The word problem*

Yves Lafont
Institut de Mathématiques de Luminy†
Université de la Méditerranée (Aix-Marseille 2) - CNRS

April 2, 2007

Using rewriting techniques, we get a quite simple proof of undecidability of the word problem for groups (*Novikov-Boone theorem*).

*Work partly supported by ANR project INVAL (*Invariants algébriques des systèmes informatiques*).
†163 avenue de Luminy, Case 907 - 13288 Marseille CEDEX 9 - France

1 Register machines

A (*deterministic*) *2-register machine* $\mathcal{R}$ is given by a sequence $r_1, \ldots, r_n$ where each r_i is an instruction of one of the following two forms:

- *increment* x (or *increment* y) *and go to* j (or *stop*);
- *if* $x = 0$ (or $y = 0$) *then go to* j (or *stop*) *else decrement it and go to* k (or *stop*).

For instance, the following machine performs multiplication by 2 (starting with $y = 0$):

1. *if* $x = 0$ *then stop else decrement it and go to* 2;
2. *increment* y *and go to* 3.
3. *increment* y *and go to* 1.

Exercise 1 *Build a 2-register machine for quotient and rest modulo 2.*

Exercise 2 *Prove that 3 registers can be simulated by 2 registers.*

Indication: Start with $2^x 3^y 5^z$ in the first register and 0 in the second one.

A *configuration* is a triple (i, x, y) where $i \in \{0, \ldots, n\}$ and $x, y \in \mathbb{N}$. Here, $i = 0$ means *stop*. Each instruction yields one or two *transitions* of the following kinds:

$$(i, x, y) \to_{\mathcal{R}} (j, x + 1, y), \qquad (i, x, y) \to_{\mathcal{R}} (j, x, y + 1),$$

$$(i, 0, y) \to_{\mathcal{R}} (j, 0, y), \qquad (i, x, 0) \to_{\mathcal{R}} (j, x, 0),$$

$$(i, x + 1, y) \to_{\mathcal{R}} (k, x, y), \qquad (i, x, y + 1) \to_{\mathcal{R}} (k, x, y).$$

In particular, our first example of machine corresponds to the following transitions:

$$(1, 0, y) \to_{\mathcal{R}} (0, 0, y), \qquad (1, x + 1, y) \to_{\mathcal{R}} (2, x, y),$$

$$(2, x, y) \to_{\mathcal{R}} (3, x, y + 1), \qquad (3, x, y) \to_{\mathcal{R}} (1, x, y + 1).$$

We introduce the preordering $\to_{\mathcal{R}}^*$ and the equivalence relation $\leftrightarrow_{\mathcal{R}}^*$ generated by $\to_{\mathcal{R}}$, and we consider the following problem:

Special halting problem: given (i, x, y), do we have $(i, x, y) \to_{\mathcal{R}}^* (0, 0, 0)$?

Exercise 3 *Prove that* $(i, x, y) \leftrightarrow_{\mathcal{R}}^* (0, 0, 0)$ *if and only if* $(i, x, y) \to_{\mathcal{R}}^* (0, 0, 0)$.

Indication: Use the fact that $\mathcal{R}$ is a deterministic machine.

Theorem 1 *The special halting problem is undecidable for some 2-register machine.*

Proof : Encode the halting problem for some *universal Turing machine*.

2 Some decision problems

If S, R is a finite presentation of a monoid M, we consider the following problems:

Unit: given $x \in S^*$, do we have $x \leftrightarrow_R^* 1$?

Equality: given $x, y \in S^*$, do we have $x \leftrightarrow_R^* y$?

Commutation: given $x, y \in S^*$, do we have $xy \leftrightarrow_R^* yx$?

Note that unit and commutation are special cases of the equality problem.

For any other finite presentation S', R' of M, we have a morphism $\varphi : S^* \to S'^*$ such that $x \leftrightarrow_R^* y$ if and only if $\varphi(x) \leftrightarrow_{R'}^* \varphi(y)$. Hence, the decidability of such a problem depends only on the monoid M.

Proposition 1 *The unit problem is undecidable for some finitely presented monoid.*

Hence, equality is undecidable for this monoid.

Proof: Given any 2-register machine $\mathcal{R}$, we introduce symbols $a, b, c_0, \ldots, c_n, d, e$, and we encode a configuration (i, x, y) by the word $[i, x, y] = ab^x c_i d^y e$. Each transition yields a rule of one of the following kinds:

$$c_i \to bc_j, \quad c_i \to c_j d, \quad ac_i \to ac_j, \quad c_i e \to c_j e, \quad bc_i \to c_k, \quad c_i d \to c_k d.$$

We add the rule $ac_0e \to 1$, and since $\mathcal{R}$ is deterministic, we get a finite orthogonal rewrite system S, R such that $(i, x, y) \to_{\mathcal{R}}^* (0, 0, 0)$ if and only if $[i, x, y] \to_R^* 1$. Furthermore, we have $u \to_R^* 1$ if and only if $u \leftrightarrow_R^* 1$ by the Church-Rosser property.

To sum up, the special halting problem for $\mathcal{R}$ reduces to the unit problem for S, R. Hence, we can apply theorem 1. □

In fact, we could also directly encode the halting problem for a Turing machine or for a *2-stack machine*. The proof would be essentially the same.

Exercise 4 *Prove that commutation is undecidable for some finitely presented monoid.*

Indication: Reduce the unit problem for M to the commutation problem for $M * \{a\}^*$.

For groups, the equality problem is equivalent to the unit problem, since we have $x = y$ if and only if $xy^{-1} = 1$. This is called the *word problem*.

Theorem 2 *The word problem is undecidable for some finitely presented group.*

The rest of this chapter is devoted to the proof of this nontrivial theorem. Indeed, the proof of proposition 1 cannot be easily extended to the case of groups, because inverses interfere with any naive encoding of machines.

3 Partial isomorphisms

We write $H < G$ if H is a subgroup of G. A *partial isomorphism* is an isomorphism $\varphi : H \to K$ where $H, K < G$. If H is finitely generated, we say that φ is *finitary*. More generally, a *partial bijection* is a bijection $\varphi : X \to Y$ where $X, Y \subset G$.

Exercise 5 *Prove that for any partial affine bijection $\varphi : u + H \to v + K$ in some additive group G, there is a partial isomorphism $\psi : \mathbb{Z}(1 + u) + H \to \mathbb{Z}(1 + v) + K$ in the additive group $\mathbb{Z} \oplus G$ such that $\psi(1 + x) = 1 + \varphi(x)$ whenever $x \in u + H$.*

If Φ is a set of partial bijections in G, we write $x \to_\Phi \varphi(x)$ whenever $x \in X$ for some $\varphi : X \to Y$ in Φ, and we introduce the equivalence relation $\leftrightarrow_\Phi^*$ generated by $\to_\Phi$. For any $x_0 \in G$, we consider the following problem:

Connection: given $x \in G$, do we have $x \leftrightarrow_\Phi^* x_0$?

Proposition 2 *The connection problem is undecidable for some finite set of finitary partial isomorphisms in some finitely presented group.*

Proof: We encode a configuration (i, x, y) for some 2-register machine $\mathcal{R}$ by the triple $[i, x, y] = (i, 2^x, 2^y)$ in the additive group $\mathbb{Z}^3$. Each transition yields a partial affine bijection of one of the following kinds:

$$\begin{array}{cc} \{i\} \times \mathbb{Z} \times \mathbb{Z} \to \{j\} \times 2\mathbb{Z} \times \mathbb{Z} & \{i\} \times \mathbb{Z} \times \mathbb{Z} \to \{j\} \times \mathbb{Z} \times 2\mathbb{Z} \\ (i, x, y) \mapsto (j, 2x, y) & (i, x, y) \mapsto (j, x, 2y) \\ & \\ \{i\} \times \{1\} \times \mathbb{Z} \to \{j\} \times \{1\} \times \mathbb{Z} & \{i\} \times \mathbb{Z} \times \{1\} \to \{j\} \times \mathbb{Z} \times \{1\} \\ (i, 1, y) \mapsto (j, 1, y) & (i, x, 1) \mapsto (j, x, 1) \\ & \\ \{i\} \times 2\mathbb{Z} \times \mathbb{Z} \to \{k\} \times \mathbb{Z} \times \mathbb{Z} & \{i\} \times \mathbb{Z} \times 2\mathbb{Z} \to \{k\} \times \mathbb{Z} \times \mathbb{Z} \\ (i, 2x, y) \mapsto (k, x, y) & (i, x, 2y) \mapsto (k, x, y) \end{array}$$

We get a finite set Φ of partial affine bijections which satisfies the following properties:

- $(i, x, y) \to_\mathcal{R} (i', x', y')$ if and only if $[i, x, y] \to_\Phi [i', x', y']$;
- if $u \to_\Phi u'$ and u is of the form $[i, x, y]$, then u' is of the form $[i', x', y']$;
- if $u \to_\Phi u'$ and u' is of the form $[i', x', y']$, then u is of the form $[i, x, y]$.

Hence, we have $(i, x, y) \leftrightarrow_\mathcal{R}^* (0, 0, 0)$ if and only if $[i, x, y] \leftrightarrow_\Phi^* [0, 0, 0]$. By exercise 3, the special halting problem for $\mathcal{R}$ reduces to the connection problem for Φ.

By exercise 5, we can replace Φ by a finite set of finitary partial isomorphisms in $\mathbb{Z}^4$. Finally, we can apply theorem 1. □

4 The Magnus problem

If S, R is a finite presentation of monoid for a group G, we write x^R for the class of x modulo R in S^*. If $H < G$ is finitely generated, we consider the following problem:

Magnus problem: given $x \in S^*$, do we have $x^R \in H$?

Note that for $H = \{1\}$, we get the word problem as a special case.

If $G < F$ and $u \in F$, we define the *centralizer* $\mathrm{Z}_G(z) = \{x \in G \mid zx = xz\} < G$.

Proposition 3 *If H is a finitely generated subgroup of a finitely presented group G, there is an element z in some finitely presented extension F of G such that $\mathrm{Z}_G(z) = H$.*

In particular, the Magnus problem for G reduces to the commutation problem for F, which is a special case of the word problem.

Proof: Choose generators $u_1, \ldots, u_n$ for the subgroup H and define F as follows:

$$F = G * \langle b \rangle / \leftrightarrow_R^* \text{ where } R = \{(bu_i, u_i b) \mid i = 1, \ldots, n\}.$$

Using the standard presentation of G, we get a presentation of F by the symbols a_x (for $x \in G$), b and $\overline{b}$, with the following relations:

$$a_x a_y = a_{xy}, \quad a_1 = 1, \quad b\overline{b} = 1, \quad \overline{b}b = 1, \quad ba_u = a_u b \text{ (if } u \in H\text{)}.$$

We choose a representative in each right class modulo H, and we write $H^\perp$ for the set of all those representatives, so that each $x \in G$ has a unique decomposition $x = uv$ with $u \in H$ and $v \in H^\perp$. Moreover, we assume that $1 \in H^\perp$.

Now, we can add the superfluous generators $b_v = ba_v$ and $c_v = \overline{b}a_v$ for each $v \in H^\perp$, and the following derivable relations:

$$b = b_1, \quad \overline{b} = c_1, \quad b_1 c_v = a_v \text{ and } c_1 b_v = a_v \text{ (if } v \in H^\perp\text{)},$$

$$b_v a_x = a_u b_w \text{ and } c_v a_x = a_u c_w \text{ (if } vx = uw \text{ with } u \in H \text{ and } v, w \in H^\perp\text{)}.$$

Then we can remove the following relations, which become derivable:

$$b\overline{b} = 1, \quad \overline{b}b = 1, \quad ba_u = a_u b \text{ (if } u \in H\text{)}, \quad b_v = ba_v \text{ and } c_v = \overline{b}a_v \text{ (if } v \in H^\perp\text{)}.$$

By removing the superfluous generators $b = b_1$ and $\overline{b} = c_1$, we get a presention of F by the symbols a_x (for $x \in G$), b_v and c_v (for $v \in H^\perp$) with the following relations:

$$a_x a_y = a_{xy}, \quad a_1 = 1, \quad b_1 c_v = a_v \text{ and } c_1 b_v = a_v \text{ (if } v \in H^\perp\text{)},$$

$$b_v a_x = a_u b_w \text{ and } c_v a_x = a_u c_w \text{ (if } vx = uw \text{ with } u \in H \text{ and } v, w \in H^\perp\text{)}.$$

This presentation is convergent (exercise 8). By the injectivity criterion, the canonical injection $\iota_1 : G \to G * \langle b \rangle$ induces an injective morphism from G into F, and similarly for $\iota_2 : \langle b \rangle \to G * \langle b \rangle$. Hence, F can be seen as an extension of both G and $\langle b \rangle$.

Now, consider the two words $b_1 a_x$ and $a_x b_1$ for $x = uv$ with $u \in H$ and $v \in H^\perp$:

- the reduced form of the first one is $a_u b_v$ (or b_v if $u = 1$);
- the second one is reduced (or its reduced form is b_1 if $x = 1$).

Hence, $b_1 a_x$ and $a_x b_1$ have the same reduced form if and only if $v = 1$, that is $x \in H$. Therefore, $H = \mathrm{Z}_G(b)$, since b_1 is just another name for b. □

Exercise 6 *Which extension F do we get in case $H = \{1\}$ and in case $H = G$?*

Exercise 7 *Prove that F is an extension of both G and $\langle b \rangle$ without using rewriting.*

Indication: Define two projections $\pi_1 : F \to G$ and $\pi_2 : F \to \langle b \rangle$.

Exercise 8 *Check that the above presentation of F is noetherian and confluent.*

Exercise 9 *Prove that $G \cap \langle L \cup \{b\} \rangle = L$ for any $L < G$.*

Indication: Choose representatives in L when it is possible, and check that if a word consists of symbols whose indices are in L, so does its reduced form.

5 Higman-Neumann-Neumann extensions

Let $\varphi : H \to K$ be a partial isomorphism in G. If $z \in G$ is such that $zxz^{-1} = \varphi(x)$ for all $x \in H$, we say that z *represents* φ. If $X \subset G$ is such that $\varphi(H \cap X) = K \cap X$, we say that X is φ-*invariant*. Note that in that case, X is also φ^{-1}-invariant.

Proposition 4 *If $\varphi : H \to K$ is a finitary partial isomorphism in a finitely presented group G, there is an element z in some finitely presented extension F of G such that z represents φ and $G \cap \langle L \cup \{z\} \rangle = L$ for any φ-invariant subgroup L of G.*

Proof: Choose generators $u_1, \ldots, u_n$ for the subgroup H and define F as follows:

$$F = G * \langle b \rangle / \leftrightarrow_R^* \text{ where } R = \{(bu_i, \varphi(u_i)b) \mid i = 1, \ldots, n\}.$$

We introduce the sets $H^\perp$ and $K^\perp$ as in the proof of proposition 3. We get a convergent presention of F by the symbols a_x (for $x \in G$), b_v (for $v \in H^\perp$) and c_v (for $v \in K^\perp$) with the following relations:

$$a_x a_y = a_{xy}, \quad a_1 = 1, \quad b_1 c_v = a_v \text{ (if } v \in K^\perp), \quad c_1 b_v = a_v \text{ (if } v \in H^\perp),$$

$$b_v a_x = a_{\varphi(u)} b_w \text{ (if } vx = uw \text{ with } u \in H \text{ and } v, w \in H^\perp),$$

$$c_v a_x = a_{\varphi^{-1}(u)} c_w \text{ (if } vx = uw \text{ with } u \in K \text{ and } v, w \in K^\perp).$$

By the intectivity criterion, F is an extension of both G and $\langle b \rangle$. Moreover, if $x \in H$, the reduced form of $b_1 a_x c_1$ is $a_{\varphi(x)}$ (or 1 if $x = 1$), which means that b represents φ. The second property is proved by the same method as for exercise 9. □

Exercise 10 *Prove that $G \cap b^{-1}Gb = H$ and $G \cap bGb^{-1} = K$.*

This means that, given $G < F$, the partial isomorphism $\varphi : H \to K$ is completely determined by $b \in F$. This F is called a *Higman-Neumann-Neumann extension of G*.

Let Φ be a set of partial isomorphisms in G. If $Z \subset G$ is such that any $\varphi \in \Phi$ is represented by some $z \in Z$, we say that Z *represents* Φ. If $X \subset G$ is such that X is φ-invariant for any $\varphi \in \Phi$, we say that X is Φ-*invariant*.

Proposition 5 *If Φ is a finite set of finitary partial isomorphisms in a finitely presented group G, there is a finite subset Z of some finitely presented extension F of G such that Z represents Φ and $G \cap \langle L \cup Z \rangle = L$ for any Φ-invariant subgroup L of G.*

Proof: Let $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ with $\varphi_i : H_i \to K_i$ for each i. By iterating the previous construction, we get a chain of finitely presented extensions $G = F_0 < F_1 < \cdots < F_n$ and $z_i \in F_i$ which represents φ_i for each i, so that $Z = \{z_1, \ldots, z_n\}$ represents Φ.

If L is a Φ-invariant subgroup of G, we define $L_i = \langle L \cup \{z_1, \ldots, z_i\} \rangle < F_i$ for each i. In particular, $L_0 = L$, so that $G \cap L_0 = G \cap L = L$. More generally, we prove that $G \cap L_i < L$ by induction on i:

If it holds for $i < n$, then $H_{i+1} \cap L_i < G \cap L_i < L$ so that $H_{i+1} \cap L_i = H_{i+1} \cap L$. Similarly, $K_{i+1} \cap L_i = K_{i+1} \cap L$, and since L is φ_{i+1}-invariant, so is L_i. Hence, $G \cap L_{i+1} < F_i \cap L_{i+1} = F_i \cap \langle L_i \cup \{z_{i+1}\} \rangle = L_i$ so that $G \cap L_{i+1} < G \cap L_i < L$.

Finally, $G \cap \langle L \cup Z \rangle = G \cap L_n < L$, and the converse inclusion holds trivially. □

6 Formal conjugates

For any group G, we define $\widehat{G} = G * \langle b \rangle$. This group is an extension of both G and $\langle b \rangle$. Note also that $\widehat{H} = H * \langle b \rangle = \langle H \cup \{b\} \rangle < \widehat{G}$ for any $H < G$.

We also define $\sharp x = xbx^{-1} \in \widehat{G}$ for any $x \in G$, and $X^\sharp = \langle \sharp X \rangle < \widehat{G}$ for any $X \subset G$, where $\sharp X = \{\sharp x \mid x \in X\} \subset \widehat{G}$. Note that $X^\sharp < G^\sharp < \widehat{G}$.

Proposition 6 *For any group G, the family $(\sharp x)_{x \in G}$ is free in $\widehat{G}$.*

Proof: Using the standard presentation of G, we get a presentation of $\widehat{G}$ by the symbols a_x (for $x \in G$), b and $\overline{b}$, with the following relations:

$$a_x a_y = a_{xy}, \quad a_1 = 1, \quad b\overline{b} = 1, \quad \overline{b}b = 1.$$

We add the superfluous generators $b_x = a_x b a_{x^{-1}}$ and $\overline{b}_x = a_x \overline{b} a_{x^{-1}}$ for each $x \in G$, and the following derivable relations:

$$b = b_1, \quad \overline{b} = \overline{b}_1, \quad b_x\overline{b}_x = 1, \quad \overline{b}_x b_x = 1, \quad a_x b_y = b_{xy} a_x, \quad a_x \overline{b}_y = \overline{b}_{xy} a_x.$$

Then we remove the following relations, which become derivable:

$$b\overline{b} = 1, \quad \overline{b}b = 1, \quad b_x = a_x b a_{x^{-1}}, \quad \overline{b}_x = a_x b a_{x^{-1}}.$$

By removing the superfluous generators $b = b_1$ and $\overline{b} = c_1$, we get a presention of $\widehat{G}$ by the symbols a_x, b_x and $\overline{b}_x$ (for $x \in G$) with the following relations:

$$a_x a_y = a_{xy}, \quad a_1 = 1, \quad b_x\overline{b}_x = 1, \quad \overline{b}_x b_x = 1, \quad a_x b_y = b_{xy} a_x, \quad a_x \overline{b}_y = \overline{b}_{xy} a_x.$$

This presentation is convergent (exercise 11).

Let F be the free group generated by the symbols b_x (for $x \in G$). We have a convergent presentation of F by the symbols b_x and $\overline{b}_x$ (for $x \in G$) with the following relations:

$$b_x\overline{b}_x = 1, \quad \overline{b}_x b_x = 1.$$

Since b_x is just another name for $\sharp x$, the result follows from the injectivity criterion. □

Exercise 11 *Check that the above presentation of $\widehat{G}$ is noetherian and confluent.*

Exercise 12 *Prove that $\sharp x \in X^\sharp$ if and only if $x \in X$.*

Indication: Check that if a word consists of symbols of the form b_x or $\overline{b}_x$ with $x \in X$, so does its reduced form.

Exercise 13 *Prove that $\widehat{H} \cap X^\sharp = (H \cap X)^\sharp$ for any $H < G$ and $X \subset G$.*

Indication: Check that if a word consists of symbols whose indices are in H, so does its reduced form.

Any partial isomorphism $\varphi : H \to K$ in G extends to $\widehat{\varphi} : \widehat{H} \to \widehat{K}$ in $\widehat{G}$ with $\widehat{\varphi}(b) = b$. In particular, $\widehat{\varphi}(\sharp x) = \sharp\varphi(x)$ for any $x \in H$ and $\widehat{\varphi}(X^\sharp) = \varphi(X)^\sharp$ for any $X \subset H$.

Exercise 14 *Prove that if $X \subset G$ is φ-invariant, then $X^\sharp < \widehat{G}$ is $\widehat{\varphi}$-invariant.*

Proposition 7 *If Φ is a finite set of finitary partial isomorphisms in a finitely presented group G, there is a finite subset Z of some finitely presented extension F of $\widehat{G}$ such that for any $x, x_0 \in G$, we have $x \leftrightarrow^*_\Phi x_0$ if and only if $\sharp x \in \langle \{\sharp x_0\} \cup Z \rangle$.*

Proof: We have a finite set $\widehat{\Phi}$ of finitary partial isomorphisms in $\widehat{G}$. By proposition 5, we get some finitely presented extension F of $\widehat{G}$ and a finite subset Z of F such that Z represents $\widehat{\Phi}$. Hence, it is easy to see that $\sharp x \in \langle \{\sharp x_0\} \cup Z \rangle$ whenever $x \leftrightarrow^*_\Phi x_0$.

Let $x_0 \in G$ and $X_0 = \{x \in G \,|\, x \leftrightarrow^*_\Phi x_0\}$. Then X_0 is Φ-invariant by construction. By exercise 14, $X_0^\sharp$ is $\widehat{\Phi}$-invariant, so that $\widehat{G} \cap \langle X_0^\sharp \cup Z \rangle = X_0^\sharp$. If $\sharp x \in \langle \{\sharp x_0\} \cup Z \rangle$, then $\sharp x \in \widehat{G} \cap \langle X_0^\sharp \cup Z \rangle = X_0^\sharp$. By exercise 12, we get $x \in X_0$, that is $x \leftrightarrow^*_\Phi x_0$. $\square$

Hence, the connection problem for Φ reduces to the Magnus problem for some $H < F$. By proposition 2, the Magnus problem is undecidable for some $H < F$, and theorem 2 follows from proposition 3. Note that commutation for groups is also undecidable.

Exercise 15 *Starting from a 2-register machine with n instructions, p of them being branchings, how many generators and relations do we get for the group of theorem 2?*