The word problem for a class of groups with infinite presentation: A computationally universal problem in the BSS model

Klaus Meer, University of Southern Denmark, Odense

joint work with Martin Ziegler, Paderborn

IMA Minneapolis, April 2007

Abstract

The word problem for discrete groups is well-known to be undecidable by a Turing Machine; more precisely, it is reducible both to and from and thus equivalent to the discrete Halting Problem.
The present work introduces and studies a real extension of the word problem for a certain class of groups which are presented as quotient groups of a free group and a normal subgroup. Most important, these groups may be generated by uncountably many generators with index running over certain sets of real numbers. This includes many mathematically important groups which are not captured by the finite framework of the classical word problem.
Our contribution extends computational group theory from the discrete to the Blum-Shub-Smale (BSS) model of real number computations. We believe this to be an interesting step towards applying BSS theory, in addition to semi-algebraic geometry, also to further areas of mathematics.
The main result establishes the word problem for such groups to be computationally equivalent to the Halting Problem for BSS machines. It thus provides the first non-trivial example of a natural problem complete, that is, computationally universal for this model.

1. Introduction

In 1936, Alan M. Turing introduced the now so-called Turing Machine and proved the associated Halting Problem H, that is the question of termination of a given such machine M, to be undecidable. On the other hand simulating a machine M on a Universal Turing Machine establishes H to be semi-decidable. In the sequel, several other problems P were also revealed semi-, yet un-decidable. Two of them, Hilbert's Tenth and the Word Problem for groups, became particularly famous, not least because they arise and are stated in purely mathematical terms whose relation to computer science turned out considerable a surprise.

For real number problems of Scientific Computation as for example in Numerics, Computer Algebra, and Computational Geometry on the other hand, several independent previous formalizations were in 1989 subsumed in a real counterpart to the classical Turing Machines called the Blum-Shub-Smale, for short BSS model.

It bears many structural similarities to the discrete setting like for example the existence of a Universal Machine or the undecidability of the associated real Halting Problem $\mathbb{H}$, that is the question of termination of a given BSS-machine $\mathbb{M}$.

Concerning BSS-complete problems $\mathbb{P}$ however, not many are known so far. The Turing-complete ones for example and, more generally, any discrete problem becomes decidable over the reals; and *extending* an undecidable discrete problem to the reals generally does not work either:

Example 1. Hilbert's Tenth Problem (over R) is the task of deciding, given a multivariate polynomial equation over R, whether it has a solution in R. For integers $R = \mathbb{Z}$, this problem was proven (Turing-)undecidable. For reals $R = \mathbb{R}$ however, it *is* (BSS-)decidable by virtue of Tarski's Quantifier Elimination.

The goal of this work is to extend the classical word problem for finitely presented groups to a new class of groups and show its computational equivalence to the real Halting Problem $\mathbb{H}$.

2. The Word Problem: Classical and new setting

Definition 1.

a) The *free group* $\langle X\rangle$ *generated by a set* X, is the set of all finite sequences $\bar{w} = x_1^{\epsilon_1}\cdots x_n^{\epsilon_n}$ with $n \in \mathbb{N}$, $x_i \in X$, $\epsilon_i \in \{-1,+1\}$, equipped with concatenation $\circ$ as group operation subject to the rules

$$x \circ x^{-1} \quad = \quad 1 \quad = \quad x^{-1} \circ x \qquad \forall x \in X,$$

where $x^1 := x$ and where 1 denotes the empty word (unit element).

b) For a group H and $W \subseteq H$, $\langle W\rangle_H$ is the subgroup of H generated by W and $\langle W\rangle_{H\mathfrak{n}}$ the normal subgroup of H generated by W.

c) For X and $R \subseteq \langle X\rangle$ consider the quotient group $G := \langle X\rangle/\langle R\rangle_{\mathfrak{n}}$, also denoted by $\langle X|R\rangle$. If both X and R are finite, the tuple (X,R) will be called a finite presentation of G; if X is finite and R recursively enumerable (by a Turing machine, that is in the discrete sense; equivalently: semi-decidable), it is a recursive presentation; if X is finite and R arbitrary, G is finitely generated.

Definition 2. (Word Problem) The word problem for $\langle X|R\rangle$ is the task of deciding, given $\bar{w} \in \langle X\rangle$, whether $\bar{w} = 1$ holds in $\langle X|R\rangle$.

The famous work of Novikov and, independently, Boone establishes the word problem for finitely presented groups to be Turing-complete:

Theorem 1. (Novikov, Boone, 1958/59) There exists a finitely presented group $\langle X|R\rangle$ whose associated word problem is many-one reducible by a Turing machine from the discrete Halting Problem H.

An important tool in the proof is

Theorem 2. (Higman Embedding Theorem) Every recursively presented group can be embedded in a finitely generated one.

The above embedding theorem gives a reduction from the word problem of recursively presented groups to that of finitely generated ones.

Note here that trivially each such embedding is computable by a Turing machine. Computability (in the BSS model) of embeddings will not any longer be a triviality for the groups we consider below!

Definition 3. (Real Groups and their Word Problem) Let $X \subseteq \mathbb{R}^\infty := \bigoplus_{d\in\mathbb{N}} \mathbb{R}^d$ and $R \subseteq \langle X\rangle \subseteq \mathbb{R}^\infty$. The tuple (X,R) is called a presentation of the real group $G = \langle X|R\rangle$. This presentation is algebraically generated if X is BSS-decidable and $X \subseteq \mathbb{R}^N$ for some $N \in \mathbb{N}$. G is termed algebraically enumerated if R is in addition BSS semi-decidable; if R is even BSS-decidable, call G algebraically presented. The word problem for the presented real group $G = \langle X|R\rangle$ is the task of BSS-deciding, given $\bar{w} \in \langle X\rangle$, whether $\bar{w} = 1$ holds in G.

Correspondence between classical discrete and new real notions:

Turing	BSS
finitely generated	algebraically generated
recursively presented	algebraically enumerated
finitely presented	algebraically presented

The next example shows already one major difference to finitely presented groups: Decidability of the word problem might depend on the representation.

Example 2. Three presentations $\langle X|R\rangle$ of $(\mathbb{Q},+)$:

a) $X = \{x_r : r \in \mathbb{Q}\}, \quad R = \{x_r x_s = x_{r+s} : r,s \in \mathbb{Q}\}$.

b) $X = \{x_{p,q} : p,q \in \mathbb{Z}, q \neq 0\}$,
$R = \{x_{p,q}x_{a,b} = x_{(pb+aq,qb)} : p,q,a,b \in \mathbb{Z}\} \cup \{x_{p,q} = x_{(np,nq)} : p,q,n \in \mathbb{Z}, n \neq 0\}$.

c) Let $(b_i)_{i\in I}$ denote an algebraic basis of the $\mathbb{Q}$–vector space $\mathbb{R}$; w.l.o.g. $0 \in I$ and $b_0 = 1$. Consider the linear projection $P : \mathbb{R} \to \mathbb{Q}$, $\sum_i r_i b_i \mapsto r_0$ with $r_i \in \mathbb{Q}$;
$X = \{x_t : t \in \mathbb{R}\}$
$R = \{x_t x_s = x_{t+s} : t,s \in \mathbb{R}\} \cup \{x_t = x_{P(t)} : t \in \mathbb{R}\}$.

Case b) yields an algebraic presentation, a) is not even algebraically generated but c) is. The word problem is decidable for a) and b) but not for c).

Example 3. Weil representation of $SL_2(\mathbb{R})$

Main Results

Theorem 3. Let $G = \langle X|R\rangle$ denote an algebraically enumerated real group. Then the associated word problem is BSS semi-decidable.

Proof idea: Quantifier elimination for real closed fields.

Main Theorem. There exists an algebraically presented real group $\mathcal{H} = \langle X|R\rangle$ such that $\mathbb{H}$ is BSS-reducible to the word problem in $\mathcal{H}$.

Sketch of proof ideas:

- generalization of group theoretic tools to our setting: effective homomorphisms, amalgamation, HNN extensions
- introduce effectively benign (e.b.) groups; description of each path set as e.b. subgroup of an algebraically presented group. Notion allows reduction of word problem between certain real groups
- joining path sets by exploiting properties of e.b. groups gives computable embedding in free algebraically presented group.

A few proof details

Definition 4. (HNN extensions) Let $G = \langle X|R\rangle$, let $A = \langle V|R\rangle$, $B = \langle W|R\rangle$ be subgroups of G, and $\phi' : \langle V\rangle \to \langle W\rangle$ be a realization of an isomorphism ϕ between A and B. The Higman-Neumann-Neumann (HNN) extension of G relative to A, B and ϕ is the presented group

$$\langle G; t \mid ta = \phi(a)t \forall a \in A\rangle := \big\langle X \cup \{t\} \mid R \cup \{\phi'(\bar{v})t\bar{v}^{-1}t^{-1} : \bar{v} \in V\}\big\rangle,$$

where $t \notin X$ is a new generator called the *stable letter*.
Note: $A = B$ possible in above definition.

Definition 5. (Effectively benign groups) Let $X \subseteq \mathbb{R}^\infty$, $V \subseteq \langle X\rangle$. The subgroup $A = \langle V|R\rangle$ of $G = \langle X|R\rangle$ is effectively benign (e.b.) in G if the HNN extension $\langle X; t \mid ta = at \forall a \in A\rangle$ admits an effective embedding into some algebraically presented group $K = \langle Y|S\rangle$.

Important: If A is e.b. in G, then A's word problem is reducible to K's.

Lemma 1. (Properties of e.b. groups)
a) Let $A = \langle V|R\rangle \subseteq H = \langle W|R\rangle \subseteq G = \langle X|R\rangle$ sub-/groups, $V \subseteq \langle W\rangle, W \subseteq \langle X\rangle$. If W is decidable and A e.b. in G, then A is e.b. in H.
b) If $G = \langle X|R\rangle$ is algebraically presented and subgroup $A = \langle V|R\rangle$ has decidable V, then A is e.b. in G.

c) If A is e.b. in G and $\phi : G \to H$ an effective embedding, then $\phi(A)$ is e.b. in $\phi(G)$.
d) Let $(A_i)_{i\in I}$ be uniformly e.b. in G, then $\langle \bigcup_{i\in I} A_i\rangle$ admits a presentation e.b. in G.

Path sets and e.b. groups

Consider $\mathbb{H} \subseteq \mathbb{R}^\infty$ real halting problem, $\mathbb{M}$ BSS machine semi-deciding $\mathbb{H}$, γ computation path with path set $\mathbb{A}_\gamma \subseteq \mathbb{R}^d$, $\mathbb{B}_\gamma \subseteq \mathbb{R}^D$ set of intermediate results for computation along γ($d, D \in \mathbb{N}$ only depend on γ).

Goal: Use Lemma 1 to express $\mathbb{A}_\gamma$ as a group U_γ e.b. in an algebraically presented group G to be defined.

Theorem 5. Let $X := \{x_{(i,s)} : s \in \mathbb{R}, i \in \mathbb{N}\} \cup \{y\}, G := \langle X\rangle$ and subgroup $U_\gamma := \langle \bar{w}_{\bar{r}} : \bar{r} \in \mathbb{A}_\gamma\rangle$ where $\bar{w}_{(r_1,\ldots,r_d)} := x^{-1}_{(k,r_d)} \cdots x^{-1}_{(1,r_1)} \cdot y \cdot x_{(1,r_1)} \cdots x_{(k,r_d)}$ for $r_1,\ldots,r_d \in \mathbb{R}$.

Then U_γ has a presentation which is effectively benign in the algebraically presented group G.

To prove Theorem 5 one assigns to each operation σ along path γ a suitable group L_σ. The latter is a subgroup of a HNN extension C of G. The definition of C below guarantees L_σ to be e.b. in G.

Definition 6. Let C denote the infinite HNN extension

$$\left\langle G \; ; \; \begin{array}{ll} a_{(i,t)} & \forall t \in \mathbb{R}\ \forall i \in \mathbb{N} \\ m_{(i,t)} & \forall 0 \neq t \in \mathbb{R}\ \forall i \in \mathbb{N} \end{array} \middle| \; \begin{array}{ll} a_{(i,t)} \cdot g = \phi_{(i,t)}(g) \cdot a_{(i,t)} & \forall g \in G\ \forall (i,t) \\ m_{(i,t)} \cdot g = \psi_{(i,t)}(g) \cdot m_{(i,t)} & \forall g \in G\ \forall (i,t) \end{array} \right\rangle$$

Here, $\phi_{(i,t)}, \psi_{(i,t)} : G \to G$ denote the isomorphisms

$$\begin{array}{llll} \phi_{(i,t)} : x_{(i,s)} \mapsto x_{(i,s+t)}, & x_{(j,s)} \mapsto x_{(j,s)}, & y \mapsto y & \\ \psi_{(i,t)} : x_{(i,s)} \mapsto x_{(i,s\cdot t)}, & x_{(j,s)} \mapsto x_{(j,s)}, & y \mapsto y & \end{array} \quad \forall s \in \mathbb{R} \ .$$

Note: Commuting a stable letter $a_{(i,t)}$ 'causes' a real addition in the sense that $a_{(i,t)} \cdot x_{(i,s)} \cdot a^{-1}_{(i,t)} = x_{(i,s+t)}$. Furthermore:

$$a_{(i,t)} \cdot \bar{w}_{(r_1,\ldots,r_i,\ldots,r_D)} \cdot a^{-1}_{(i,t)} \quad = \quad \bar{w}_{(r_1,\ldots,r_i+t,\ldots,r_D)}.$$

Similarly with generators $m_{(i,t)}$ for multiplication.

Now obtain efficiently benignness of U_γ from that of all the L_σ's along Lemma 1.

Finally, combine all the path groups U_γ by a similar technique to obtain the Main Theorem.

Reference. K. Meer, M. Ziegler: Real Computational Universality: The Word Problem for a class of groups with infinite presentation. Preprint 2006.

If interested send email to: meer@imada.sdu.dk