Algorithmic problems in solvable groups

Olga Kharlampovich
(McGill University)

Les Diableteres, 2010

Group identities

Reference "Algorithmic problems in varieties", Kharlampovich, Sapir, IJAC, 4&5, (1995), 379-602.

Definition A variety of groups is a class of groups satisfying an identity (a law).

Ex. $\mathcal{N}_c$ a variety of all nilpotent groups of degree $\leq c$. They satisfy the identity

$$(x_1, x_2, \ldots, x_{c+1}) = 1,$$

where $(x_1, x_2) = x_1^{-1} x_2^{-1} x_1 x_2$.

$\mathcal{A}^n$ a variety of $\leq n$ solvable groups, in particular, $\mathcal{A}$ abelian groups, $\mathcal{A}^2$ metabelian groups.

$Z\mathcal{A}^2$ central-metabelian groups

$$(((x_1, x_2), (x_3, x_4)), x_5) = 1.$$

We will talk about finitely presented groups from a variety and relatively finitely presented groups (finite number of relations plus the identity).

Solvable groups

The solvable groups are interesting as far as few things are known on their behavior up to quasi-isometry.

For polycyclic groups this is still an open question.

In the case of nilpotent groups there is much more information.

First, a consequence of Gromov's theorem on polynomial growth is that virtual nilpotency is a geometric property in the class of groups (we recall that a group is called virtually nilpotent if it has a nilpotent subgroup of finite index). In nilpotent groups, the filling order is at most polynomial of degree $c + 1$, where c is the class of the group, and it is exactly polynomial of degree $c + 1$ if the group is free nilpotent.

Solvable groups

In the Heisenberg group H^3 it was shown by Thurston that the filling order is cubic (which implies that H^3 is not automatic). Gromov gave an outline of proof that the other Heisenberg groups H^{2n+1} have quadratic filling order and Allcock gave the complete proof by means of symplectic geometry. Olshanskii and Sapir later gave a combinatorial proof.

Solvable groups

The property of being virtually solvable is not a geometric property (Ershler). On the other hand, certain solvable groups are very rigid with respect to quasi-isometry (Solvable Baumslag-Solitar groups (Farb, Mosher)). Thurston has shown that the group Sol has exp. filling order (so it is not automatic). Gersten: $BS(1;p)$ has exp. filling order. Gromov showed that the semidirect product of R^n and $R^{n-1}, n \geq 3$, has quadratic filling order. Arzhantseva and Osin constructed a sequence of discrete nonpolycyclic solvable groups with filling orders that are at most cubic. Drutu studied the filling order for Lie solvable groups. The discrete groups she studied are all polycyclic.

Word problem

There are two classes of solvable group varieties where the solvability of the word problem is well known: the varieties of nilpotent groups and the varieties of metabelian groups.
All nilpotent and metabelian varieties of groups are finitely based. Every finitely generated nilpotent groups is finitely presented, representable by matrices over Z and residually finite. This implies the solvability of the word problem in nilpotent varieties. The word problem in a nilpotent group is solvable in polynomial time.
Finitely generated groups in the variety $\mathcal{A}^2$ are finitely presented in this variety and residually finite, hence have solvable word problem (Ph. Hall). The word problem is solvable in polynomial time because such groups are matrix groups.

Word problem

There are two classes of solvable group varieties where the solvability of the word problem is well known: the varieties of nilpotent groups and the varieties of metabelian groups.
All nilpotent and metabelian varieties of groups are finitely based.
Every finitely generated nilpotent groups is finitely presented, representable by matrices over Z and residually finite. This implies the solvability of the word problem in nilpotent varieties. The word problem in a nilpotent group is solvable in polynomial time.
Finitely generated groups in the variety $\mathcal{A}^2$ are finitely presented in this variety and residually finite, hence have solvable word problem (Ph. Hall). The word problem is solvable in polynomial time because such groups are matrix groups.

Word problem

1. Determine whether or not the WP is solvable for groups, relatively finitely presented in the variety $\mathcal{A}^n, n \geq 3$ (Mal'cev). There exists a group relatively f.p. in $\mathcal{A}^n, n \geq 5$ with unsolvable WP (Remeslennikov).
   In our terminology, the question is whether the WP is solvable in the varieties $\mathcal{A}^n$.
2. Construct a finitely presented group, satisfying a nontrivial identity, with unsolvable WP (Adian, 74). Constructed by Kharlampovich, the group belonged to $\mathcal{A}^3 \cup Z\mathcal{N}_3\mathcal{A}$. Then Baumslag, Gildenhuys and Strebel presented this construction in terms of matrix groups and repeated it for Lie algebras.
3. Determine whether or not every recursively presented group in the variety $\mathcal{A}^n$ is embeddable in a relatively finitely presented group in the variety $\mathcal{A}^m$, for some m (Remeslennikov).

Word problem

Theorem(Kharlampovich, 88). The variety $Z\mathcal{N}_2\mathcal{A}$ has a strongly undecidable word problem (there exists a f.p. group with unsolvable word problem that belongs to this variety).
This variety is given by the identity

$$((((x_1, x_2), (x_3, x_4)), (x_5, x_6)), x_7) = 1.$$

Theorem (Kh, 87) In any subvariety of $\mathcal{N}_2\mathcal{A}$ the WP is solvable.
Theorem (Bieri and Strebel, 80) Every (absolutely) finitely presented group that belongs to $\mathcal{N}_2\mathcal{A}$ is residually finite.

Word problem

Theorem (Kh, 93) The varieties $Z\mathcal{N}_2\mathcal{A} \cap \mathcal{B}_p\mathcal{A}$, ($p \geq 5$, prime) are minimal varieties with unsolvable word problem.
Theorem (Sapir, 92) The varieties $\mathcal{A}_p\mathcal{A}_q\mathcal{A}$ (p, q, are distinct primes) are minimal varieties with unsolvable word problem.

Theorem (Kh) The word problem is solvable in the varieties $\mathcal{N}_2\mathcal{N}_c \cap Z\mathcal{N}_2\mathcal{A}$.

Let $\mathcal{Y}_c$ be a variety defined in $Z\mathcal{N}_2\mathcal{A}$ by the identity $((x_1, \ldots, x_{c+2}), (y_1, \ldots, y_{c+2}), (z_1, \ldots, z_c)) = 1$.

Theorem (Kh) The WP is unsolvable in the varieties $\mathcal{Y}_c$ for any $c \geq 1$.

Notice that, $\mathcal{Y}_{c-1} \subset \mathcal{N}_2\mathcal{N}_c \cap Z\mathcal{N}_2\mathcal{A} \subset \mathcal{Y}_{c+1}$.

Minsky Machines

The hardware of a (two-tape) Minsky machine consists of two tapes and a head. The tapes are infinite to the right and are divided into infinitely many cells numbered from the left to the right, starting with 0. The first cells on both tapes always contain 1, all other cells have 0. The head may acquire one of several internal states: $q_0, \ldots, q_N$; q_0 is called *the terminal state*. At every moment the head looks at one cell of the first tape and at one cell of the second tape. So the *configuration* of the Minsky machine may be described by the triple (m, q_k, n) where m (resp. n) is the number of the cell observed by the head on the first (resp. second) tape, q_i is the state of the head.

Every command has the following form:

$$q_i, \epsilon, \delta \longrightarrow q_j, T^{\alpha}, T^{\beta}.$$

where $\epsilon, \delta \in \{0, 1\}, \alpha, \beta \in \{-1, 0, 1\}$.

The machine always starts working at state q_1 and ends at the *terminal state* q_0.

Minsky Machines

The program (software) for a Minsky machine is a set of commands of the above form.
One says that a Minsky machine *calculates* a function $f(m)$ if for every m starting at the configuration $(m, q_1, 0)$ it ends at the configuration $(f(m), q_0, 0)$. If m does not belong to the domain of f then the machine works forever and never gets to the terminal state.

Theorem For every partially recursive function $f(m)$ there exists a Minsky machine which calculates the partial function $g_f : 2^m \longrightarrow 2^{f(m)}$.

High school definition

Consider two glasses. We assume that these glasses are of infinite height. Another (more restrictive!) assumption is that we have infinitely many coins. There are four *operations*: “Put a coin in a glass”, “Take a coin from a glass if it is not empty”. We are able to check if a glass is/isn’t empty. A *program* is a numbered sequence of instructions.

An *instruction* has one of the following forms:

- Put a coin in the glass # n and go to instruction # j;
- If the glass # n is not empty then take a coin from this glass and go to instruction # j otherwise go to instruction # k.
- Stop.

A program starts working with the command number 1 and ends when it comes to the Stop instruction which will always have number 0. We say that a program calculates a function $f(m)$ if, starting with m coins in the first glass and empty second glass, we end up with $f(m)$ coins in the first glass and empty second glass.

Semigroups

A configuration of a Minsky algorithm is a triple (m, k, n), where m is the number of coins in the first glass, n is the number of coins in the second glass, and k is the number of the instruction we are executing. So the number of an instruction in the algorithm plays the role of an inner state!

Semigroups

There are two important semigroup interpretations of Minsky machines: the semigroups S_1 and S_2 below. Let M be a Minsky machine with internal states $q_0, \dots, q_N$. Then both S_1 and S_2 are generated by the elements $q_0, \dots, q_N$ and a, b, A, B. The correspondences between commands of M and relations of S_1 and S_2 are given by the following tables. Every command corresponds to one relation in S_1 and one relation in S_2.

Semigroups

Command	S_1
$q_i, 0, 0 \rightarrow q_j,\ T^\alpha,\ T^\beta$	$aq_ib = a^{1+\alpha}q_jb^{1+\beta}$
$q_i, 1, 0 \rightarrow q_j,\ T^\alpha,\ T^\beta$	$Aq_ib = Aa^\alpha q_jb^{1+\beta}$
$q_i, 0, 1 \rightarrow q_j,\ T^\alpha,\ T^\beta$	$aq_iB = a^{1+\alpha}q_jb^\beta B$
$q_i, 1, 1 \rightarrow q_j,\ T^\alpha,\ T^\beta$	$Aq_iB = Aa^\alpha q_jb^\beta B$

(1)

Semigroups

Command	S_2
$q_i, 0, 0 \to q_j,\ T^\alpha,\ T^\beta$	$q_i ab = q_j a^{1+\alpha} b^{1+\beta}$
$q_i, 1, 0 \to q_j,\ T^\alpha,\ T^\beta$	$q_i Ab = q_j a^\alpha A b^{1+\beta}$
$q_i, 0, 1 \to q_j,\ T^\alpha,\ T^\beta$	$q_i aB = q_j a^{1+\alpha} b^\beta B$
$q_i, 1, 1 \to q_j,\ T^\alpha,\ T^\beta$	$q_i AB = q_j a^\alpha A b^\beta B$

(2)

Semigroups

The canonical words in S_i are the following:

Configuration	S_1	S_2
(m, q_k, n)	$Aa^m q_k b^n B$	$q_k a^m A b^n B$

(3)

To make these interpretations work and to make these semigroups satisfy as many identities as possible we need also some additional relations independent of the commands of M.
In the semigroup S_2 we need the following commutativity relations:

$$ab = ba, \ aB = Ba, \ bA = Ab, \ AB = BA. \qquad (4)$$

Also we need all relations of the type

$$xy = 0$$

where xy is a two letter word which is not a subword of $w(m, q_k, n)$ for some m, n or of any word obtained from $w(m, q_k, n)$ by the commutativity relations above.

Semigroups

Thus we have the following additional relations in S_1: all two letter words are equal to 0 except Aa, Aq_i, a^2, aq_i, q_ib, q_iB, b^2, bB.
And we have the following additional relations in S_2: all two letter words are equal to 0 except q_ia, q_ib, q_iA, q_iB, a^2, aA, ab, aB, ba, b^2, bB, bA, Ab, AB, Ba, BA.

Lemma 1 If we pass from the configuration $\psi = (m, q_k, n)$ to another configuration $\psi_1 = (m', q_{k'}, n')$ by a command κ then we pass from the word $w(m, q_k, n)$ to the word $w(m', q_{k'}, n')$ by the relation corresponding to κ.

Let us prove this only for the case of the semigroup S_2 and the command $\kappa : q_k, 1, 0 \to q_{k'}, T^\alpha, T^\beta$. All other cases are similar. Since the command κ is applicable to the configuration (m, q_k, n), in this configuration, the head observes the first cell on the first tape and not the first cell on the second tape. Thus $m = 0,\ n \neq 0$. Then $m' = \alpha,\ n' = n + \beta$ (in this case α can not be negative). Now $w(m, q_k, n) = q_k b^n AB$ and the relation corresponding to κ is $q_k bA = q_{k'} a^\alpha b^{1+\beta} A$. Since $AB = BA$ and $aB = Ba$ we have $w(m, q_k, n) = q_k b^n AB = q_k bAb^{n-1}B$. Thus we can apply our relation and replace $q_i bA$ by $q_{k'} a^\alpha b^{1+\beta} A$. As a result we obtain the word $q_{k'} a^\alpha b^{1+\beta} Bb^{n-1} A$ which is equal to $q_{k'} a^\alpha Ab^{n+\beta} B$ since $bA = Ab$. The last word is equal to $w(m', q_{k'}, n')$ as desired.

Semigroups

Lemma 2 If we can proceed from the word $w(\psi_1)$ to the word $w(\psi_2)$ by using relations, then M transforms ψ_1 amd ψ_2 into the same configuration.

1. For every canonical word $w(m, q_k, n)$ there exists at most one relation corresponding to a command of M which is applicable to this word from the left to the right (this means that one replaces the left hand side of this relation by the right hand side of it).

2. Any application of a relation from tables (1) or (2) to any canonical word — from the left to the right or from the right to the left — gives us another canonical word (we do not distinguish words in S_2 which are obtained from each other by the commutativity relations)

Groups

We begin with the group G generated by the elements $q_0, \ldots, q_N, a, b, A, B$, with defining relations

$$(a, b) \ = \ (a, B) \ = \ (A, b) \ = \ (A, B) \ = \ 1,$$

where (x, y) denotes the commutator $x^{-1}y^{-1}xy$, and relations given by the second table where the product is replaced by the commutator. The canonical words are also similar
(We have agreed to read the commutator (x, y, z) as $((x, y), z)$ and $(x, y^{(n)})$ as $(x, y, \ldots, y)$.):

$$w(m, q_k, n) = (q_k, a^{(m)}, b^{(n)}, A, B).$$

Now, to prove Lemma 1 we need to be able to permute adjacent letters, say, A and B in any canonical word, regardless of the place where these letters occur.

Groups

So we have to construct a finite family of relations which would imply all the desired permutations. We would succeed if we could find finitely many relations which make the normal subgroup generated by all the q's Abelian. Indeed, then we could consider this normal subgroup as a module over the group ring of the group generated by $\{a, b, A, B\}$. Now if x belongs to this normal Abelian subgroup then the commutator (x, u, v) will correspond to the element $x^{(u-1)(v-1)}$ of this module. And, the equality $(u, v) = 1$ implies $(u-1)(v-1) = (v-1)(u-1)$ and so $x^{(u-1)(v-1)} = x^{(v-1)(u-1)}$.

Groups

Lemma BR$_G$. *Suppose that a group G is generated by three sets $X, K = \{a_i \mid i = 1, \ldots, m\}, K' = \{a_i' \mid i = 1, \ldots, m\}$ such that*
(1) The subgroup generated by $K \cup K'$ is Abelian;
(2) For every $a \in K$ and every $x \in X$ we have $x^{f(a)} = x^{a'}$ (for some monic polynomial f of a which has at least two terms;);
(3) $(x_1^{a_1^{\alpha_1} \ldots a_m^{\alpha_m}}, x_2) = 1$, for every $x_1, x_2 \in X$, and every $\alpha_1, \ldots, \alpha_m \in \{0, 1, -1\}$.
Then the normal subgroup generated by X in the subgroup $< X \cup K \cup K' >$ is Abelian and G is metabelian.
If the elements a_i and a_i' and the set X satisfy this Lemma we will call a_i' a BR-conjoint to a_i with respect to X.

Groups

we add new generators $\{d,\ a',\ b',\ \tilde{a},\ \tilde{b},\ \tilde{a}',\ \tilde{b}'\}$ and the relations saying that a' is a BR-conjoint to a with respect to the set of q's and with respect to A; b' is a BR-conjoint to b with respect to the set of q's and with respect to B; $\tilde{a}'$ is a BR-conjoint to $\tilde{a}$ with respect to the set $\{q, (q, A)\}$ and with respect to d; $\tilde{b}'$ is a BR-conjoint to $\tilde{b}$ with respect to the set $\{q, (q, B)\}$ and with respect to d

In addition to these relations we have to add other relations: $(q_i, a) = (q_i, \tilde{a})$, $(q_i, a') = (q_i, \tilde{a}')$, $(q_i, b) = (q_i, \tilde{b})$ and $(q_i, b') = (q_i, \tilde{b}')$. Also we add the relations: $(q_i, A, a) = 1$, $(q_i, A, a') = 1$, $(q_i, B, b) = 1$, $(q_i, B, b') = 1$ and $(q_i, A, A) = (q_i, A, q_j) = 1$, $(q_i, B, B) = (q_i, B, q_j) = 1, (q_i, q_j) = 1$. We add the corresponding relations for $d, \tilde{a}, \tilde{a}', \tilde{b}, \tilde{b}'$ too.

Now we are able to prove that that the normal subgroup generated by $q_0, q_1, \ldots, q_n$ is abelian and to prove Lemma 1.

To prove Lemma 2 we construct a homomorphic image of the group G. We will use a semidirect product. Let S_3 be the semigroup from the previous subsection.
Let us take the direct product T_2 of cyclic groups generated by the elements x_u where u runs over all non-zero elements of S_3. By definition let $x_0 = 1$. We want to define automorphisms corresponding to letters $A, B, d, a, b, a', b', \tilde{a}, \tilde{b}, \tilde{a}', \tilde{b}'$ of the group T_2 in such a way that the subgroup, generated by the set $\{x_u, u \in S_3, A, B, d, a, b, a', b', \tilde{a}, \tilde{b}, \tilde{a}', \tilde{b}'\}$ in the semidirect product of T_2 and this group of automorphisms, becomes a homomorphic image of G.

Groups

There is not much freedom in defining these automorphisms. For every $v \in \{a,\ b,\ A,\ B,\ d\}$ we should have $(x_u, v) = x_{uv}$, i.e. $x_u^{-1} v^{-1} x_u v = x_{uv}$. From this we immediately deduce that x_u^v should be equal to $x_u x_{uv}$. So if we denote by ϕ_v the automorphism corresponding to v, we should have $\phi_v(x_u) = x_u x_{uv}$. We can similarly deduce the definitions of automorphisms corresponding to other letters.
But how to prove that these are actually automorphisms?

Groups

To choose a suitable operation we start the construction of G from the end. We first define $\hat{G}$, and then define G itself. Namely, we define automorphisms of a suitable direct product of cyclic groups, then find out which operation $*$ satisfies the property $q_u * v = q_{uv}$, and replace the commutator by this operation $*$.
Of course, we have to choose the automorphisms corresponding to letters in such a way that automorphisms corresponding to members of a BR-pair form a BR-pair themselves. Practically this means that if (u, v) is a BR-pair, and $x^{f(u)} = x^v$ (see condition 2 of Lemma BR_G), then we have to define an automorphism u and then only check that $f(v)$ is also an automorphism for some monic polynomial f of degree > 1 which has at least 2 terms.

Groups

The solution is the following (Kh90).
Instead of T_2 let us take T_3, a free Abelian group generated by the elements $x_{i,j,u}$ where u runs over all non-zero elements of S_3 and $i, j \in 1, 2, 3$. By definition let $x_{i,j,0} = 1$. We see that instead of one element x_u (for every u) we have now 9 "brothers" $x_{i,j,u}$.
Let us define the automorphisms. For simplicity we will denote automorphisms corresponding to letters a, a', b, b', A, B by the same letters.
Let us start with automorphisms a, a'. We have to define $x^{a}_{i,j,u}$ and $x^{a'}_{i,j,u}$ for every i, j, u. First suppose that u does not contain A. Then let

$$x^{a}_{i,j,u} = \begin{cases} x_{i,j,u}x_{i,j+1,u}x_{ij+2,u}x_{i,j,ua}, & \text{if } j = 1; \\ x_{i,j,u}x^{-1}_{i,j-1,u}, & \text{if } j = 2; \\ x_{i,j-2,u}, & \text{if } j = 3. \end{cases}$$

$$x^{a'}_{i,j,u} = x^{-1}_{i,j,u}x^{a}_{i,j,u}.$$

Groups

If u contains letter A, then let $x^{a}_{i,j,u} = x^{a'}_{i,j,u} = x_{i,j,u}$.

Groups

$$
\begin{aligned}
x_{1,3,u}^{a^{-1}} &= x_{1,2,u}^{-1} x_{1,3,u}^{-1} x_{1,3,ua}^{-1} \\
x_{1,2,u}^{a^{-1}} &= x_{1,2,u} x_{1,3,u}, \\
x_{1,1,a}^{a^{-1}} &= x_{1,3,u}.
\end{aligned}
$$

Automorphisms b, b' are defined similarly. Let u not contain B. Then

$$
x_{i,j,u}^{b} = \begin{cases} x_{i,j,u} x_{i+1,j,u} x_{i+2,j,u} x_{i,j,ub}, & \text{if } i = 1; \\ x_{i,j,u} x_{i-1,j,u}^{-1}, & \text{if } i = 2; \\ x x_{i-2,j,u}, & \text{if } i = 3. \end{cases}
$$

$$
x_{i,j,u}^{b'} = x_{i,j,u}^{-1} x_{i,j,u}^{b}.
$$

If u contains B, then $x_{i,j,u}^{b} = x_{i,j,u}^{b'} = x_{i,j,u}$.

Groups

If $w \in \{A, B, d\}$ then let $x^{w}_{i,j,u} = x_{i,j,u}x_{i,j,uw}$.

It is easy to see that a works with the second additional indexes (j), and b works with the first additional index (i). This, by the way, automatically makes the mappings a and b commute.
Now we can define a partial operation $*$. We know that for every $w \in \{a, b, A, B\}$ we should have

$$x_{1,1,u} * w = x_{1,1,uw}.$$

From this relation we can deduce the form of the operation $*$:
For every $f \in G$ let
$f * a = f^{-1}f^{a}f^{-a^{-1}}f^{(a')^{-1}}, f * b = f^{-1}f^{b}f^{-b^{-1}}f^{(b')^{-1}}$, for $z \in A, B$
let $f * z = (f, z)$.