Isomorphism problem for virtually free groups

Michal Ferov

University of Technology Sydney

November 27, 2017

Joint work (in progress) with Murray Elder and Alan Logan.

Isomorphism problem in groups

Given two structures, it is natural to ask whether they are isomorphic. This is called *the isomorphism problem*. In this talk we will consider isomorphism problem for groups.

Definition (Isomorphism problem for groups)

Given two groups G_1, G_2 we ask whether $G_1 \cong G_2$.

Isomorphism problem in groups

Given two structures, it is natural to ask whether they are isomorphic. This is called *the isomorphism problem*. In this talk we will consider isomorphism problem for groups.

Definition (Isomorphism problem for groups)

Given two groups G_1, G_2 we ask whether $G_1 \cong G_2$.

How are the groups G_1, G_2 given?

- Cayley table?
- Generators and a "nice" formula?
- *Presentation!*

Group Presentation

Definition

Let X be a set and let $R \subseteq (X \cup X^{-1})^*$ be a set of words over X (and inverses). We say that $\langle X \mid R \rangle$ is a presentation of a group G if $G \cong F(X)/\langle R \rangle^{F(X)}$. We say that X is the set of generators and R is the set of relators.

Convention: we will often interpret the relators as relations, i.e. $aba^{-1}b^{-1}$ can be interpreted as $ab = ba$.

Group Presentation

Definition

Let X be a set and let $R \subseteq (X \cup X^{-1})^*$ be a set of words over X (and inverses). We say that $\langle X \mid R \rangle$ is a presentation of a group G if $G \cong F(X)/\langle R \rangle^{F(X)}$. We say that X is the set of generators and R is the set of relators.

Convention: we will often interpret the relators as relations, i.e. $aba^{-1}b^{-1}$ can be interpreted as $ab = ba$.

Example

- $\langle a, b \mid ab = ba \rangle$,
- $\langle c_1, \ldots, c_n \mid c_i^2 = c_{i+1}$ for $i = 1, \ldots, n-1, c_n^2 = 1 \rangle$,
- $\langle a, t \mid t^2 = 1, tat = a^{-1} \rangle$,
- $\langle a, b, c \mid bab^{-1} = a^2, cbc^{-1} = b^2, aca^{-1} = c^2 \rangle$.

Which one of these is trivial?

Unsovable!

Theorem (Adian-Rabin)

The problem of deciding whether or not a finite presentation represents the trivial group is not recursive.

Unsovable!

Theorem (Adian-Rabin)

The problem of deciding whether or not a finite presentation represents the trivial group is not recursive.

Corollary

The isomorphism problem for finitely presented groups is not recursive.

Unsovable!

Theorem (Adian-Rabin)

The problem of deciding whether or not a finite presentation represents the trivial group is not recursive.

Corollary

The isomorphism problem for finitely presented groups is not recursive.

In general, the isomorphism problem not known to be solvable for many classes of groups. It is known to be recursive for *hyperbolic groups* but it is not known to be primitively recursive. It is known to be primitively recursive for *finitely generated virtually free groups* but no explicit bound on the complexity (space or time) is known.

Virtually-free groups

Definition

We say that a group G is virtually free if G contains a subgroup F such that F is free and $|G : F| < \infty$.

Virtually-free groups

Definition

We say that a group G is virtually free if G contains a subgroup F such that F is free and $|G : F| < \infty$.

There are many equivalent characterisations of virtually free group. For a finitely generated group G the following (and many more) are equivalent:

- G is virtually free,
- the word problem in G is context free,
- Cayley graph of G is quasi-isometric to a tree,
- G acts properly discontinuously cocompactly on a graph of finite tree width,
- G splits as *finite graph of finite groups*.

Free constructions in groups

There are two main types of "free" group-theoretic constructions: amalgams and HNN-extensions.

A *graph of groups* is a generalisation of both.

Free constructions in groups

There are two main types of "free" group-theoretic constructions: amalgams and HNN-extensions.

- Suppose $A \leq G_1$ and also $A \leq G_2$. The *amalgam* of G_1 and G_2 along A, denote $G_1 *_A G_2$, is the smallest group with an universal property containing both the factors in a compatible way – pushout.

A *graph of groups* is a generalisation of both.

Free constructions in groups

There are two main types of "free" group-theoretic constructions: amalgams and HNN-extensions.

- Suppose $A \leq G_1$ and also $A \leq G_2$. The *amalgam* of G_1 and G_2 along A, denote $G_1 *_A G_2$, is the smallest group with an universal property containing both the factors in a compatible way – pushout.
- Suppose $K_1, K_2 \leq H$ and that $K_1 \cong K_2$ via a map ϕ. Then a *HNN-extension* of H along ϕ, denote $H*_\phi$, is the smallest group in which ϕ can be realised as conjugation by an element of infinite order outside of H.

A *graph of groups* is a generalisation of both.

Graphs of groups

Graph of groups consist of the following data:

1. a graph Γ
2. collection of vertex groups $(G_v)_{v \in V\Gamma}$,
3. collection of edge groups $(G_e)_{e \in E\Gamma}$,
4. and boundary monomorphisms $\alpha_e \colon G_e \to G_{\alpha(e)}$ and $\omega_e \colon G_e \to G_{\omega(e)}$ for every $e \in E\Gamma$.

Graphs of groups

Graph of groups consist of the following data:

1. a graph Γ
2. collection of vertex groups $(G_v)_{v \in V\Gamma}$,
3. collection of edge groups $(G_e)_{e \in E\Gamma}$,
4. and boundary monomorphisms $\alpha_e \colon G_e \to G_{\alpha(e)}$ and $\omega_e \colon G_e \to G_{\omega(e)}$ for every $e \in E\Gamma$.

Most solutions for isomorphism problem decompose given groups into graphs of groups in a specific way. These decompositions are unique up to an equivalence. However, finding such decompositions in general is not primitively recursive.

Effective decompositions

Theorem (MF-Elder-Logan)

Let G be a finitely generated virtually free group and let $C \in \mathbb{N}$ such that $|Q| < C$ for every $Q \in G$ with $|Q| < \infty$. Furthermore, suppose that for some decomposition as a graph of finite groups the underlying graph does not contain a loop. Then an explicit bound on the space complexity of an algorithm can be given.

Effective decompositions

Theorem (MF-Elder-Logan)

Let G be a finitely generated virtually free group and let $C \in \mathbb{N}$ such that $|Q| < C$ for every $Q \in G$ with $|Q| < \infty$. Furthermore, suppose that for some decomposition as a graph of finite groups the underlying graph does not contain a loop. Then an explicit bound on the space complexity of an algorithm can be given.

Proof.

Use the fact that G is δ-hyperbolic with $\delta \leq C$:

- find all maximal finite subgroups in a $(2\delta + 1)$-ball in the Cayley graph,
- find unique representants of conjugacy classes,
- find conjugates with maximal intersections,
- in a systematic manner, build a graph.

□

Effective isomorphism problem

Theorem (MF-Elder-Logan)

Let G_1, G_2 be as before. Then there is an explicit bound on the amount of space needed to decide whether $G_1 \cong G_2$.

Effective isomorphism problem

Theorem (MF-Elder-Logan)

Let G_1, G_2 be as before. Then there is an explicit bound on the amount of space needed to decide whether $G_1 \cong G_2$.

Proof.

Perform a brute-force method:

- use previous theorem to find the decompositions,
- list all equivalent decompositions,
- compare pairwise.

□

Each step can be realised by a computation whose space complexity can be bound by an explicit function of C and the size of the presentation.

THANK YOU!