Algorithmic problems in solvable groups, Part 2

Olga Kharlampovich
(McGill University)

Les Diableteres, 2010

Markov properties

The existence of a semigroup and a group with undecidable word problem allowed one to prove the undecidability of many properties of finitely presented semigroups and groups.

Here are some examples of those properties: finiteness, triviality, commutativity and so on. All these properties and many others satisfy the following condition: They hold in some finitely presented algebra G_1 and do not hold in any algebra containing some finitely presented algebra G_2 (G_1 and G_2 may be different for different properties).

Such properties have been called Markov properties after A.A.Markov proved the undecidability of each of them for finitely presented semigroups. In the class of groups, the undecidability of an arbitrary Markov property has been proved by Adian and Rabin . Similar results have been obtained for associative and Lie algebras by L.A.Bokut' .

Isomorphism problem

A program of the Minsky machine, can be chosen in such a way that the group with unsolvable word problem will be Hopfian. Hence the following result is true.

Theorem All varieties of solvable groups with undecidable (resp. strongly undecidable) word problem enumerated in the previous talk have undecidable (resp. strongly undecidable) isomorphism problem.

Proof $G/ << g >>$ is isomorphic to G iff $g = 1$ in G.

Isomorphism problem

The isomorphism problem for finitely generated nilpotent groups has been solved in the positive by Grunevald and Segal.

Theorem(Segal, 83)
There exists an algorithm deciding for given two finite presentations of polycyclic-by-finite groups if these groups are isomorphic and if so giving an explicit isomorphism.

To prove the solvability of the isomorphism problem for polyciclic-by-finite groups we first of all reduce this problem to the analogous problem for torsion free polycyclic-by-finite groups.

Isomorphism problem

The isomorphism problem for finitely generated nilpotent groups has been solved in the positive by Grunevald and Segal.
Theorem(Segal, 83)
There exists an algorithm deciding for given two finite presentations of polycyclic-by-finite groups if these groups are isomorphic and if so giving an explicit isomorphism.

To prove the solvability of the isomorphism problem for polyciclic-by-finite groups we first of all reduce this problem to the analogous problem for torsion free polycyclic-by-finite groups.

Isomorphism problem

For any two finitely generated torsion-free polyciclic-by-finite groups G_1 and G_2, one can find numbers n_1 and n_2 that satisfy the following two properties:

1. the semidirect product of G_i and $Aut(G_i)$, where $i = 1, 2$ is effectively embeddable into the group of invertible integer matrices of order n_i, $GL_{n_i}(\mathbf{Z})$, (we denote this embedding by β_{G_i}). Here "effectively embeddable" means that we can compute the image of each generator of G_i
2. Groups G_1 and G_2 are isomorphic if and only if $n_1 = n_2 = n$ and there exists an integer matrix $A \in GL_n(\mathbf{Z})$ such that $A^{-1}\beta_G A = \beta_H$.

Isomorphism problem

Now we can consider the set of all polycyclic-by-finite subgroups of the group $GL_n(\mathbf{Z})$ for some n. The group $GL_n(\mathbf{Z})$ acts on this set by conjugations. Our goal is to check if two subgroups belong to the same orbit of this action.

An important feature of the papers of Grunewald and Segal is a (partial) reduction of this problem to the problem of whether two vectors of a vector space with an action of $GL_n(\mathbf{Z})$ are in the same orbit of this action.
This shows that one has to consider actions of the group $GL_n(\mathbf{Z})$ on vector spaces. Groups $GL_n(\mathbf{Z})$ belong to the class of the so called arithmetic groups.
There exists a deep theory of actions of arithmetic groups (see, Borel, Harish-Chandra). The first problem was to make this theory "effective", that is to find algorithms where only existence theorems were known. A solution of this problem was an important achievement of Grunewald and Segal.

Isomorphism problem

Using these algorithms they proved that if an action of an arithmetic group on a vector space is in some natural sense explicitly given then it is algorithmically decidable whether two elements are in the same orbit.

This result has many applications to different algorithmic problems not only in algebra but also in number theory. We have mentioned some of the applications to the isomorphism problem. In particular this result allowed Grunewald and Segal to complete the solution of the isomorphism problem for nilpotent and then for polycyclic-by-finite groups.

Isomorphism problem

It is worth mentioning that the solvability of the problem of isomorphism to a fixed finitely presented nilpotent group G has been proved earlier by Pickel, 71.
Recall that two universal algebras are called quasi-isomorphic if they have the same finite homomorphic images. Pickel proved that the set non-isomorphic finitely generated nilpotent groups which are quasi-isomorphic to a fixed group G is finite. Later Grunewald, Pickel and Segal extended this result to arbitrary polycyclic-by-finite groups.

Isomorphism problem

By a result of Groves, 71, every finitely generated group in a variety is polycyclic-by-finite if and only if this variety does not contain varieties $\mathcal{A}_p\mathcal{A}$ for all prime p.
Thus varieties $\mathcal{A}_p\mathcal{A}$ are smallest varieties which are not covered by Segal's theorem. Unfortunately even for these varieties the solvability of the isomorphism problem is not known.
Problem Is the isomorphism problem decidable in the following varieties:

a) $\mathcal{A}_p\mathcal{A}$, where p is prime;

b) $\mathcal{A}\mathcal{A}$ (the variety of metabelian groups);

c) $\mathcal{N}_2\mathcal{A}$?

It is quite possible that the answers in cases a), b), c) are different.

Isomorphism problem

The problem of isomorphism to a fixed group G in these varieties is also hard and the answers are not known. Groves and Miller III, 86 showed that it is decidable whether a finitely presented metabelian group is a free metabelian group. Thus the problem of isomorphism to a free metabelian group is decidable in $\mathcal{A}^2$. Noskov proved that this result can be obtained by a Pickel-type argument: for every finitely generated free metabelian group G there are only finitely many finitely generated metabelian groups which are quasi-isomorphic but not isomorphic to G. Pickel constructed an example infinitely many non-isomorphic but quasi-isomorphic finitely generated metabelian groups.

Isomorphism problem

Problem Describe varieties of solvable groups in which every set of quasi-isomorphic finitely generated groups is finite. Does the variety $\mathcal{A}_p\mathcal{A}$ satisfy this property for some p?
Notice that if the answer to the second half of this problem is negative then the first part has an easy solution:
nilpotent-by-locally finite varieties. This follows from a result of Groves mentioned above.

Isomorphism problem

The general isomorphism problem for metabelian groups is actually a commutative algebra problem.
These connection are based on the fact that the first derived subgroup G' of any metabelian group G is a module over the commutative ring $\mathbf{Z}(G/G')$. If G is finitely generated then the ring and the module are finitely generated. This follows from the result of P.Hall that every normal subgroup in a finitely generated metabelian group is finitely generated as a normal subgroup (Hall54). If two metabelian groups are isomorphic then these rings must be isomorphic and the modules must be isomorphic also.
The isomorphism problems for finitely generated commutative rings and for finitely generated modules over finitely generated commutative rings are very hard and the answers are unknown.

Isomorphism problem

Theorem (Baumslag, Cannonito, Miller III, 81) There is an algorithm which, given a finite presentation of a group in the variety $\mathcal{A}^n$, decides if the group is polycyclic, and if so, produces the polyciclic presentation of this group.

Corollary The following properties of a group finitely presented in the variety $\mathcal{A}^n$ are effectively recognizable: polycyclic; nilpotent; Abelian; finite; cyclic; trivial.

Metabelian groups

Theorem (Baumslag, Cannonito, Miller III, 92) Let G be a relatively finitely presented metabelian group. There is an algorithm which finds a finite presentation of the $Z(G/G')$-module G'. Hence there is an algorithm which finds the centre $Z(G)$, and also a finite presentation of $Z(G)$. There is also an algorithm which finds (a finite subset whose normal closure is) the Fitting subgroup $Fit(G)$.

Corollary Let G be a relatively finitely presented metabelian group. Then there exist algorithms which can:

decide if G is torsion-free;

decide if a given element of G has finite order;

enumerate all possible orders of elements in G;

to find the limit of the lower central series of G;

to decide if a finitely presented metabelian group is residually nilpotent;

to find the Frattini subgroup of G.

Isomorphism problem

The isomorphism problem is solvable for
Torsion free non-splittable hyperbolic groups (Sela),
Limit (or f.g. fully residually free) groups (Bumagin, Kharlampovich, Myasnikov)
Torsion free relatively hyperbolic groups with abelian parabolics (Dahmani, Groves)
Hyperbolic groups (Dahmani will talk about)

Magnus embedding

For a free group $F = F(X)$ of rank r denote by $F^{(1)} = F' = [F, F]$ the *derived* subgroup of F, and by $F^{(d)} = [F^{(d-1)}, F^{(d-1)}]$ – the *d-th derived subgroup* of F, $d \geq 2$. The quotient group $A_r = F_r/F_r'$ is a *free abelian group* of rank r, $M_r = F_r/F_r^{(2)}$ is a *free metabelian group* of rank r, and $S_{r,d} = F_r/F_r^{(d)}$ is a *free solvable group* of rank r and class d. In the sequel we usually identify the set X with its canonical images in A_r, M_r and $S_{r,d}$.

Magnus embedding

One of the most powerful approaches to study free solvable groups is via the Magnus embedding. To explain we need to introduce some notation. Let $G = F/N$ and $\mathbb{Z}G$ the group ring of G with integer coefficients. By $\mu : F \to G$ we denote the canonical factorization epimorphism, as well its linear extension to $\mu : \mathbb{Z}F \to \mathbb{Z}G$. Let T be a free (left) $\mathbb{Z}G$-module of rank r with a basis $\{t_1, \ldots, t_r\}$. Then the set of matrices

$$M(G) = \begin{pmatrix} G & T \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} g & t \\ 0 & 1 \end{pmatrix} \mid g \in G, t \in T \right\}$$

forms a group with respect to the matrix multiplication. It is easy to see that the group $M(G)$ is a discrete wreath product $M(G) = A_r wr G$ of the free abelian group A_r and the group G.

Magnus embedding

Theorem (Magnus:1939) The homomorphism $\phi : F \to M(G)$ defined by

$$x_i \overset{\phi}{\mapsto} \begin{pmatrix} x_i^{\mu} & t_i \\ 0 & 1 \end{pmatrix}, \quad i = 1, \ldots, r,$$

satisfies $\ker \phi = N'$. Therefore, ϕ induces a monomorphism

$$\phi : F/N' \hookrightarrow M(F/N).$$

Magnus embedding

The monomorphism ϕ is now called the *Magnus embedding*. The Magnus embedding allows one to solve WP in the group F/N' if WP in $G = F/N$ is decidable. Indeed, observe that

$$x_i^{-1} \overset{\phi}{\mapsto} \begin{pmatrix} (x_i^{-1})^{\mu} & (-x_i^{-1})^{\mu} t_i \\ 0 & 1 \end{pmatrix}, \quad i = 1, \ldots, r.$$

Now, if for $i = 1, \ldots, r$ and $\varepsilon = \pm 1$ we define the value

$$\delta(x_i^{\varepsilon}) = \begin{cases} 1, & \text{if } \varepsilon = 1; \\ (-x_i^{-1})^{\mu}, & \text{if } \varepsilon = -1; \end{cases}$$

Magnus embedding

then given a word $w = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n} \in F(X)$ one can compute its image $\phi(w)$ in $M(G)$ as follows

$$\phi(w) = \phi(x_{i_1}^{\varepsilon_1}) \dots \phi(x_{i_n}^{\varepsilon_n})$$

$$= \begin{pmatrix} \mu(x_{i_1}^{\varepsilon_1}) & \delta(x_{i_1}^{\varepsilon_1}) t_{i_1} \\ 0 & 1 \end{pmatrix} \cdot \dots \cdot \begin{pmatrix} \mu(x_{i_n}^{\varepsilon_n}) & \delta(x_{i_n}^{\varepsilon_n}) t_{i_n} \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \mu(x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}) & \sum_{j=1}^{n} (x_{i_1}^{\varepsilon_1} \dots x_{i_{j-1}}^{\varepsilon_{j-1}})^{\mu} \delta(x_{i_j}^{\varepsilon_j}) t_{i_j} \\ 0 & 1 \end{pmatrix}$$

and then, using a decision algorithm for WP in G, check if the resulting matrix $\phi(w)$ is the identity matrix or not.

Magnus embedding

To estimate the complexity of such an algorithm notice first, that the coefficients from $\mathbb{Z}G$ that occur in the upper-right corner of the matrix $\phi(w)$ have $O(|w|)$ summands. Secondly, to check whether or not an element $h = m_1 v_1 + \ldots + m_k v_k \in \mathbb{Z}G$, where $m_i \in$ and $v_i \in G$ are given as words in the generators X from G, is trivial in $\mathbb{Z}G$ it requires $O(k^2)$ comparisons of the type $v_i = v_j$? in G. This gives an estimate for the time function T' of WP in F/N' via the time function T for WP in F/N:

$$T'(n) = O(rn^2 T(n)),$$

where $n = |w|$. Since WP in A_r can be decided in linear time the estimate above shows that the complexity of WP in M_r is $O(rn^3)$. Moreover, induction on the solvability class d gives a polynomial estimate $O(r^{d-1} n^{2d-1})$ for WP in the free solvable group $S_{r,d}$. Thus, the Magnus embedding gives a straightforward polynomial time (in r and n) decision algorithm for *WP* in $S_{r,d}$, but the degree of the polynomial grows with d. In particular, this algorithm is not polynomial as a uniform algorithm on the whole class of free