct an algorithm to determine for an arbitrary finitely presented group $G = \langle X \mid R \rangle$ and any two words u and v in the alphabet $X \cup X^{-1}$ whether or not u and v represent the same element of G.*

Certainly, Dehn and Thue believed that such an algorithm should exist.

Notice, that not only they asked to find a decision algorithm they were actually asking to find a uniform decision algorithm that would work for all such groups (and semigroups).

The Word Problem

If the group G is fixed one does not need relations to formulate WP in G (only a fixed finite set of generators).

Furthermore, decidability of WP in G does not depend on a given finite set of generators, it is a property of the group.

Classical examples of undecidable WP

In 1947 Markov and Post constructed independently first finitely presented semigroups with undecidable EP.

In 1955 Novikov, and soon after W.W. Boone, constructed independently finitely presented groups with undecidable EP.

More examples of undecidable WP

Now there are much shorter examples of semigroups with undecidable word problem constructed by G. S. Tseitin, D. Scott, Matiyasevich, Makanin.

Other examples of groups with undecidable Word Problem are due to J. L. Britton, V.V. Borisov, and D.J. Collins.

An excellent exposition of the results in this area with complete and improved proofs is given in the survey by S.I. Adian and V.G. Durnev.

Groups with undecidable WP

All the classical examples of groups with undecidable WP are based on the same idea:

given a Turing machine M one constructs a group $G(M)$ such that the WP in G simulates the Halting Problem of M.

The Halting Problem for M

For a given initial configuration C of the tape decide if M halts when started on C or not.

Turing: The Halting Problem for a universal Turing machine is undecidable.

Simulation: For a given configuration C one effectively constructs a word w_C in the generators of $G(T)$ such that M halts on C if and only if $w_C = 1$ in G.

Hence, if the Halting Problem for M is undecidable then the WP in $G(M)$ is undecidable.

The Halting Problem for M

For a given initial configuration C of the tape decide if M halts when started on C or not.

Turing: The Halting Problem for a universal Turing machine is undecidable.

Simulation: For a given configuration C one effectively constructs a word w_C in the generators of $G(T)$ such that M halts on C if and only if $w_C = 1$ in G.

Hence, if the Halting Problem for M is undecidable then the WP in $G(M)$ is undecidable.

The Halting Problem for M

For a given initial configuration C of the tape decide if M halts when started on C or not.

Turing: The Halting Problem for a universal Turing machine is undecidable.

Simulation: For a given configuration C one effectively constructs a word w_C in the generators of $G(T)$ such that M halts on C if and only if $w_C = 1$ in G.

Hence, if the Halting Problem for M is undecidable then the WP in $G(M)$ is undecidable.

Undecidable WP

Are there really different types of groups with undecidable WP?

Theorem

For every c.e. Turing degree T there is a finitely presented group G with the word problem $WP(G)$ of Turing degree T.

So, yes, there are different types of groups with undecidable WP.

But what are the algebraic properties of these groups? Not much is known.

Undecidable WP

Are there really different types of groups with undecidable WP?

Theorem

For every c.e. Turing degree T there is a finitely presented group G with the word problem $WP(G)$ of Turing degree T.

So, yes, there are different types of groups with undecidable WP.

But what are the algebraic properties of these groups? Not much is known.

Undecidable WP

Are there really different types of groups with undecidable WP?

Theorem

For every c.e. Turing degree T there is a finitely presented group G with the word problem $WP(G)$ of Turing degree T.

So, yes, there are different types of groups with undecidable WP.

But what are the algebraic properties of these groups? Not much is known.

Generic complexity

In the era when much of the focus is on practical computing, the complexity of computations became an important issue.

A new notion of generic complexity of computations was developed (Kapovich, Miasnikov, Shpilrain, Schupp).

In this model one is looking for partial decision algorithms which are correct (do not make any errors) and perform well on typical, i.e. generic inputs.

Generic complexity

WP is generically decidable in a group G with a finite generating set X if there is a correct partial algorithm A that solves the Word Problem in G on most words from $F(X)$.

That is, the halting set of A is generic with respect to the stratification of $F(X)$ given by the standard length function $|\cdot|$ on $F(X)$.

Generic complexity

WP is generically decidable in a group G with a finite generating set X if there is a correct partial algorithm A that solves the Word Problem in G on most words from $F(X)$.

That is, the halting set of A is generic with respect to the stratification of $F(X)$ given by the standard length function $|\cdot|$ on $F(X)$.

Generic sets

Recall, that $T \subseteq F(X)$ is generic in $F(X)$ if

$$\rho_n(T) = \frac{|T \cap S_n|}{|S_n|} \to 1 \textit{ for } n \to \infty,$$

where $S_n = \{w \in F(X) \mid |w| = n\}$.

Furthermore, T is exponentially generic if $\rho_n(T)$ converges to 1 exponentially fast.

Question

What are groups $G = \langle X \mid R \rangle$ with really hard WP?

Known:

- There are groups $G(M)$ with undecidable word problem.
- For a universal Turing machine M the WP in $G(M)$ is as hard as possible: WP(G) is an m-complete c.e. set.
- However, in all classical examples of groups $G(M)$ the WP is linear time decidable on some generic sets of inputs.

Question: Are there finitely (or recursively) presented groups with WP hard on most inputs?

Remark [Hamkins and Myasnikov]

The halting problem for Turing machines is easy (linear time) on most inputs.

Groups with hard WP

Question: Are there finitely (or recursively) presented groups with WP hard on most inputs?

Remark [Hamkins and Myasnikov]

The halting problem for Turing machines is easy (linear time) on most inputs.

Take a finitely presented semigroup

$$\mathfrak{S} = \langle a_1, \ldots, a_n | r_1 = s_1, \ldots, r_k = s_k \rangle = \langle A \mid R \rangle$$

For a letter $x \notin A$ put

$$\mathfrak{S}_x = \langle A, x | R, x = xa_1, \ldots, x = xa_n, x = xx \rangle.$$

Theorem [Myasnikov, Rybalov]

If the word problem in $\mathfrak{S}$ is undecidable then the word problem in $\mathfrak{S}_x$ is super-undecidable (undecidable on every generic subset of inputs).

Tseitin Example

Example

In 1956 Tseitin constructed a semigroup $\mathfrak{T}$ presented by 5 generators and 7 relations with unsolvable word problem:

$$\mathfrak{T} = \langle a, b, c, d, e \mid ca, ad = da, bc = cb, bd = db,$$

$$ce = eca, de = edb, cca = ccae \rangle.$$

In this case the super-undecidable semigroup $\mathfrak{T}_x$ has 6 generators and 13 relators whose total length is equal to 49.

Theorem (Gilman, Myasnikov, Osin)

Let G be a finitely presented amenable group with an unsolvable word problem. The word problem for G is not solvable on any exponentially generic set of inputs.

Finitely presented amenable groups with an unsolvable word problems exist [Kharlampovich].

Question Does there exist a group whose word problem is not solvable on any generic sets of inputs?

Question Does there exist a a group whose word problem is not solvable on any set of positive density?

Algorithmically finite groups

A finitely generated group G is algorithmically finite if there is no any algorithmic way to produce an infinite set of pairwise distinct elements of G.

More precisely, let G be be a group generated by a finite set X and $\eta : F(X) \to G$ the canonical projection.

Definition

A group G is algorithmically finite if for every infinite computably enumerable subset $W \subseteq F(X)$ there exist at least two distinct words $u, v \in W$ such that $\eta(u) = \eta(v)$.

Algorithmically finite groups

A finitely generated group G is algorithmically finite if there is no any algorithmic way to produce an infinite set of pairwise distinct elements of G.

More precisely, let G be be a group generated by a finite set X and $\eta : F(X) \to G$ the canonical projection.

Definition

A group G is algorithmically finite if for every infinite computably enumerable subset $W \subseteq F(X)$ there exist at least two distinct words $u, v \in W$ such that $\eta(u) = \eta(v)$.

Elementary properties

Let $G = \langle X \rangle$ be an algorithmically finite group. Then:

1. For every infinite computably enumerable subset $W \subseteq F(X)$, there exist infinitely many pairs of distinct words $u_i, v_i \in W$ such that $\eta(u_i) = \eta(v_i)$.
2. If WP is decidable on a computably enumerable subset $W \subseteq F(X)$, then $\eta(W)$ is finite.

Basic properties of Dehn Monsters

Recall that a *section* of a group G is a quotient group of a subgroup of G.

Elementary Properties

Let G be an algorithmically finite group. Then the following hold.

1. Every finitely generated section of G is algorithmically finite.
2. WP is undecidable in every finitely generated infinite section of G.
3. G is a torsion group.

Independence of generators

If a finitely generated group G is algorithmically finite with respect to some finite generating set X then it is algorithmically finite with respect to any finite generating set of G.

Hence, algorithmic finiteness is a property of a group, not a presentation.

Clearly every finite group is algorithmically finite.

Theorem [Myasnikov, Osin]

There exists a recursively presented infinite algorithmically finite group.

We will see later that WP in algorithmically finite groups is decidable only on negligible sets of inputs (sets of measure zero).

Motivated by this observation, we call recursively presented infinite algorithmically finite groups Dehn monsters.

The proof of this result is based on new ideas and does not interpret any machines.

Instead, it uses Golod-Shafarevich presentations as a tool to control consequences of relations and simple and immune sets from computability theory.

These groups are not finitely presented.

What is decidable in every recursively presented group?

Let G be a group generated by a finite set X. For elements $u_1, \ldots, u_k \in F(X)$ put

$$Cos(u_1, \ldots, u_k) = u_1 WP(G) \cup \ldots \cup u_k WP(G).$$

Lemma

Let $G = \langle X \mid R \rangle$ be a recursively presented group.Then for any $u_1, \ldots, u_k \in F(X)$ the following holds:

- The set $Cos(u_1, \ldots, u_k)$ is an infinite computably enumerable subset of $F(X)$;
- WP is decidable in $Cos(u_1, \ldots, u_k)$.

What is decidable in a Dehn monster?

Theorem

Let $G = \langle X \mid R \rangle$ be a Dehn monster. Then:

- Every computably enumerable subset $W \subseteq F(X)$ with decidable WP in G is contained in the set $Cos(u_1, \ldots, u_k)$ for some $u_1, \ldots, u_k \in F(X)$.
- Every computably enumerable subset $W \subseteq F(X)$ with decidable WP in G is negligible, i.e.,

$$\lim_{n \to \infty} \rho_n(W) = 0.$$

- If G is non-amenable, then W is exponentially negligible, i.e., there exists $t > 1$ such that

$$\rho_n(W) = O(t^{-n}).$$

Here, as before, $\rho_n(W) = \frac{|W \cap S_n|}{|S_n|}$.

Golod-Shafarevich and algorithmically finite groups

Theorem [Myasnikov, Osin]

For every Golod-Shafarevich group $\langle X \mid S\rangle$ there exists a simple set of relations $R \subseteq F(X)$ such that the quotient $\langle X \mid S \cup R\rangle$ is again Golod-Shafarevich algorithmically finite group.

Corollary

There exists a recursively presented non-amenable algorithmically finite group (Dehn Monsters).

Magnus Embeddings

Let $X = \{x_1, ..., x_d\}$ be a finite set.

$\Lambda_p = \mathbb{Z}_p[[u_1, \ldots, u_d]]$ the ring of non-commutative formal power series over the field $\mathbb{Z}_p$ (p is a fixed prime) in d variables $u_1, \ldots, u_d$.

The map $X \to \Lambda_p$ given by

$$x_i \mapsto 1 + u_i$$

extends (uniquely) to an injective homomorphism

$$\pi : F(X) \to \Lambda_p^*,$$

called the Magnus embedding.

Zassenhaus filtration

The Zassenhaus p-series (filtration)

$$F = D_1F > D_2F > \ldots > D_nF > \ldots$$

in F is defined by the dimension subgroups D_nF of F, where

$$D_nF = \{f \in F \mid f \equiv 1 \ mod \ I_n\}$$

It is not hard to see that for any $f \in F$ there exists a unique $n \geq 1$, termed the degree $deg(g)$ of f, such that $f \in D_nF \smallsetminus D_{n+1}F$.

$$D_1F = F, \quad [D_iF, D_jF] \subseteq D_{i+j}F, \quad (D_iF)^p \subseteq D_{ip}F.$$

In particular, the quotients F/D_nF are finite p-groups.

Let $P = \langle X \mid R \rangle$ be a presentation.

Denote by $n_i(R)$ the number of relators in R of degree i with respect to the Zassenhaus p-series in $F(X)$.

Consider the following formal power series in t:

$$H_p(X, R, t) = 1 - \hat{d}t + \Sigma_{i=1}^{\infty} n_i(R) t^i,$$

where $\hat{d} = d(\Gamma_{\hat{p}})$ is the minimal number of topological generators of the pro-p completion $\Gamma_{\hat{p}}$ of the discrete group Γ defined by the presentation $\langle X \mid R \rangle$.

It is known that $\hat{d} = |X|$ if and only if $n_1(R) = 0$.

Golod-Shafarevich presentation

Definition

A presentation $P = \langle X \mid R \rangle$ is termed a *Golod-Shafarevich presentation* if there exists $0 < t_0 < 1$ such that $H_p(X, R, t_0) < 0$.

The following is the principal result about Golod-Shafarevich presentations. It was proved by Golod and Shafarevich with some further improvements by Vinberg and Gaschutz.

Theorem

Any Golod-Shafarevich presentation defines an infinite group.

Construction

Idea of the construction:

Starting with a given Golod-Shafarevich presentation $G = \langle X \mid S \rangle$ we construct a set of relations $R \subseteq F(X)$ in such a way that the following requirements are satisfied for each $e \in \mathbb{N}$ (below $k(G)$ is a fixed natural number which depends on G):

($\mathbf{L}_e$) $|\{r \in R \mid deg(r) \leq e\}| \leq \max\{e - k(G), 0\}$.

($\mathbf{M}_e$) If a c.e. set W_e is infinite, then there are two distinct words $u, v \in W_e$ such that $uv^{-1} \in R$.

Now we describe an algorithm A that enumerates such a subset $R \subseteq F(X)$ in stages $0, 1, 2, \ldots, s, \ldots,$.

- At each stage s for each as yet unsatisfied condition $(\mathbf{M}_e)$, $e < s$, A enumerates W_e up to s steps and looks for two distinct words $u, v \in W_e$ such that their images are equal in the quotient $F/D_{e+k(G)}F$.

  Since the Magnus embedding is effective, the quotient groups group F/D_iF have uniformly solvable Word Problem. Thus A can effectively either find such a pair u, v or conclude that there is no such a pair at this stage for a given $e < s$.

Now we describe an algorithm A that enumerates such a subset $R \subseteq F(X)$ in stages $0, 1, 2, \ldots, s, \ldots,$.

- At each stage s for each as yet unsatisfied condition $(\mathbf{M}_e)$, $e < s$, A enumerates W_e up to s steps and looks for two distinct words $u, v \in W_e$ such that their images are equal in the quotient $F/D_{e+k(G)}F$.

  Since the Magnus embedding is effective, the quotient groups group F/D_iF have uniformly solvable Word Problem. Thus A can effectively either find such a pair u, v or conclude that there is no such a pair at this stage for a given $e < s$.

- If such a pair u, v for an unsatisfied M_e, $e < s$ occurs at the stage s, the algorithm includes the word uv^{-1} into R, and marks $(\mathbf{M}_e)$ as satisfied.
- When the stage s is finished (note that there are at most s unsatisfied conditions $(\mathbf{M}_e)$ with $e < s$ to check at this stage) the algorithm goes to the stage $s + 1$.

- If such a pair u, v for an unsatisfied M_e, $e < s$ occurs at the stage s, the algorithm includes the word uv^{-1} into R, and marks $(\mathbf{M}_e)$ as satisfied.
- When the stage s is finished (note that there are at most s unsatisfied conditions $(\mathbf{M}_e)$ with $e < s$ to check at this stage) the algorithm goes to the stage $s + 1$.

Construction

If W_e is infinite then there are some distinct words $u, v \in W_e$ that define the same element in the finite quotient $F/D_{e+k(G)}F$.

Thus the set $R \subseteq F(X)$ produced by A satisfies all conditions $(\mathbf{M}_e)$, $e \in \mathbb{N}$.

To see that all the conditions $(\mathbf{L}_e)$ are satisfied observe that if some relation uv^{-1} was added to R at some stage for a given set W_e then $u = v$ in $F/D_{e+k(G)}F$, so

$$deg(uv^{-1}) \geq e + k(G).$$

This shows that $|\{r \in R \mid deg(r) \leq i\}| \leq \max\{i - k(\varepsilon), 0\}$, as claimed.

Construction

If W_e is infinite then there are some distinct words $u, v \in W_e$ that define the same element in the finite quotient $F/D_{e+k(G)}F$.

Thus the set $R \subseteq F(X)$ produced by A satisfies all conditions $(\mathbf{M}_e)$, $e \in \mathbb{N}$.

To see that all the conditions $(\mathbf{L}_e)$ are satisfied observe that if some relation uv^{-1} was added to R at some stage for a given set W_e then $u = v$ in $F/D_{e+k(G)}F$, so

$$deg(uv^{-1}) \geq e + k(G).$$

This shows that $|\{r \in R \mid deg(r) \leq i\}| \leq \max\{i - k(\varepsilon), 0\}$, as claimed.

If W_e is infinite then there are some distinct words $u, v \in W_e$ that define the same element in the finite quotient $F/D_{e+k(G)}F$.

Thus the set $R \subseteq F(X)$ produced by A satisfies all conditions $(\mathbf{M}_e)$, $e \in \mathbb{N}$.

To see that all the conditions $(\mathbf{L}_e)$ are satisfied observe that if some relation uv^{-1} was added to R at some stage for a given set W_e then $u = v$ in $F/D_{e+k(G)}F$, so

$$deg(uv^{-1}) \geq e + k(G).$$

This shows that $|\{r \in R \mid deg(r) \leq i\}| \leq \max\{i - k(\varepsilon), 0\}$, as claimed.

Construction

If W_e is infinite then there are some distinct words $u, v \in W_e$ that define the same element in the finite quotient $F/D_{e+k(G)}F$.

Thus the set $R \subseteq F(X)$ produced by A satisfies all conditions $(\mathbf{M}_e)$, $e \in \mathbb{N}$.

To see that all the conditions $(\mathbf{L}_e)$ are satisfied observe that if some relation uv^{-1} was added to R at some stage for a given set W_e then $u = v$ in $F/D_{e+k(G)}F$, so

$$deg(uv^{-1}) \geq e + k(G).$$

This shows that $|\{r \in R \mid deg(r) \leq i\}| \leq \max\{i - k(\varepsilon), 0\}$, as claimed.

Open problems: finite presentations

Notice, that Golod-Shafarevich Dehn monsters are not finitely presented.

Open Problem 1

Does there exist a finitely presented Dehn monster?

This is a real challenge, since every Dehn monster is an infinite torsion group and no examples of finitely presented infinite torsion groups are known.

Open Problem 2

Does there exist a finitely presented group such that

a) WP is decidable only on negligible sets of inputs;

b) WP is undecidable on every generic set of inputs?

Open problems: finite presentations

Notice, that Golod-Shafarevich Dehn monsters are not finitely presented.

Open Problem 1

Does there exist a finitely presented Dehn monster?

This is a real challenge, since every Dehn monster is an infinite torsion group and no examples of finitely presented infinite torsion groups are known.

Open Problem 2

Does there exist a finitely presented group such that

a) WP is decidable only on negligible sets of inputs;
b) WP is undecidable on every generic set of inputs?

Open problems: more paradoxical

There are residually finite finitely generated infinite algorithmically finite groups.

They are not finitely presented, of course.

Problem 3

Does there exist a residually finite Dehn Monster?

Open problems: more paradoxical

We also observe that every elementary amenable algorithmically finite group is finite.

This motivates another problem.

Problem 4

Does there exist an infinite amenable algorithmically finite group (an amenable Dehn Monster)?