Found Comput Math (2009) 9: 599–609
DOI 10.1007/s10208-009-9048-2

FOUNDATIONS OF COMPUTATIONAL MATHEMATICS
The Journal of the Society for the Foundations of Computational Mathematics

Real Computational Universality: The Word Problem for a Class of Groups with Infinite Presentation

Klaus Meer · Martin Ziegler

Received: 17 August 2007 / Revised: 7 January 2009 / Accepted: 17 March 2009 / Published online: 29 April 2009

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. As a main difference to discrete groups these groups may be generated by *un*countably many generators with index running over certain sets of real numbers. We study the word problem for such groups within the Blum–Shub–Smale (BSS) model of real number computation. The main result establishes the word problem to be computationally equivalent to the Halting Problem for such machines. It thus gives the first non-trivial example of a problem *complete*, that is, computationally universal for this model.

Keywords Word problem for groups · Computational universality · Blum–Shub–Smale model · Real halting problem

Mathematics Subject Classification (2000) 20F10 · 68Q17 · 68Q10

Communicated by Felipe Cucker.

M. Ziegler supported by DFG (project Zi1009/1-2).

K. Meer (✉)
Theoretical Computer Science, BTU Cottbus, Konrad-Wachsmann-Allee 1, 03046 Cottbus, Germany
e-mail: meer@informatik.tu-cottbus.de

M. Ziegler
Faculty of Computer Science, Electrical Engineering and Mathematics, University of Paderborn, 33095 Paderborn, Germany
e-mail: ziegler@upb.de

1 Introduction

In the classical theory of computation relying on Turing machines the Halting Problem H was the first problem shown to be undecidable. It asks for the termination of a given Turing machine on the empty string as input. Later on, several other and more natural problems P were shown to be of the same degree of undecidability as the Halting Problem. 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 to be kind of a surprise. The corresponding undecidability proofs both proceed by constructing from a given Turing Machine M an instance x_M of the problem P under consideration such that $x_M \in P$ iff M terminates; in other words, a reduction from H to P. As P is easily seen to be semi-decidable this establishes, conversely, reducibility to H and thus Turing-completeness of P.

In this paper we want to study related questions in the Blum–Shub–Smale model, for short BSS model [1, 2]. It is a real counterpart of the Turing model dealing with computations over the real numbers. As for Turing machines there exist universal BSS machines and a related Halting Problem $\mathbb{H}$.

Definition 1 The *real Halting Problem* $\mathbb{H}$ is the following decision problem. Given the code $c_{\mathbb{M}} \in \mathbb{R}^\infty$ of a BSS machine $\mathbb{M}$, does M terminate its computation on input 0?

Both the existence of such a coding for BSS machines and the undecidability of $\mathbb{H}$ in the BSS model were shown in [1]. Concerning other BSS-complete problems $\mathbb{P}$ however, not many are known so far. For example, the Turing-complete ones and, more generally, all discrete problems become decidable over the reals by allowing real constants in the algorithms. Similarly, extending an undecidable discrete problem to the reals usually does not result in a complete problem either. For example, Hilbert's Tenth Problem, which asks whether a given multivariate polynomial equation has a solution, is decidable over $\mathbb{R}$ due to quantifier elimination. And other provably undecidable problems over the reals, such as the Mandelbrot Set or the rationals $\mathbb{Q}$, are supposedly (concerning the first) or, concerning the latter, have actually been established [14] not reducible from and thus strictly easier than $\mathbb{H}$. In fact the only BSS-complete $\mathbb{P}$ essentially differing from $\mathbb{H}$ we are aware of is a certain countable existential theory in the language of ordered fields [6].

The current work presents a real version of the word problem for groups and proves it to be reducible both from and to the real Halting Problem. We introduce a certain class of groups that are generated as quotient groups over a free group which has uncountably many generators. These groups bear some resemblance to certain recent presentations of continuous fundamental groups from topology [5] where, too, the set of generators ('alphabet') is allowed to be infinite and in fact of continuum cardinality. There however words generally have transfinite length whereas we require them to consist of finitely many symbols only. On the other side, the groups we analyze also differ significantly from the usual problems studied in the BSS model which typically stem from semi-algebraic geometry. Indeed, the papers dealing with

groups G in the BSS setting [4, 8, 20] treat such G as underlying structure of the computational model, that is, not over the reals $\mathbb{R}$ and its arithmetic. [22] considers the question of computationally realizing G and its operation, not of deciding properties of (elements of) G. In a rare exception, Derksen, Jeandel, and Koiran do consider BSS-decidability (and complexity) of properties of a real group [7]; however they lack completeness results. Also, their group is not fixed nor presented but given by some matrix generators. For instance, finiteness of the multiplicative subgroup of $\mathbb{C}$ generated by $\exp(2\pi i/x)$, $x \in \mathbb{R}$, is equivalent to $x \in \mathbb{Q}$ and thus undecidable yet not reducible from $\mathbb{H}$ [14]; whereas any fixed such group is isomorphic either to $(\mathbb{Z}, +)$ or to $(\mathbb{Z}_n, +)$ for some $n \in \mathbb{N}$ and has a decidable word problem.

Our work is structured as follows. Section 2 gives a short introduction to the classical word problem in finitely presented groups. We then introduce real counterparts called algebraically presented groups, the core objects of our interest, and illustrate the definition with a few examples. The word problem for these groups is defined and shown to be semi-decidable in the BSS model of computation over the reals. Section 3 recalls some basic notions from computational group theory needed later on. Then, the main result is proved: The real Halting Problem can be reduced to the word problem of algebraically presented real groups. We close in Sect. 3.3 with some discussions.

We suppose the reader to be familiar with the BSS model. Since potential readers likely are complexity theorists we decided to include the presentation of some concepts from combinatorial group theory in Sect. 3.1. It is certainly recommended to study the related material from original sources. In particular, we found the books by Rotman [21] and by Lyndon and Schupp [13] extremely helpful.

2 Word-Problem for Groups

In this section we briefly recall the definition of the classical word problem. We then introduce the class of groups we are interested in and prove semi-decidability of the corresponding word problem in the BSS model.

2.1 The Classical Setting

We briefly recall the classical word problem.

Definition 2 (a) Let X be a set. The *free group generated by* X, denoted by $F = (\langle X\rangle, \circ)$ or more briefly $\langle X\rangle$, is the set $(X \cup X^{-1})^*$ 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

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

where $x^1 := x$ and where 1 denotes the empty word, that is, the unit element.

(b) For a group H and $W \subseteq H$, denote by

$$\langle W\rangle_H := \left\{ w_1^{\epsilon_1} \cdots w_n^{\epsilon_n} : n \in \mathbb{N}, w_i \in W, \epsilon_i = \pm 1 \right\}$$

the subgroup of H generated by W. The *normal* subgroup of H generated by W is

$$\langle W\rangle_{Hn} := \left\langle \left\{ h \cdot w \cdot h^{-1} : h \in H, w \in W \right\} \right\rangle_H .$$

For $h \in H$, we write h/W for the W-coset $\{h \cdot w : w \in \langle W\rangle_{Hn}\}$ of all $g \in H$ with $g \equiv_W h$.

(c) Fix sets X and $R \subseteq \langle X\rangle$ and consider the quotient group $G := \langle X\rangle/\langle R\rangle_n$, denoted by $\langle X|R\rangle$, of all R-cosets of $\langle X\rangle$.

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*.

Intuitively, R induces further rules "$\bar{w} = 1$, $\bar{w} \in R$" in addition to (1); put differently, distinct words $\bar{u}, \bar{v} \in \langle X\rangle$ might satisfy $\bar{u} = \bar{v}$ *in* G, that is, by virtue of R. Observe that the rule "$w_1^{\epsilon_1} \cdots w_n^{\epsilon_n} = 1$" induced by an element $\bar{w} = (w_1^{\epsilon_1} \cdots w_n^{\epsilon_n}) \in R$ can also be applied as "$w_1^{\epsilon_1} \cdots w_k^{\epsilon_k} = w_n^{-\epsilon_n} \cdots w_{k+1}^{-\epsilon_{k+1}}$".

Definition 2 (Continued) (d) 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:

Fact 3 (a) *For any finitely presented group* $\langle X|R\rangle$, *its associated word problem is semi-decidable* (*by a Turing machine*).

(b) *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.

(a) is immediate. For the non-trivial Claim (b), see, e.g., one of [3, 13, 18, 21].

In order to establish Fact 3(b), the following result is crucial.

Fact 4 (Higman Embedding Theorem) *Every recursively presented group can be embedded in a finitely presented group.*

Proof See, e.g., [13, Sect. IV.7] or [21, Theorem 12.18]. □

2.2 Presenting Real Groups

We now define the kind of groups we are interested in and illustrate the definition with a few examples. Semi-decidability of the related word-problem is shown.

Definition 5 Let $X \subseteq \mathbb{R}^\infty$ 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 in addition is BSS semi-decidable; if R is further 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.

Remark 6 (a) More formally, in the above definition R is a set of *vectors of vectors* of varying lengths. However, by suitably encoding delimiters we shall regard R as effectively embedded into *single* vectors of varying lengths.

(b) Although X inherits from $\mathbb{R}$ algebraic structure such as addition $+$ and multiplication $\times$, Definition 2(a) of the free group $G = (\langle X\rangle, \circ)$ considers X as a plain set only. In particular, (group-)inversion in G must not be confused with (multiplicative) inversion: $5 \circ \frac{1}{5} \neq 1 = 5 \circ 5^{-1}$ for $X = \mathbb{R}$. This difference may be stressed notationally by writing 'abstract' generators $x_{\bar{a}}$ indexed with real vectors $\bar{a}$; here $x_5^{-1} \neq x_{1/5}$ holds more intuitively.

(c) Isomorphic (that is, essentially identical) groups $\langle X|R\rangle \cong \langle X'|R'\rangle$ may have different presentations (X, R) and (X', R'). Even when $R = R'$, X need not be unique! Nevertheless we adopt from literature such as [13] the convention of speaking of "the group $\langle X|R\rangle$", meaning a group with presentation (X, R).

For a BSS-machine to read or write a word $\bar{w} \in \langle X\rangle = (X \cup X^{-1})^*$ of course means to input or output a vector $(w_1, \epsilon_1, \ldots, w_n, \epsilon_n) \in (\mathbb{R}^N \times \mathbb{N})^n$. In this sense, rules of type (1) which are implicit in the free group are obviously decidable and may without loss of generality be included in R.

The following are some examples of groups presented in the above way.

Example 7 (a) Every finite *or recursive* presentation is an algebraic presentation. Its word problem is BSS-decidable.

(b) The following is the so-called Weil presentation of $\mathrm{SL}_2(\mathbb{R})$. For each $b \in \mathbb{R}$, write

$$U(b) := \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \qquad V := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$S(a) := V \cdot U\left(\frac{1}{a}\right) \cdot V \cdot U(a) \cdot V \cdot U\left(\frac{1}{a}\right) \in \mathrm{SL}_2(\mathbb{R}).$$

Let $X = \{x_{U(b)} : b \in \mathbb{R}\} \cup \{X_V\}$. Furthermore let R denote the union of the following four families of relations (which are easy but tedious to state formally as subsets of $\langle X\rangle$):

SL1: "$U(\cdot)$ *is an additive homomorphism*";
SL2: "$S(\cdot)$ *is a multiplicative homomorphism*";
SL3: "$V^2 = S(-1)$";
SL4: "$S(a) \cdot U(b) \cdot S(1/a) = U(ba^2) \forall a, b$".

According to [12], $\langle X|R\rangle$ is isomorphic to $\mathrm{SL}_2(\mathbb{R})$ under the natural homomorphism.

(c) The following are presentations $\langle X|R\rangle$ of $(\mathbb{Q}, +)$:

(i) $X = \{x_r : r \in \mathbb{Q}\}$, $R = \{x_r x_s = x_{r+s} : r, s \in \mathbb{Q}\}$.
(ii) $X = \{x_{p,q} : p, q \in \mathbb{Z}, q \neq 0\}$,
$R = \{x_{p,q}x_{a,b} = x_{(pb+aq,qb)} : p, q, a, b \in \mathbb{Z}\} \cup \{x_{p,q} = x_{(np,nq)} : p, q, n \in \mathbb{Z}, n \neq 0\}$.
(iii) Let $(b_i)_{i\in I}$ denote an algebraic basis of the $\mathbb{Q}$-vector space $\mathbb{R}$; without loss to generality $0 \in I$ and $b_0 = 1$. Consider the linear projection $P : \mathbb{R} \to \mathbb{Q}$,

$\sum_i r_i b_i \mapsto r_0$ with $r_i \in \mathbb{Q}$.

$$X = \{x_t : t \in \mathbb{R}\}, \qquad R = \{x_t x_s = x_{t+s} : t, s \in \mathbb{R}\} \cup \{x_t = x_{P(t)} : t \in \mathbb{R}\}.$$

Case (ii) yields an algebraic presentation, (i) is not even algebraically generated but (iii) is. The word problem is decidable for (i): e.g., by effective embedding into $(\mathbb{R}, +)$; and so is it for (ii) although not for (iii): $x_t = 1 \Leftrightarrow P(t) = 0$ but both $P^{-1}(0) = \{\sum_{j\in J} b_j q_j : 0 \notin J \subseteq I \text{ finite}, q_j \in \mathbb{Q}\}$ and its complement are totally disconnected and uncountable, hence BSS-undecidable.

(d) Any semi-algebraic group is algebraically presented. Here, a semi-algebraic group is a semi-algebraic subset of some $\mathbb{R}^n$ bearing a group structure. The graph of the group operation is required to be definable (i.e., semi-algebraic) in $\mathbb{R}^{3n}$. In the algebraic presentation of such a group we can take X as the group elements and R as the graph relation.

The first result below shows that the word problem for any algebraically enumerated real group is not harder than the real Halting Problem.

Theorem 8 *Let $G = \langle X|R\rangle$ denote an algebraically enumerated real group. Then the associated word problem is BSS semi-decidable.*

Proof First, if a $Y \subseteq \mathbb{R}^\infty$ is (semi-)decidable, then so is $\langle Y\rangle$. To see this for a given string $\bar{w} = (y_1, \ldots, y_k) \in \mathbb{R}^k$, consider all 2^{k-1} partitions of $\bar{w}$ into non-empty subwords. For each subword, (semi-)decide whether it belongs to $Y \cup Y^{-1}$. Accept iff, for at least one partition, all its subwords succeed.

Next, for an input w of the word problem for G we have $\bar{w} \equiv 1 \Leftrightarrow \bar{w} \in \langle R\rangle_n$, that is, if and only if

$$\begin{aligned} &\exists n \in \mathbb{N} \exists \bar{x}_1, \ldots, \bar{x}_n \in \langle X\rangle \exists \bar{r}_1, \ldots, \bar{r}_n \in \langle R\rangle : \\ &\bar{w} = \bar{x}_1 \bar{r}_1 \bar{x}_1^{-1} \cdot \bar{x}_2 \bar{r}_2 \bar{x}_2^{-1} \cdots \bar{x}_n \bar{r}_n \bar{x}_n^{-1}. \end{aligned} \tag{2}$$

Since both X and R were assumed to be semi-decidable, the same holds for $\langle X\rangle$ and $\langle R\rangle$. This yields semi-decidability of (2). Indeed, let $f, g :\subseteq \mathbb{R}^\infty \to \mathbb{R}^\infty$ be BSS-computable with $\langle X\rangle = \text{range}(f)$ and $\langle R\rangle = \text{range}(g)$; then it is easy to construct (but tedious to formalize) from f and g a BSS-computable function on $\mathbb{R}^\infty$ ranging over all $n \in \mathbb{N}$, all $\bar{w} \in \langle X\rangle$, all $\bar{x}_1, \ldots, \bar{x}_n \in \langle X\rangle$, and all $\bar{r}_1, \ldots, \bar{r}_n \in \langle R\rangle$. Compose its output with the decidable test "$\bar{w} = \bar{x}_1 \bar{r}_1 \bar{x}_1^{-1} \cdots \bar{x}_n \bar{r}_n \bar{x}_n^{-1}$?" and, if successful, return $\bar{w}$. This constitutes a function on $\mathbb{R}^\infty$ with range exactly $\langle R\rangle_n$. By quantifier elimination over $\mathbb{R}$ the latter is equivalent to semi-decidability of the word problem in G, see [15]. □

3 Reduction *from* the Real Halting Problem

This section proves the main result of the paper, the continuous counterpart to Fact 3(b): The word problem for algebraically presented real groups is in general not only undecidable in the BSS model but in fact as hard as the real Halting Problem.

3.1 Basics from Group Theory and Their Presentations

For sake of completeness this subsection briefly recalls some constructions from group theory and their properties to be used in the next subsection. The familiar reader can skip this part. For a more detailed exposition as well as proofs of the cited results we refer to the two textbooks [13, 21].

Here, no (e.g., effectivity) assumptions are made concerning the set of generators nor relations presenting a group. To start with let us briefly extend the standard notions of a subgroup and a homomorphism to the setting of *presented* groups:

Definition 9 A *subgroup* U of the presented group $G = \langle X|R\rangle$ is a tuple (V, S) with $V \subseteq \langle X\rangle$ and $S = R \cap \langle V\rangle$. This will be denoted by $U = \langle V|R_V\rangle$ or, more relaxed, $U = \langle V|R\rangle$.

A *realization* of a homomorphism $\psi : G \to H$ between presented groups $G = \langle X|R\rangle$ and $H = \langle Y|S\rangle$ is a mapping $\psi' : X \to \langle Y\rangle$ whose unique extension to a homomorphism on $\langle X\rangle$ maps R-cosets to S-cosets.

A realization of an isomorphism ϕ is a realization of ϕ as a homomorphism.

Fact 10 (Nielsen) *Let* $U \subseteq \langle X\rangle$.

(a) *Suppose* U *is finite. Then there exists a finite* $V \subseteq \langle X\rangle$ *such that* $\langle U\rangle_{\langle X\rangle} = \langle V\rangle_{\langle X\rangle}$ *and* V *is* Nielsen reduced *in the sense that it satisfies for all* $u, v, w \in V \cup V^{-1}$:
(N0) $u \neq 1$.
(N1) *If* $uv \neq 1$, *then* $|uv| \geq \max\{|u|, |v|\}$.
(N2) *If* $uv \neq 1 \neq vw$, *then* $|uvw| > |u| - |v| + |w|$
where $|u|$ *denotes the length of* $u \in \langle X\rangle$.

(b) *Suppose* U *is Nielsen-reduced. Then* $u_1, \ldots, u_n \in U \cup U^{-1}$ *with* $u_i u_{i+1} \neq 1$ *implies* $|u_1 \cdots u_n| \geq n$. *In particular the subgroup* $\langle U\rangle_{\langle X\rangle}$ *of* $\langle X\rangle$ *is again free and isomorphic to* $\langle U\rangle$.

(c) *Every subgroup of* $\langle X\rangle$ *is free.*

Proof Cf. [13, Sect. I.2]. □

Definition 11 (Free Product) Consider two presented groups $G = \langle X|R\rangle$ and $H = \langle Y|S\rangle$ with disjoint generators $X \cap Y = \emptyset$—e.g., by proceeding to $X' := X \times \{1\}$, $Y' := Y \times \{2\}$, $R' := R \times \{1\}$, $S' := S \times \{2\}$. The *free product* of G and H is the presented group

$$G * H := \langle X \cup Y|R \cup S\rangle.$$

Similarly for the free product $\ast_{i\in I} G_i$ with $G_i = \langle X_i|R_i\rangle$, i ranging over an arbitrary index set I.

In many situations one wants to identify certain elements of a free product of groups. These are provided by a basic construction called *Higman–Neumann–Neumann* (or shortly HNN) extension, see [10, 13, 21].

Definition 12 (HNN Extension) Let $G = \langle X|R\rangle$, $A = \langle V|R\rangle$, $B = \langle W|R\rangle$ be subgroups of G, and ϕ' a realization of an isomorphism between A and B. The *Higman–Neumann–Neumann* (HNN) extension of G relative to A, B and ϕ is the presented group

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

G is the *base* of the HNN extension, $t \notin X$ is a new generator called the *stable letter*, and A and B are the *associated subgroups* of the extension.

Similarly for the HNN extension $\langle G; (t_i)_{i\in I} \mid t_i a = \phi_i(a)t_i\forall a \in A_i\forall i \in I\rangle$ with respect to a family of isomorphisms $\phi_i : A_i \to B_i$ and subgroups $A_i, B_i \subseteq G$, $i \in I$.

HNN extensions admit simple and intuitive characterizations for a word to be, in the resulting group, equivalent to 1. These results are connected to some very famous names in group theory. Proofs can be found, e.g., in [13, Chap. IV] or [21, Chap. 11].

Fact 13 (Higman–Neumann–Neumann) *Let $G^* := \langle G; t|ta = \phi(a)t\forall a \in A\rangle$ be an HNN extension of G. Then, identity $g \mapsto g$ is an embedding of G into G^*.*

Fact 14 (Britton's Lemma) *Let $G^* := \langle G; t|ta = \phi(a)t\forall a \in A\rangle$ be an HNN extension of G. Consider a sequence $(g_0, t^{\epsilon_1}, g_1, \ldots, t^{\epsilon_n}, g_n)$ with $n \in \mathbb{N}$, $g_i \in G$, $\epsilon_i \in \{-1, 1\}$. If it contains no consecutive subsequence (t^{-1}, g_i, t) with $g_i \in A$ nor (t, g_j, t^{-1}) with $g_j \in B$, then there holds $g_0 \cdot t^{\epsilon_1} \cdot g_1 \cdots t^{\epsilon_n} \cdot g_n \neq 1$ in G^*.*

3.2 The Main Result

With the preparations and tools from the previous sections we may now establish the main result of this work: the existence of an algebraically presented group such that the real Halting Problem can be reduced to the word problem of that group.

The next corollary reduces in an elementary way the membership problem in a set to the word problem in a suitably defined group.

Corollary 15 *Let $X := \{x_r : r \in \mathbb{R}\}$, $H \subseteq X^\infty$ and let s and t be two further elements not in X. For an element $(x_{r_1}, \ldots, x_{r_d}) \in X^\infty$ coded via $r := (r_1, \ldots, r_d)$ define $\bar{w}_r$ in the free group generated by X and s as*

$$\bar{w}_{r_1,\ldots,r_d} := x_{r_d}^{-1} \cdots x_{r_1}^{-1} \cdot s \cdot x_{r_1} \cdots x_{r_d}.$$

Now let G be the group generated by X, s, t and presented by relations saying that t and $\bar{w}_r$ commute iff r codes an element in H:

$$G = \big\langle X, s, t|t\bar{w}_r = \bar{w}_r t\ \forall r = (r_1, \ldots, r_d) \text{ such that } (x_{r_1}, \ldots, x_{r_d}) \in H\big\rangle.$$

Then in G we have $t \cdot \bar{w}_r \cdot t^{-1} \cdot \bar{w}_r^{-1} = 1$ if and only if $(x_{r_1}, \ldots, x_{r_d}) \in H$.

Proof The words $\bar{w}_r, (x_{r_1}, \ldots, x_{r_d}) \in X^\infty$ are Nielsen-reduced in the free group $\langle X, s\rangle$. Thus, the set of all $\bar{w}_r, r \in \mathbb{R}^\infty$ forms a free set in this group. Now the group

G in the statement is an HNN-extension of $\langle X, s\rangle$. According to Britton's lemma $t \cdot \bar{w}_r \cdot t^{-1} \cdot \bar{w}_r^{-1} = 1$ in G if and only if $(x_{r_1}, \ldots, x_{r_d}) \in H$. □

The corollary holds as well for arbitrary sets X not related to $\mathbb{R}^\infty$.

Example 16 If we choose $X = \{0, 1\}$ and H as the classical Halting problem, then the corollary gives a group G with undecidable word problem. However, this group is not finitely presented.

Theorem 17 *There exists an algebraically presented real group $\mathcal{H} = \langle X|R\rangle$ such that the real Halting problem $\mathbb{H}$ is BSS-reducible to the word problem in $\mathcal{H}$.*

Proof Let $\mathbb{H}$ be semi-decided by some constant-free universal BSS Machine $\mathbb{M}$. Denote by $n \mapsto \gamma_n$ an effective enumeration of all computational paths of $\mathbb{M}$ and let $\mathbb{H}_n \subseteq \mathbb{H}$ be the set of inputs accepted at path γ_n. Without loss of generality we can assign a dimension $d(n)$ to each such path, i.e., $\mathbb{H}_n \subseteq \mathbb{H} \cap \mathbb{R}^{d(n)}$. Let G be the group defined in Corollary 15 with $H := \mathbb{H}$:

$$G = \big\langle X, s, t | t\bar{w}_r = \bar{w}_r t \ \ \forall r = (r_1, \ldots, r_{d(n)}) \text{ such that } (x_{r_1}, \ldots, x_{r_d}) \in \mathbb{H}\big\rangle.$$

The set of rules is semi-decidable. The following construction transforms it into a decidable set of rules. Take a new generator k, $k \notin \{s, t, x_r | r \in \mathbb{R}\}$ and define $\mathcal{H}$ as

$$\mathcal{H} = \big\langle x_r, r \in \mathbb{R}; s; t; k | k = 1, t \cdot \bar{w}_r \cdot t^{-1} \cdot \bar{w}_r^{-1} k^n = 1 \ \forall n \in \mathbb{N}, \forall r \text{ such that}$$
$$(x_{r_1}, \ldots, x_{r_{d(n)}}) \in \mathbb{H}_n\big\rangle.$$

Now in $\mathcal{H}$ we have

$$t \cdot \bar{w}_r \cdot t^{-1} \cdot \bar{w}_r^{-1} = 1 \Leftrightarrow t \cdot \bar{w}_r \cdot t^{-1} \cdot \bar{w}_r^{-1} \cdot k^n = 1 \quad \text{for an } n \in \mathbb{N}$$
$$\Leftrightarrow (x_{r_1}, \ldots, x_{r_{d(n)}}) \in \mathbb{H}_n \quad \text{for an } \ n \in \mathbb{N}.$$

Thus, the word problem in $\mathcal{H}$ is at least as hard as the real Halting problem. Finally, the set of rules defining $\mathcal{H}$ is decidable since each $\mathbb{H}_n$ is. □

Note that since a universal BSS Machine does not need constants, it follows that the real Halting Problem $\mathbb{H}$ is reducible to the word problem of an algebraically presented group $\langle X|R\rangle$ with X semi-algebraic and R countable unions of sets semi-algebraic over $\mathbb{Q}$!

3.3 Conclusions and Questions

This note has introduced the class of algebraically presented real groups given as a quotient group of a free group and a normal subgroup. The free group was defined through a possibly uncountable set of generators BSS-decidable in some fixed dimensional space; the relations are similarly generated by a BSS-decidable set. We then considered the word problem for such groups: Given a finite sequence of generators,

decide whether this word is equivalent (with respect to the relations) to the unit element? We believe our results to be an interesting step into the direction of extending the BSS theory into different areas of mathematics. Many of the known computability and complexity results in the BSS model are closely related to computational problems of semi-algebraic sets. Though these play an important role in our approach as well, the resulting problem is located in the area of computational group theory; its connection to semi-algebraic geometry is visible in the background only.

The above proof works as well for the BSS model over the complex numbers and more general structures, for example those defined in [9] and by Poizat [19].

There remain some interesting questions to be investigated further.

In our approach it seems crucial for the relations R to live in $\mathbb{R}^\infty$; this holds in view of the rules defining $\mathcal{H}$ in the proof of Theorem 17. They include words $\bar{w}_{\bar{r}}$ of length $1 + 2d(n)$ and thus unbounded in n.

Question 1 Can one restrict the set of relations to some finite-dimensional and definable subset of a suitable $\mathbb{R}^M$?

A positive answer could be seen as a real analogue of the Novikov–Boone theorem.

It would furthermore be nice to have a real counterpart to the famous Higman Embedding Theorem (Fact 4):

Question 2 Does every semi-algebraically presented real group admit a (BSS-computable) embedding into an effectively presented one?

Special classes of discrete groups with *decidable* word problems have been investigated with respect to the computational *complexity* of this decision [11, 17]. This looks interesting to carry over to the reals; for instance in the form of

Question 3 Can we find a class of groups whose word problem is (decidable and) complete for a certain complexity class like $\mathcal{NP}_\mathbb{R}$?

This would be interesting in order to extend the yet sparse list of known $\mathcal{NP}_\mathbb{R}$-complete problems.

Finally, an entire bunch of interesting questions results from inspecting further classical undecidability results in the new framework. We close here by just referring to the survey paper [16] in which a lot of related issues are discussed.

Acknowledgements We are very thankful to an anonymous referee. Her/his extremely careful reading and insightful remarks helped to improve the paper a lot. In particular, an earlier proof of our main result could be simplified significantly.

References

1. L. Blum, M. Shub, S. Smale, On a theory of computation and complexity over the real numbers: $\mathcal{NP}$-completeness, recursive functions, and universal machines, *Bull. Am. Math. Soc.* **21**, 1–46 (1989).

2. L. Blum, F. Cucker, M. Shub, S. Smale, *Complexity and Real Computation* (Springer, New York, 1998).
3. W.W. Boone, The word problem, *Proc. Natl. Acad. Sci. U.S.A.* **44**, 265–269 (1958).
4. M. Bourgade, Separations et transferts dans la hiérarchie polynomiale des groupes abéliens infinis, *Math. Log. Q.* **47**, 493–502 (2001).
5. J.W. Cannon, G.R. Conner, The combinatorial structure of the Hawaiian earring group, *Topology Appl.* **106**, 225–271 (2000).
6. F. Cucker, The arithmetical hierarchy over the reals, *J. Log. Comput.* **2**(3), 375–395 (1992).
7. H. Derksen, E. Jeandel, P. Koiran, Quantum automata and algebraic groups, *J. Symb. Comput.* **39**, 357–371 (2005).
8. C. Gaßner, The $\mathcal{P} = \mathcal{DNP}$ problem for infinite abelian groups, *J. Complex.* **17**, 574–583 (2001).
9. J.B. Goode, Accessible telephone directories, *J. Symb. Log.* **59**, 92–105 (1994).
10. G. Higman, B.H. Neumann, H. Neumann, Embedding theorems for groups, *J. Lond. Math. Soc.* **24**, 247–254 (1949).
11. D.F. Holt, S. Rees, C.E. Röver, R.M. Thomas, Groups with context-free co-word problem, *J. Lond. Math. Soc.* **71**(3), 643–657 (2005).
12. S. Lang, $\mathrm{SL}_2(\mathbb{R})$ (Springer, New York, 1985).
13. R.C. Lyndon, P.E. Schupp, *Combinatorial Group Theory* (Springer, Berlin, 1977).
14. K. Meer, M. Ziegler, An explicit solution to Post's problem over the reals, *J. Complex.* **24**(1), 3–15 (2008).
15. C. Michaux, Ordered rings over which output sets are recursively enumerable, *Proc. Am. Math. Soc.* **112**, 569–575 (1991).
16. C.F. Miller III, Decision problems for groups—survey and reflections, in *Algorithms and Classification in Combinatorial Group Theory*, ed. by G. Baumslag, C.F. Miller III. Math. Sci. Res. Inst. Publ., vol. 1 (Springer, New York, 1992), pp. 1–59.
17. D.E. Muller, P.E. Schupp, Groups, the theory of ends, and context-free languages, *J. Comput. Syst. Sci.* **26**, 295–310 (1983).
18. P.S. Novikov, On the algorithmic unsolvability of the word problem in group theory. Tr. Mat. Inst. Steklov **44** (1955).
19. B. Poizat, *Les Petits Cailloux* (Aléas, Lyon, 1995).
20. M. Prunescu, A model-theoretic proof for $\mathcal{P} \neq \mathcal{NP}$ over all infinite abelian groups, *J. Symb. Log.* **67**, 235–238 (2002).
21. J.J. Rotman, *An Introduction to the Theory of Groups*, 4th edn. (Springer, Berlin, 1995).
22. J.V. Tucker, Computability and the algebra of fields, *J. Symb. Log.* **45**, 103–120 (1980).