Real Computational Universality: The Word Problem for a class of groups with infinite presentation

Klaus Meer[1⋆] and Martin Ziegler[2⋆⋆]

[1] IMADA, Syddansk Universitet, Campusvej 55,
5230 Odense M, Denmark (meer@imada.sdu.dk)
[2] Japan Advanced Institute Of Science and Technology,
and University of Paderborn (ziegler@upb.de)

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 main difference with discrete groups, these groups may be generated by *un*countably many generators with index running over certain sets of real numbers. This includes a variety of 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 computation. It provides a 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 not only semi-decidable (and thus reducible *from*) but also reducible *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.

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. The according 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.

Turing Machines are still nowadays, 70 years after their introduction, considered the appropriate model of computation for discrete problems, that is, over bits and integers. For

⋆ partially supported by the IST Programme of the European Community, under the PASCAL Network of Excellence, IST-2002-506778 and by the Danish Natural Science Research Council SNF. This publication only reflects the authors' views. Part of the work has been done during a sabbatical which K. Meer spent at the Forschungsinstitut für Diskrete Mathematik at the university of Bonn, Germany. The hospitality during that stay is gratefully acknowledged.
⋆⋆ supported by DFG (project Zi1009/1-1) and by JSPS (ID PE 05501).

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 [BSS89, BCSS98]. 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 [BSS89, EXAMPLE §1.6]; 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 has been proven (Turing-)undecidable [Mat70]. For reals $R = \mathbb{R}$ however, it *is* (BSS-)decidable by virtue of TARSKI's Quantifier Elimination [BCSS98, top of p.97].

□

1.1 Relation to Previous Works

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 [MZ05] *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 [Cuc92, THEOREM 2.13].

The present work closes this structural gap by presenting a real generalization of the word problem for groups and proving it to be reducible both from and to the real Halting Problem. On the way to that, we significantly extend notions from classical and computational (discrete, i.e.) combinatorial group theory to the continuous setting of BSS-computability. Several examples reveal these new notions as mathematically natural and rich. They bear some resemblance to certain recent presentations of continuous fundamental groups from topology [CC00] 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 only finitely many symbols.

We find our synthesis of computational group theory and real number computability to 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 [Bou01, Gas01, Pru02] treat such G as underlying structure of the computational model, that is, not over the reals $\mathbb{R}$ and its arithmetic. [Tuc80] considers the question of computational realizing G and its operation, not of deciding properties of (elements of) G. A rare exception, DERKSEN, JEANDEL, and KOIRAN do consider BSS-decidability (and complexity) of properties of a real group [DJK05]; 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 $\mathbb{H}$ [MZ05]; whereas any fixed such group is isomorphic either to $(\mathbb{Z}, +)$ or to $(\mathbb{Z}_n, +)$ for some $n \in \mathbb{N}$ and has decidable word problem (Examples 12 and 13).

1.2 Overview

Our work is structured as follows. In Section 2 we recall basic notions of real number computation. Section 3 starts with a review of the classical word problem in *finitely* presented groups. Then we introduce real counterparts called algebraically presented groups, the core objects of our interest. We give some guiding examples of mathematical groups

that fit into this framework. The word problem for these groups is defined and shown to be semi-decidable in the BSS model of computation over the reals. Section 4 proves our main result: We recall basic concepts from algebra used in the analysis of the word problem (Section 4.1) like Higman-Neumann-Neumann (for short: HNN) extensions and Britton's Lemma (Section 4.2). It follows the concept of a benign subgroup (Section 4.3); in the discrete case, this notion due to [Hig61] relies implicitly on finiteness presumptions and thus requires particular care when generalizing to the continuous case. Sections 4.4 and 4.5 prove the paper's central claim: The real Halting Problem can be reduced to the word problem of algebraically presented real groups. We close in Section 5 with some conclusions.

The paper tries to be self-contained for complexity theorists. This especially holds with respect to the presentation of some concepts from combinatorial group theory. It is certainly recommended to study the related material from original sources. In particular, we found the books by ROTMAN [Rot95] and by LYNDON and SCHUPP [LS77] extremely helpful.

2 BSS-Machines and the Real Halting Problem

This section summarizes very briefly the main ideas of real number computability theory. For a more detailed presentation see [BCSS98].

Essentially a (real) BSS-machine can be considered as a Random Access Machine over $\mathbb{R}$ which is able to perform the basic arithmetic operations at unit cost and which registers can hold arbitrary real numbers. Its inputs are thus finite sequences over $\mathbb{R}$ of possibly unbounded length.

Definition 2. [BSS89]

a) *Let $\mathbb{X} \subseteq \mathbb{R}^\infty := \biguplus_{d\in\mathbb{N}} \mathbb{R}^d$, i.e. a set of finite sequences of real numbers. Its* DIMENSION, $\dim(\mathbb{X})$, *is the smallest $D \in \mathbb{N}$ such that $\mathbb{X} \subseteq \bigoplus_{d\le D} \mathbb{R}^d$; $\dim(\mathbb{X}) = \infty$ if no such D exists.*

b) *A* BSS-MACHINE $\mathbb{M}$ OVER $\mathbb{R}$ WITH ADMISSIBLE INPUT SET $\mathbb{X}$ *is given by a finite set I of instructions labeled by $1,\dots,N$. A configuration of $\mathbb{M}$ is a quadruple $(n,i,j,\bar{y}) \in I\times\mathbb{N}\times\mathbb{N}\times\mathbb{R}^\infty$. Here, n denotes the currently executed instruction, i and j are used as addresses (copy-registers) and $\bar{y}$ is the actual content of the registers of $\mathbb{M}$. The initial configuration of $\mathbb{M}$'s computation on input $\bar{x}\in\mathbb{X}$ is $(1,1,1,\bar{x})$. If $n = N$ and the actual configuration is $(N,i,j,\bar{y})$, the computation stops with output $\bar{y}$. The instructions $\mathbb{M}$ is allowed to perform are of the following types:*

- **computation:** *$n : y_s \leftarrow y_k \circ_n y_l$, where $\circ_n \in \{+,-,\times,\div\}$; or $n : y_s \leftarrow \alpha$ for some $\alpha \in \mathbb{R}$.*
  The register #s will get the value $y_k \circ_n y_l$ or α, respectively. All other register-entries remain unchanged. The next instruction will be $n+1$; moreover, the copy-register i is either incremented by one, replaced by 0, or remains unchanged. The same holds for copy-register j.
- **branch:** *n:* **if** $y_0 \ge 0$ **goto** $\beta(n)$ **else goto** $n+1$. *According to the answer of the test the next instruction is determined (where $\beta(n) \in I$). All other registers are not changed.*
- **copy:** *$n : y_i \leftarrow y_j$, i.e. the content of the "read"-register is copied into the "write"-register. The next instruction is $n+1$; all other registers remain unchanged.*

c) *The size of an $\bar{x}\in\mathbb{R}^d$ is $\mathrm{size}_\mathbb{R}(\bar{x}) = d$. The cost of any of the above operations is 1. The cost of a computation is the number of operations performed until the machine halts.*

d) *For some $\mathbb{X}\subseteq\mathbb{R}^\infty$ we call a function $f : \mathbb{X}\to\mathbb{R}^\infty$ (BSS-)computable iff it is realized by a BSS machine over admissible input set $\mathbb{X}$. Similarly, a set $\mathbb{X}\subseteq\mathbb{R}^\infty$ is decidable in $\mathbb{R}^\infty$ iff its characteristic function is computable. $\mathbb{X}$ is called a decision problem or a language over $\mathbb{R}^\infty$.*

e) A BSS oracle machine using an oracle set $\mathbb{O} \subseteq \mathbb{R}^\infty$ is a BSS machine with an additional type of node called oracle node. Entering such a node the machine can ask the oracle whether a previously computed element $\bar{y} \in \mathbb{R}^\infty$ belongs to $\mathbb{O}$. The oracle gives the correct answer at unit cost.

A real Halting Problem now can be defined straightforwardly as well.

Definition 3. *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 [BSS89].

3 Word-Problem for Groups

Groups occur ubiquitously in mathematics, and having calculations with and in them handled by computers constitutes an important tool both in their theoretical investigation and in practical applications as revealed by the flourishing field of *Computational Group Theory* [FK91, FK95, HEB05]. Unfortunately already the simplest question, namely equality '$a = b$' of two elements $a, b \in G$ is in general undecidable for groups G reasonably presentable to a digital computer, that is, in a finite way — the celebrated result obtained in the 1950ies independently by NOVIKOV [Nov59] and BOONE [Boo58]. In the canonical model of real number decidability[1] on the other hand, *every* discrete problem $L \subseteq \Sigma^*$ is solvable [BSS89, EXAMPLE §1.6], rendering the word problem for finitely presented groups trivial.

However, whenever we deal with computational questions involving groups of real or complex numbers, the Turing model seems not appropriate anyway. As an example take the unit circle in $\mathbb{R}^2$ equipped with complex multiplication. There is a clear mathematical intuition how to compute in this group; such computations can be formalized in the BSS model. We thus aim at a continuous counterpart to the discrete class of finitely presented groups for which the word problem is universal for the BSS model.

After recalling basic notions related to the (classical) word problem of finitely presented groups (Section 3.1) we introduce in Section 3.2 the larger class of algebraically presented real groups. Section 3.3 gives several examples showing how this new class covers natural groups occurring in mathematics. Next (Section 3.4) we establish semi-decidability of the word problem for algebraically presented groups, that is, reducibility to the Halting Problem $\mathbb{H}$ in the real number model of Blum, Shub, and Smale. Our main result then proves the existence of algebraically presented groups for which the word problem is reducible from $\mathbb{H}$; this covers the entire Section 4.

3.1 The Classical Setting

Here, the setting for the classical word problem is briefly recalled. A review of the main algebraic concepts needed in our proofs is postponed to Section 4.

Definition 4. *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 $\bar{w} = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ with $n \in \mathbb{N}$, $x_i \in X$, $\varepsilon_i \in \{-1, +1\}$, equipped with concatenation $\circ$ as group operation subject to the rules*

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

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

[1] We remark that in the other major and complementary model of real number computation, decidability makes no sense as it corresponds to evaluating a characteristic and thus discontinuous function which is uncomputable due to the so-called Main Theorem of Recursive Analysis [Wei00, THEOREM 4.3.1].

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

$$\langle W\rangle_H := \left\{ w_1^{\varepsilon_1} \cdots w_n^{\varepsilon_n} : n \in \mathbb{N}, w_i \in W, \varepsilon_i = \pm 1 \right\}$$

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

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

For $h \in H$, we write h/W for its W–coset $\{h \cdot w : w \in \langle W\rangle_{H\mathrm{n}}\}$ 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 $G := \langle X\rangle / \langle R\rangle_{\mathrm{n}}$, 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[2] 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 Equation (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 "$w_1^{\varepsilon_1} \cdots w_n^{\varepsilon_n} = 1$" induced by an element $\bar{w} = (w_1^{\varepsilon_1} \cdots w_n^{\varepsilon_n}) \in R$ can also be applied as "$w_1^{\varepsilon_1} \cdots w_k^{\varepsilon_k} = w_n^{-\varepsilon_n} \cdots w_{k+1}^{-\varepsilon_{k+1}}$".

Definition 4 (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 5. *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. □

Of course, a) is immediate. For the highly nontrivial Claim b), see e.g. one of [Boo58, Nov59, LS77, Rot95].

Example 6. $\mathcal{H} := \left\langle \{a,b,c,d\} \,\middle|\, \{a^{-i}ba^i = c^{-i}dc^i : i \in H\} \right\rangle$
is a *recursively* presented group with word problem reducible from H; compare the proof of [LS77, THEOREM §IV.7.2]. □

In order to establish Fact 5b), we need a *finitely* presented group. This step is provided by the remarkable

Fact 7 (Higman Embedding Theorem). *Every recursively presented group can be embedded in a finitely generated one.*

Proof. See, e.g., [LS77, SECTION §IV.7] or [Rot95, THEOREM 12.18]. □

Fact 7 asserts the word problem from Example 6 to be in turn reducible to that of the finitely presented group $\mathcal{H}$ is embedded into, because any such embedding is automatically effective:

[2] This notion seems misleading as R is in general *not* recursive; nevertheless it has become established in literature.

Observation 8. *Let $G = \langle X\rangle/\langle R\rangle_{\mathrm{n}}$ and $H = \langle Y\rangle/\langle S\rangle_{\mathrm{n}}$ denote finitely generated groups and $\psi : G \to H$ a homomorphism. Then, ψ is (Turing-) computable in the sense that there exists a computable homomorphism $\psi' : \langle X\rangle \to \langle Y\rangle$ such that $\psi(\bar{x}) \in \langle S\rangle_{\mathrm{n}}$ whenever $\bar{x} \in \langle R\rangle_{\mathrm{n}}$; that is, ψ' maps R-cosets to S-cosets and makes the following diagram commute:*

$$\begin{array}{ccc} \langle X\rangle & \xrightarrow{\psi'} & \langle Y\rangle \\ \downarrow & & \downarrow \\ \langle X\rangle/\langle R\rangle_{\mathrm{n}} & \xrightarrow{\psi} & \langle Y\rangle/\langle S\rangle_{\mathrm{n}} \end{array} \tag{2}$$

Indeed, due the homomorphism property, ψ is uniquely determined by its values on the finitely many generators $x_i \in X$ of G, that is, by $\psi(x_i) = \bar{w}_i/\langle S\rangle_{\mathrm{n}}$ where $\bar{w}_i \in \langle Y\rangle$. Setting (and storing in a Turing Machine) $\psi'(x_i) := \bar{w}_i$ yields the claim.

3.2 Presenting Real Groups

Regarding that the BSS-machine is the natural extension of the Turing machine from the discrete to the reals, the following is equally natural a generalization of Definition 4c+d):

Definition 9. *Let $X \subseteq \mathbb{R}^\infty$ and $R \subseteq \langle X\rangle \subseteq^3 \mathbb{R}^\infty$. 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.*

The next table summarizes the correspondence between the classical discrete and our new real notions.

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

Remark 10. a) Although X inherits from $\mathbb{R}$ algebraic structure such as addition $+$ and multiplication $\times$, the Definition 4a) 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, 'obviously' $x_5^{-1} \neq x_{1/5}$.

b) Isomorphic (that is, essentially identical) groups $\langle X|R\rangle \cong \langle X'|R'\rangle$ may have different presentations (X,R) and (X',R'); see Section 3.3. Even when $R = R'$, X need not be unique! Nevertheless we adopt from literature such as [LS77] the convention[4] of speaking of "the group $\langle X|R\rangle$", meaning a group with presentation (X,R).
This however requires some care, for instance when $\bar{w}$ is considered (as in Definition 4d) both an element of $\langle X\rangle$ and of $\langle X|R\rangle$! For that reason we prefer to write $\langle W\rangle_H$ rather than, e.g., $\mathrm{Gp}(W)$: to indicate in which group we consider a subgroup to be generated.

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 $(w_1, \varepsilon_1, \ldots, w_n, \varepsilon_n) \in (\mathbb{R}^N \times \mathbb{N})^n$. In this sense, the Rules (1) implicit in the free group are obviously decidable and may w.l.o.g. be included in R.

[3] Most formally, 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.

[4] This can be justified with respect to the solvability of the word problem in the case of *finite* presentations and *non*uniformly by virtue of TIETZE's Theorem [LS77, PROPOSITIONS §II.2.1 and §II.2.2].

3.3 Examples

Example 11. Every finite *or recursive* presentation is an algebraic presentation. Its word problem is BSS-decidable.

As long as X in Definition 4c) is at most countable, so will be any group $\langle X|R\rangle$. Only proceeding to real groups as in Definition 9 can include many interesting uncountable groups in mathematics.

Example 12. Let $\mathbb{S}$ denote the unit circle in $\mathbb{C}$ with complex multiplication. The following is an algebraic presentation $\langle X|R_1 \cup R_2\rangle$ of $\mathbb{S}$:

- $X := \{x_{r,s} : (r,s) \in \mathbb{R}^2 \setminus \{0\}\}$,
- $R_1 := \{x_{r,s} \circ x_{a,b}^{-1} : (r,s),(a,b) \neq 0 \wedge rb = sa \wedge ar > 0\}$,
- $R_2 := \{x_{r,s} \circ x_{a,b} \circ x_{u,v}^{-1} : (r,s),(a,b),(u,v) \neq 0 \wedge$
  $\wedge\, r^2+s^2 = 1 \wedge a^2+b^2 = 1 \wedge u = ra-sb \wedge v = rb+sa\}$.

Intuitively, R_1 yields the identification of (generators whose indices represent) points lying on the same half line through the origin. In particular, every $x_{r,s}$ is 'equal' (by virtue of R_1) to some $x_{a,b}$ of 'length' $a^2+b^2 = 1$. To these elements, R_2 applies and identifies $x_{r,s} \circ x_{a,b}$ with $x_{u,v}$ whenever, over the complex numbers, it holds $(r+is)\cdot(a+ib) = u+iv$. □

Clearly, the presentation of a group need not be unique; e.g. we also have $\mathbb{S} \cong \langle Y|R_2\rangle$ where $Y = \{x_{r,s} : r^2+s^2 = 1\}$. Here is a further algebraic presentation of the same group:

Example 13. Let $X := \{x_t : t \in \mathbb{R}\}$, $R := \{x_t = x_{t+1}, x_t x_s = x_{t+s} : t,s \in \mathbb{R}\}$. Then $\langle X|R\rangle$ is a 1D (!) algebraic presentation of the group $([0,1),+)$ isomorphic to $(\mathbb{S},\times)$ via $t \mapsto \exp(2\pi i t + ic)$ for any $c \in \mathbb{R}$. Yet none of these isomorphisms is BSS-computable! □

Next consider the group $\mathrm{SL}_2(\mathbb{R})$ of real 2×2 matrices A with $\det(A) = 1$. A straightforward algebraic presentation of it is given as $\langle X|R\rangle$ where $X := \{x_{(a,b,c,d)} : ad-bc = 1\}$ and $R := \{x_{(a,b,c,d)}x_{(q,r,s,t)} = x_{(u,v,w,z)} : u = aq+bs \wedge v = ar+bt \wedge w = cq+ds \wedge z = cr+dt\}$. Here as well as in the above examples, any group element $\overline{w} \in \langle X\rangle$ is equivalent (w.r.t. R) to an appropriate *single* generator $x \in X$. This is different for the following alternative, far less obvious algebraic presentation:

Example 14 (Weil Presentation of $\mathrm{SL}_2(\mathbb{R})$*).* For each $b \in \mathbb{R}$, write

$$U(b) := \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad V := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad S(a) := V \cdot U(\tfrac{1}{a}) \cdot V \cdot U(a) \cdot V \cdot U(\tfrac{1}{a}) \in \mathrm{SL}_2(\mathbb{R}) \ .$$

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 [Lan85], $\langle X|R\rangle$ is isomorphic to $SL_2(\mathbb{R})$ under the natural homomorphism. □

In all the above cases, the word problem — in Example 12 basically the question whether $(r,s) = (1,0)$ and in Example 13 whether $t = 0$ — is decidable. We next illustrate that, in the real case, different presentations of the same group may affect solvability of the word problem.

Example 15. The following are presentations $\langle X|R\rangle$ of $(\mathbb{Q},+)$:

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

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

Case b) yields an algebraic presentation, a) is not even algebraically generated but c) is. The word problem is decidable for a): e.g. by effective embedding into $(\mathbb{R},+)$; and so is it for b) although not for c): $x_t = 1 \Leftrightarrow P(t) = 0$ 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. □

Example 16. (Undecidable) real membership "$t \in \mathbb{Q}$" is reducible to the word problem of an algebraically presented real group: Consider $X = \{x_r : r \in \mathbb{R}\}$, $R = \{x_{nr} = x_r, x_{r+k} = x_k : r \in \mathbb{R}, n \in \mathbb{N}, k \in \mathbb{Z}\}$. Then $x_r = x_0 \Leftrightarrow r \in \mathbb{Q}$; also, $R \subseteq \mathbb{R}^2$ is decidable because $\mathbb{Z} \subseteq \mathbb{R}$ is. □

This however does not establish BSS-*hardness* of the real word problem because $\mathbb{Q}$ is provably easier than the BSS Halting Problem $\mathbb{H}$ [MZ05]. On the other hand, without the restriction to algebraically presented groups (and thus parallel to Example 6), it is easy to find a real group with BSS-hard word problem:

Example 17. Let $X := \{x_r, y_r : r \in \mathbb{R}\} \uplus \{s,t\} \cong (\mathbb{R} \uplus \{\infty\}) \times \{1,2\}$. and $R := \{\overline{v_{\overline{r}}} = \overline{w_{\overline{r}}} : \overline{r} \in \mathbb{H}\}$ where, for $\overline{r} \in \mathbb{R}^d$, we abbreviated $\overline{v_{\overline{r}}} := x_{r_d}^{-1} \cdots x_{r_1}^{-1} \cdot s \cdot x_{r_1} \cdots x_{r_d}$ and $\overline{w_{\overline{r}}} := y_{r_d}^{-1} \cdots y_{r_1}^{-1} \cdot t \cdot y_{r_1} \cdots y_{r_d}$. In $G := \langle X|R\rangle$, it is $\overline{v_{\overline{r}}} = \overline{w_{\overline{r}}}$ iff $\overline{r} \in \mathbb{H}$; compare Fact 38. Therefore, $\overline{r} \mapsto \overline{v_{\overline{r}}} \cdot \overline{w_{\overline{r}}}$ constitutes a reduction from $\mathbb{H}$ to the word problem in G. However, G has just *semi*-decidable relations. □

The construction of an *algebraically presented* group with BSS-complete word problem in Section 4 is the main contribution of the present work.

3.4 Reducibility *to* the Real Halting Problem

We first show that, parallel to Fact 5a), the word problem for any algebraically enumerated real group is not harder than the BSS Halting Problem.

Theorem 18. *Let $G = \langle X|R\rangle$ denote a algebraically enumerated real group. Then the associated word problem is BSS semi-decidable.*

Recall that semi-decidability of $A \subseteq \mathbb{K}^\infty$ (that is, being a halting set) is equivalent to recursive enumerability

$$A = \text{range}(f) \quad \text{for some computable, partial function } f :\subseteq \mathbb{K}^\infty \to \mathbb{K}^\infty$$

in the Turing ($\mathbb{K} = \mathbb{F}_2$) as well as the BSS ($\mathbb{K} = \mathbb{R}$) model; in the latter case by virtue of TARSKI's quantifier elimination [Mic91].

Lemma 19. *For $Y \subseteq \mathbb{R}^\infty$, it holds: If Y is (semi-)decidable, then so is $\langle Y\rangle$.*

Proof. Given a string $\overline{w} = (y_1, \ldots, y_k) \in \mathbb{R}^k$, consider all 2^{k-1} partitions of $\overline{w}$ into non-empty subwords. For each subword, decide or semi-decide whether it belongs to $Y \cup Y^{-1}$. Accept iff, for at least one partition, all its subwords succeed. □

[5] That is, as opposed to a Banach space basis, every vector admits a representation as linear combination of *finitely* many out of these (here uncountably many) base elements.

Proof (Theorem 18). By Definition 4b+c), $\bar{w} \equiv 1 \Leftrightarrow \bar{w} \in \langle R \rangle_{\mathrm{n}}$, that is, if and only if

$$\exists n \in \mathbb{N}\ \exists \bar{x_1}, \ldots, \bar{x_n} \in \langle X \rangle\ \exists \bar{r_1}, \ldots, \bar{r_n} \in \langle R \rangle : \quad \bar{w} = \bar{x_1}\bar{r_1}\bar{x_1}^{-1} \cdot \bar{x_2}\bar{r_2}\bar{x_2}^{-1} \cdots \bar{x_n}\bar{r_n}\bar{x_n}^{-1} \quad . \quad (3)$$

Since both X and R were required to be semi-decidable, same holds for $\langle X \rangle$ and $\langle R \rangle$. This yields semi-decidability of (3). Indeed, let $f, g :\subseteq \mathbb{R}^\infty \to \mathbb{R}^\infty$ be BSS-computable with $\langle X \rangle = \mathrm{range}(f)$ and $\langle R \rangle = \mathrm{range}(g)$; 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 $\langle W \rangle_{\mathrm{n}}$. □

4 Reduction *from* the Real Halting Problem

This section proves the main result of the paper and continuous counterpart to Fact 5b): The word problem for algebraically presented real groups is in general not only undecidable (cf. Example 16) in the BSS model but in fact as hard as the real Halting Problem.

Theorem 20. *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 $\mathcal{H}$.*

We first (Sections 4.1) review some basics from group theory in the context of presented groups; specifically free products, HNN extensions and BRITTON's Lemma. As in the classical reduction from the Turing Halting Problem H to finitely presented groups in [LS77, SECTION §IV.7] (based on ideas of HIGMAN [Hig61] and VALIEV [Val69]), these powerful tools permit a more elegant and abstract treatment than the elementary approach pursued in, e.g., [Rot95, CHAPTER 12]. A second major ingredient, *benign* subgroups are recalled and generalized to our effective real setting in Section 4.3. This requires particular care since many properties heavily exploited in the discrete case (e.g., that the homeomorphic image of a finitely generated group is again finitely generated) are not immediately clear how to carry over to the reals (Section 4.2). For instance, a proof for the classical result may exploit MATIYASEVICH's famous solution of Hilbert's Tenth Problem, namely a Diophantine formulation of H [Mat70]. This form can be transformed into a straight line program and further on into a group theoretic one by virtue of HIGMAN's concept of benign subgroups. Our general proof strategy is conceptually similar but necessarily quite different in detail. Specifically, lacking a real Diophantine characterization of $\mathbb{H}$ (recall Example 1), Section 4.4 has to proceed differently, namely by describing each *fixed* computational path of a BSS machine as a real straight line program, and obtains from that a representation as an *effectively* benign real group. In the final step (Section 4.5), all these groups and their embeddings are joined into one single, algebraically presented one.

4.1 Basics from Group Theory and Their Presentations

This subsection briefly recalls some constructions from group theory and their properties which will heavily be used later on. For a more detailed exposition as well as proofs of the cited results we refer to the two textbooks [LS77, Rot95]. Our notational emphasis for each construction and claim lies on the particular group *presentation* under consideration — for two reasons: First and as opposed to the discrete case[4], different presentations of the same group may heavily affect its effectivity properties (Example 15). And second, sometimes there does not seem to be a 'natural' choice for a presentation (Remark 22, Footnote 6).

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

Definition 21. *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, that is, makes Equation (2) commute.*
A realization of an isomorphism ϕ is a realization of ϕ as a homomorphism.

In the above notation, $\langle \psi'(X) \big| S\rangle$ is a presentation of the subgroup $\psi(G)$ of H. For an embedding ψ, G is classically isomorphic to $\psi(G)$; Lemma 33 below contains a computable variation of this fact.

Remark 22. The intersection $A \cap B$ of two subgroups A, B of G is again a subgroup of G. For presented sub-groups $A = \langle U|R\rangle$ and $B = \langle V|R\rangle$ of $G = \langle X|R\rangle$ however, $\langle U \cap V|R\rangle$ is in general *not* a presentation of $A \cap B$.

Definition 23 (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*

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

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

In many situations one wants to identify certain elements of a free product of groups. These are provided by two basic constructions: *amalgamation* and *Higman-Neumann-Neumann* (or shortly HNN) extension, see [HNN49, LS77, Rot95]. The intuition behind the latter is nicely illustrated, e.g., in [Rot95, FIGURE 11.9].

Definition 24 (Amalgamation). *Let $G = \langle X|R\rangle$, $H = \langle Y|S\rangle$ with $X \cap Y = \emptyset$. Let $A = \langle V|R\rangle$ and $B = \langle W|S\rangle$ be respective subgroups and $\phi' : \langle V\rangle \to \langle W\rangle$ realization of an isomorphism $\phi : A \to B$. The free product of G and H* amalgamating *the subgroups A and B via ϕ is the presented group*

$$\langle G * H \mid \phi(a) = a \forall a \in A\rangle \quad := \quad \big\langle X \cup Y \mid R \cup S \cup \{\phi'(\bar{v})\bar{v}^{-1} : \bar{v} \in V\}\big\rangle \ . \tag{4}$$

Definition 25 (HNN Extension). *Let $G = \langle X|R\rangle$, $A = \langle V|R\rangle, B = \langle W|R\rangle$ 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*

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

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 $A_i, B_i \subseteq G$, $i \in I$.

Both HNN extensions and free products with amalgamation 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 [LS77, CHAPTER IV] or [Rot95, CHAPTER 11].

Fact 26 (Higman-Neumann-Neumann). *Let $G^* := \langle G; t|ta = \phi(a)t \forall a \in A\rangle$ be a HNN extension of G. Then, identity $g \mapsto g$ is an embedding of G into G^*.* □

Fact 27 (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 $(g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n)$ with $n \in \mathbb{N}$, $g_i \in G$, $\varepsilon_i \in \{-1, 1\}$. 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 it holds $g_0 \cdot t^{\varepsilon_1} \cdot g_1 \cdots t^{\varepsilon_n} \cdot g_n \neq 1$ in G^*.* □

Fact 28 (Normal Form). *Let $P := \langle G * H | \phi(a) = a \forall A \rangle$ denote a free product with amalgamation. Consider $c_1, \ldots, c_n \in G * H$, $n \in \mathbb{N}$, such that*

- *each c_i is either in G or in H;*
- *consecutive c_i, c_{i+1} come from different factors;*
- *if $n > 1$, then no c_i is in A nor B;*
- *if $n = 1$, then $c_1 \neq 1$.*

Then, $c_1 \cdots c_n \neq 1$ in P. □

4.2 First Effectivity Considerations

Regarding finitely generated groups, the cardinalities of the sets of generators (that is their *ranks*) add under free products [LS77, COROLLARY §IV.1.9]. Consequently, they can straight forwardly be bounded under both HNN extensions and free products with amalgamation. Similarly for real groups, we have easy control over the *dimension N* of set of generators according to Definition 9:

Observation 29. *For groups $G_i = \langle X_i | R_i \rangle$ with $X_i \subseteq \mathbb{R}^N$ for all $i \in I \subseteq \mathbb{R}$, the free product*

$$\mathop{\ast}_{i \in I} G_i \quad = \quad \left\langle \bigcup_{i \in I} (X \times \{i\}) \;\middle|\; \bigcup_{i \in I} (R \times \{i\}) \right\rangle$$

is of dimension at most $N + 1$. In the countable case $I \subseteq \mathbb{N}$, the dimension can even be achieved to not grow at all: by means of a bicomputable bijection $\mathbb{R} \times \mathbb{N} \to \mathbb{R}$ like $(x, n) \mapsto \langle \lfloor x \rfloor, n \rangle + (x - \lfloor x \rfloor)$.
Similarly for free products with amalgamation and for HNN extensions.

Moreover, free products, HNN extensions, and amalgamations of algebraically generated/enumerated/presented groups are, under reasonable presumptions, again algebraically generated/enumerated/presented:

Lemma 30. *a) Let $G_i = \langle X_i | R_i \rangle$ for all $i \in I \subseteq \mathbb{N}$. If I is finite and each G_i algebraically generated/enumerated/presented, then so is $\mathop{\ast}_{i \in I} G_i$.*
Same for $I = \mathbb{N}$, provided that G_i is algebraically generated/enumerated/presented uniformly in *i.*

b) Let $G = \langle X | R \rangle$ and consider the HNN extension $G^* := \langle G; (t_i)_{i \in I} \,|\, t_i a = \phi_i(a) t_i \forall a \in A_i \forall i \in I \rangle$ with respect to a family of isomorphisms $\phi_i : A_i \to B_i$ between subgroups $A_i = \langle V_i | R \rangle, B_i = \langle W_i | R \rangle$ for $V_i, W_i \subseteq \langle X \rangle$, $i \in I$.
Suppose that I is finite, each G_i is algebraically enumerated/presented, $V_i \subseteq \mathbb{R}^\infty$ is semi-/decidable, and finally each ϕ_i is effective as a homomorphism; then G^* is algebraically enumerated/presented as well.
Same for $I = \mathbb{N}$, provided that the V_i are uniformly *semi-/decidable and effectivity of the ϕ_i holds* uniformly.

c) Let $G = \langle X | R \rangle$ and $H = \langle Y | S \rangle$; let $A = \langle V | R \rangle \subseteq G$ and $B = \langle W | S \rangle \subseteq H$ be subgroups with $V \subseteq \langle X \rangle$, $W \subseteq \langle Y \rangle$, $V \subseteq \mathbb{R}^\infty$ semi-/decidable, and $\phi : A \to B$ an isomorphism and effective homomorphism. Then, their free product with amalgamation (4) is algebraically enumerated/presented whenever G and H are.

Remark 31. *Uniform* (semi-)decidability of a family $V_i \subseteq \mathbb{R}^\infty$ of course means that every V_i is (semi-)decidable not only by a corresponding BSS-machine $\mathbb{M}_i$, but all V_i by one common machine $\mathbb{M}$; similarly for *uniform* computability of a family of mappings. By virtue of (the proof of) [Cuc92, THEOREM 2.4], a both necessary and sufficient condition for such uniformity is that the real constants employed by the $\mathbb{M}_i$ can be chosen to all belong to one common finite field extension $\mathbb{Q}(c_1, \ldots, c_k)$ over the rationals. □

Recall (Observation 8) that a homomorphism between finitely generated groups is automatically effective and, if injective, has decidable range and effective inverse. For real groups however, in order to make sense out of the prerequisites in Lemma 30b+c), we explicitly have to specify the following

Definition 32. *An homomorphism $\psi : \langle X|R\rangle \to \langle Y|S\rangle$ of presented real groups is called an* effective homomorphism *if it admits a BSS-computable realization $\psi' : X \to \langle Y\rangle$ in the sense of Definition 21.*

For ψ to be called an effective embedding*, it must not only be an effective homomorphism and injective; but ψ' is also required to be injective and have decidable image $\psi'(X)$ plus a BSS-computable inverse $\chi' : \psi'(X) \subseteq \langle Y\rangle \to X$.*

Effective embeddings arise in Lemmas 33 and 36. For an injective effective homomorphism ϕ as in Lemma 30c) on the other hand, a realization needs not to be injective; for instance, ϕ' might map two equivalent (w.r.t. the relations R) yet distinct elements to the same image word.

Proof (Lemma 30).

a) If X_i is decidable for each $i \in I$, I finite, then so is $\bigcup_{i\in I}(X_i \times \{i\})$; same for semi-decidable/decidable R_i. *Uniform* (semi-)decidability of each X_i means exactly that $\bigcup_{i\in\mathbb{N}}(X_i \times \{i\})$ is (semi-)decidable.
b) The set of generators of the HNN extension is decidable as in a). The additional relations $\{\phi_i'(\overline{v})t_i\overline{v}^{-1}t_i^{-1} : \overline{v} \in V_i\}$ are semi-/decidable since, by presumption, V_i is and $\phi_i' : \langle V_i\rangle \to \langle W_i\rangle$ is computable. Uniformity enters as in a).
c) Similarly. □

Lemma 33. *Let $\psi : G = \langle X|R\rangle \to \langle Y|S\rangle = K$ denote an effective embedding.*

a) There is an effective embedding $\chi : \psi(G) \to G$ (i.e. we have an effective isomorphism).
b) If $V \subseteq \langle X\rangle$ is decidable, then the restriction $\psi|_H$ to $H = \langle V|R\rangle \subseteq G$ is an effective embedding again.
c) If G is algebraically generated and K algebraically presented then $\psi(G)$ is algebraically presented as well.

Proof. a) Let $\psi' : X \to \langle Y\rangle$ denote the effective realization of ψ with inverse χ' according to Definition 32. The unique extension of ψ' to a homomorphism has image $\psi'(\langle X\rangle) = \langle\psi'(X)\rangle$. Similar to Lemma 19 we can decide, given $\overline{w} \in \langle Y\rangle$, whether $\overline{w} \in \psi'(\langle X\rangle)$. Moreover if so, we obtain a partition $\overline{w} = (\overline{v_1}, \ldots, \overline{v_\ell})$ with $\overline{v_i} \in \psi'(X)$. Then calculating $x_i := \chi'(\overline{v_i}) \in X$ yields a computable extension of χ' to a homomorphism on $\psi'(\langle X\rangle)$ which satisfies injectivity, has decidable image and ψ' as inverse. Moreover χ' maps S-cosets to R-cosets: Take $\overline{v_1}, \overline{v_2} \in \psi'(\langle X\rangle)$ with $\overline{v_1}/S = \overline{v_2}/S$; then $\overline{u_i} := \chi'(\overline{v_i})$ have $\overline{v_i} = \psi'(\overline{u_i})$ and thus, since ψ' makes Equation (2) commute by presumption, $\overline{v_1}/S = \psi(\overline{u_1}/R) = \psi(\overline{u_2}/R) = \overline{v_2}/S$; now injectivity of ψ implies $\overline{u_1}/R = \overline{u_2}/R$.
b) The range $\psi'(V)$ of the restriction $\psi'|_V$ coincides with $\chi'^{-1}(V) \cap \langle\psi'(X)\rangle$. The first term is decidable since χ' is computable and V decidable; the second term is decidable by Definition 32 and Lemma 19.
c) Becomes clear by staring at $\psi(G) = \langle\psi'(X)|S\rangle$. □

4.3 Benign Embeddings

The requirement in Lemma 30b+c) that the subgroup(s) A be recursively enumerable or even decidable, is of course central but unfortunately violated in many cases. For instance, a subgroup of a finitely presented group in general need not even be finitely generated: Consider, e.g., the *commutator* $[G,G] := \langle\{uvu^{-1}v^{-1} : u,v \in G\}\rangle$ of the free group $G = \langle\{a,b\}\rangle$ and compare Remark on p.177 of [LS77]. Similarly the algebraically presented real group

$(\mathbb{R},+)$ has a subgroup (Example 15a) which is not algebraically generated. Nevertheless, both can obviously be effectively embedded into a, respectively, finitely presented and an algebraically presented group. This suggests the notion of *benign* subgroups, in the classical case (below, Item a) introduced in [Hig61]. Recall that there, effectivity of an embedding drops off automatically.

Definition 34. *a) Let X be finite, $V \subseteq \langle X\rangle$. The subgroup $A = \langle V|R\rangle$ of $G = \langle X|R\rangle$ is (classically)* benign in *G if the HNN extension $\langle X;t\,|\,ta = at\forall a \in A\rangle$ can be embedded into some finitely presented group $K = \langle Y|S\rangle$.*

b) 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 in *G if the HNN extension $\langle G;t\,|\,ta = at\forall a \in A\rangle$ admits an effective embedding into some algebraically presented group $K = \langle Y|S\rangle$.*

c) Let $I \subseteq \mathbb{N}$. A family $(A_i)_{i\in I}$ of subgroups of G is uniformly effectively benign in *G if, in the sense of Remark 31, there are groups K_i uniformly algebraically presented and uniformly effective embeddings $\phi_i : \langle G;t_i|t_ia_i = a_it_i\forall a_i \in A_i\rangle \to K_i$.*

The benefit of benignity is revealed in the following

Remark 35. In the notation of Definition 34b), if A is effectively benign in G then the word problem for A is reducible to that for K: Fact 26.
Moreover in this case, the *membership problem* for A in G — that is the question whether given $\overline{x} \in \langle X\rangle$ is equivalent (w.r.t. R) to an element of A — is also reducible to the word problem for K: According to Fact 27, $a := \overline{x}/R$ satisfies $\quad t\cdot a\cdot t^{-1}\cdot a^{-1} = 1 \Leftrightarrow a \in A$. $\square$

We now collect some fundamental properties frequently used later on. They extend corresponding results from the finite framework. Specifically, Lemma 36b) generalizes [LS77, LEMMA §IV.7.7(i)] and Claims d+e) generalize [LS77, LEMMA §IV.7.7(ii)].

Lemma 36. *a) Let $A = \langle V|R\rangle \subseteq H = \langle W|R\rangle \subseteq G = \langle X|R\rangle$ denote a chain of sub-/groups with $V \subseteq \langle W\rangle$ and $W \subseteq \langle X\rangle$. If W is decidable and A effectively benign in G, then it is also effectively benign in H.*

b) If $G = \langle X|R\rangle$ is algebraically presented and subgroup $A = \langle V|R\rangle$ has decidable generators $V \subseteq \langle X\rangle$, then A is effectively benign in G.

c) If A is effectively benign in G and $\phi : G \to H$ an effective embedding, then $\phi(A)$ is effectively benign in $\phi(G)$.

d) Let A and B be effectively benign in algebraically presented G. Then $A \cap B$ admits a presentation effectively benign in G.

e) Let A, B, G as in d); then $\langle A \cup B\rangle_G$ admits a presentation[6] effectively benign in G.

f) Let $(A_i)_{i\in I}$ be uniformly effectively benign in G (Definition 34c). Then $\langle \bigcup_{i\in I} A_i\rangle$ admits a presentation effectively benign in G.

The above claims hold uniformly in that the corresponding effective embeddings do not introduce new real constants.

Proof. a) Let ψ be an effectively realizable embedding of the HNN extension $\langle X;t|ta = \phi(a)t\forall a \in A\rangle$ into some algebraically presented $K = \langle Y|S\rangle$. Since $W \cup \{t\}$ is decidable, Lemma 33b) asserts the restriction of ψ to yield an effective embedding of the HNN extension $\langle W;t|ta = \phi(a)t\forall a \in A\rangle$ into K.

b) The identity being an effectively realizable embedding (X is decidable, now apply Lemma 33b), it suffices to observe that the HNN extension

$$K \quad := \quad \langle G;t\,|\,at = ta\forall a \in A\rangle \quad = \quad \langle X;t\,|\,R \cup \{\overline{vt} = t\overline{v}\forall \overline{v} \in V\}\rangle$$

is algebraically presented itself. Indeed, X, R, and the additional relations parametrized by V are decidable by presumption.

[6] possibly different from $\langle V \cup W|R\rangle$

c) The presented HNN extension under consideration,

$$\langle \phi'(X); s \,|\, \phi'(\overline{v})s = s\phi'(\overline{v}) \forall \overline{v} \in V \rangle \ , \tag{5}$$

is the image under ϕ of $\langle G; t | at = ta \forall a \in A \rangle$ by extending $\phi'(t) := s$. The latter HNN extension by presumption embeds into some (finite-dim.) algebraically presented K via some effective ψ. According to Lemma 33a), ϕ admits an effective inverse. Hence the composition $\psi \circ \phi^{-1}$ consitutes the desired effective embedding of (5) into K.

d) By assumption there exist two algebraically presented groups $K = \langle Y|S\rangle$ and $L = \langle Z|T\rangle$ together with realizations $\phi' : X \cup \{r\} \to \langle Y \rangle$, $\psi' : X \cup \{r\} \to \langle Z \rangle$ of effective embeddings

$$\begin{aligned} \phi \ : G_A \ &:= \ \langle G; r | ar = ra \forall a \in A \rangle \ = \ \langle X; r \,|\, R \cup \{\, \overline{v}r = r\overline{v} : \overline{v} \in V \ \} \rangle \ \to K \ = \ \langle Y|S \rangle \\ \psi \ : G_B \ &:= \ \langle G; r | br = rb \forall b \in B \rangle \ = \ \langle X; r \,|\, R \cup \{\overline{w}r = r\overline{w} : \overline{w} \in W\} \rangle \ \to L \ = \ \langle Z|T \rangle \ . \end{aligned}$$

We shall realize an embedding χ of the HNN extension $G_C := \langle G; r | cr = rc \forall c \in C \rangle$ into an algebraically presented group for the presentation[7] $C := \big\langle \{\overline{w} \in \langle W \rangle : \overline{w}/R \in A\} \,\big|\, R \big\rangle$ for $A \cap B$. To this end observe that $\phi(G) = \langle \phi'(X) | S \rangle$ and $\psi(G) = \langle \psi'(X) | T \rangle$ are subgroups of K and L, respectively, and isomorphic due to Fact 26 with isomorphism[7] $\phi \circ \psi^{-1} : \psi(G) \to \phi(G)$ realized by $\phi' \circ \psi'^{-1}$ according to Lemma 33. Definition 24 is thus applicable and we are entitled to consider the free group with amalgamation

$$\begin{aligned} P &:= \big\langle K * L \,\big|\, \phi\big(\psi^{-1}(\ell)\big) = \ell \forall \ell \in \psi(G) \big\rangle \\ &= \big\langle Y \cup Z \,\big|\, S \cup T \cup \{\phi'\big(\psi'^{-1}(\overline{z})\big) = \overline{z} : \overline{z} \in \psi'(X)\} \big\rangle \ . \end{aligned} \tag{6}$$

P is algebraically presented because of Lemma 30c). Moreover $\phi(G) = \psi(G)$ in P according to (6). Also, $s := \phi'(r)$ commutes exactly with $\phi(A)$ and $t := \psi'(r)$ exactly with $\psi(B)$, so $s \cdot t$ commutes exactly with $\phi(A) \cap \psi(B)$. Therefore, $\chi' : X \cup \{r\} \to \langle Y \cup Z \rangle$, $x \mapsto \psi'(x)$, $r \mapsto s \cdot t$ respects cosets in the sense of Equation (2) and thus realizes an embedding $\chi : \langle G; r | cr = rc \forall c \in C \rangle \to P$ as desired.

e) With notations as in d), it holds

$$\begin{aligned} \psi(\langle A \cup B \rangle_G) \ = \ \phi(\langle A \cup B \rangle_G) \ &= \ \langle \phi(A) \cup \phi(B) \rangle_P \ = \ \langle \phi(A) \cup \psi(B) \rangle_P \\ &= \ \langle \phi(r \cdot G \cdot r^{-1}) \cup \psi(r \cdot G \cdot r^{-1}) \rangle_P \ \cap \ \phi(G) \ ; \end{aligned}$$

the first line because ϕ and ψ are injective homomorphisms coinciding on G; the second because A and only A commutes with r in G_A due to Britton's Lemma (Fact 27), similarly for B in G_B. Now $\phi(G)$ is algebraically presented due to Lemma 33c) and thus effectively benign in P by Claim b). Similarly, $\langle \phi(r \cdot G \cdot r^{-1}) \cup \psi(r \cdot G \cdot r^{-1}) \rangle_P$ has decidable generators and is thus effectively benign in P as well. Claim d) now asserts effective benignty of $\phi(\langle A \cup B \rangle)$ in P; and therefore also in $\phi(G) \subseteq P$ according to Claim a) combined with Lemma 33c). Claim c) combined with Lemma 33a) finally yields effective benignty of $\langle A \cup B \rangle$ in G.

f) Let $(\phi_i')_{i \in I}$ denote the uniformly computable realizations of embeddings $\phi_i : G_i := \langle G; r | ar = ra \forall a \in A_i \rangle \to K_i$. Fix $j \in I$. Similar to Equation 6) and the proof of e), we have

$$\begin{aligned} \phi_j\Big(\big\langle \mathop{\ast}_{i \in I} A_i \big\rangle_G\Big) \ &= \ \Big\langle \bigcup_{i \in I} \phi_i\big(r \cdot G \cdot r^{-1}\big) \Big\rangle_P \ \cap \ \phi_j(G), \\ P \ &:= \ \Big\langle \mathop{\ast}_{i \in I} K_i \,\Big|\, \phi_i\big(\phi_j^{-1}(\ell)\big) = \ell \forall \ell \in \phi_j(G) \forall i \in I \Big\rangle \end{aligned}$$

where (by uniformity, see Lemma 30) P and $\phi_j(G)$ are algebraically presented, and $\big\langle \bigcup_{i \in I} \phi_i(r \cdot G \cdot r^{-1}) \big\rangle_P$ has decidable generators of bounded dimension, compare Observation 29. □

We are now ready to start with the main part of the proof.

[7] Notice the arbitrarily broken symmetry between the groups/embeddings (A, ϕ) and (B, ψ) involved.

4.4 Dealing with a single path set

Consider the real halting problem $\mathbb{H} \subseteq \mathbb{R}^\infty$ together with an appropriate BSS machine $\mathbb{M}$ which accepts exactly inputs $\bar{r}$ belonging to $\mathbb{H}$ and stalls for all others. The accepting paths of $\mathbb{M}$ admit an effective enumeration (γ_n), $n \in \mathbb{N}$. Here, each path γ_n is described by a finite sequence (of length $D = D(\gamma_n) \in \mathbb{N}$, say) of primitive arithmetic operations, assignments, and comparisons performed along it. Each such path γ gives rise to the (possibly empty) set $\mathbb{A}_\gamma \subseteq \mathbb{R}^d$, $d = d(\gamma) \in \mathbb{N}$, of inputs $\bar{r} \in \mathbb{R}^d$ on which $\mathbb{M}$ follows exactly this path. Both functions $n \mapsto d(\gamma_n)$ and $n \mapsto D(\gamma_n)$ are computable.

A computational path γ together with an input $(r_1, \ldots, r_d)$ following it give rise to a sequence $r_{d+1}, \ldots, r_D \in \mathbb{R}$ of intermediate results, each one being the result from a composition of at most two previous ones. For instance, $r_i = r_j \pm r_k$ with $d < i \leq D$ and $1 \leq j, k < i$; or $r_i = \alpha$ for some machine constant $\alpha \in \mathbb{R}$ of $\mathbb{M}$; branches take the form "$r_i \geq 0$?".The advantage of this description of γ as a set $\mathbb{B}_\gamma \subseteq \mathbb{R}^D$ of $(r_1, \ldots, r_d, r_{d+1}, \ldots, r_D)$ is that each intermediate result r_i may be accessed several times but gets assigned only once.

In view of Remark 35, our goal is to write $\mathbb{A}_{\gamma_n}$ as a subgroup U_{γ_n} effectively benign in a suitable algebraically presented group such that membership to $\mathbb{A}_{\gamma_n}$ is reducible to that of U_{γ_n}; with the additional constraint that all constructions work *uniformly* in n — in fact using only constants already present in $\mathbb{M}$; compare Remark 31 and see Footnote 9. However for notational convenience, n (and thus also γ, d, D) will be kept fixed and occasionally omitted throughout this subsection. They reappear in Section 4.5 when the subgroups U_{γ_n}, $n \in \mathbb{N}$, are finally glued together.

Definition 37. *Let*

$$X \;:=\; \{x_{(i,s)} : s \in \mathbb{R}, i \in \mathbb{N}\} \cup \{y\} \;\cong\; (\mathbb{R} \times \mathbb{N}) \cup \{\infty\}, \quad G \;:=\; \langle X \rangle$$

denote a free group with subgroups

$$H_{\leq d} := \langle \{y, x_{(i,s)} : s \in \mathbb{R}, i \leq d\} \rangle \quad \textit{and} \quad H_{>d} := \langle x_{(i,s)} : s \in \mathbb{R}, i > d \rangle \;\; .$$

Furthermore consider the subgroups

$$U_\gamma \;:=\; \langle \bar{w}_{\bar{r}} : \bar{r} \in \mathbb{A}_\gamma \rangle \quad \textit{and} \quad V_\gamma \;:=\; \langle \bar{w}_{\bar{s}} : \bar{s} \in \mathbb{B}_\gamma \rangle$$

with the abbreviation $\bar{w}_{(r_1,\ldots,r_k)} := x_{(k,r_k)}^{-1} \cdots x_{(1,r_1)}^{-1} \cdot y \cdot x_{(1,r_1)} \cdots x_{(k,r_k)}$ *for* $r_1, \ldots, r_k \in \mathbb{R}$.

The reason for the complicated definition of $\bar{w}$ (instead of, e.g., $\bar{v}_{\bar{r}} := x_{(1,r_1)} \cdots x_{(k,r_k)}$) lies in the following

Fact 38. *The words* $\bar{w}_{\bar{r}}$, $\bar{r} \in \mathbb{A}_\gamma$, *are* Nielsen-reduced—*compare* [LS77, p.223]—*and thus freely generate* U_γ [LS77, PROPOSITION §I.2.5]. *In particular,* $\bar{w}_{\bar{r}} \in U_\gamma$ *iff* $\bar{r} \in \mathbb{A}_\gamma$.

Theorem 39. *U_γ is (or rather, has a presentation) effectively benign in algebraically presented G.*

The proof of this theorem proceeds in several steps. Let $(o_{d+1}, \ldots, o_D)$ denote the arithmetic operations, assignments, and branched tests performed on the path γ; cf. left column of Figure 1. For each such o, define a subgroup W_o of G as in the middle column of Figure 1. Since the generators involved are free, we have

Lemma 40. *It holds*

$$V_\gamma \;=\; \bigcap\nolimits_{i=d+1}^{D} W_{o_i}$$

and

$$U_\gamma \;=\; \langle V_\gamma \cup H_{>d} \rangle \;\cap\; H_{\leq d}$$

Proof. Let us focus on the second claim, the argument for the first one proceeds similarly. Inclusion "$U_\gamma \subseteq \langle V_\gamma \cup H_{>d}\rangle \cap H_{\leq d}$" holds since to every word $\bar{w}_{\bar{r}} \in U_\gamma$, $(r_1,\ldots,r_d) \in \mathbb{A}_\gamma$, there corresponds an extension $\bar{w}_{\bar{s}} \in V_\gamma$ with $\bar{s} = (r_1,\ldots,r_d,r_{d+1},\ldots,r_D) \in \mathbb{B}_\gamma$; and the symbols $x_{(i,r)}$ with $i > d$ can be cancelled from $\bar{w}$ by means of $H_{>d}$, thus transforming into an element of $H_{\leq d}$.
For the reverse inclusion, observe that the words $\bar{w}_{\bar{s}} \in V_\gamma$ equivalent to a word in $H_{\leq d}$ are exactly those with symbols $x_{(i,r)}$, $i > d$, removed and with $i \leq d$ unmodified. □

We will now show that the W_o are effectively benign in G; hence Lemma 36d) establishes the same for V_γ. Since the respective sets of generators are easily decidable, Lemma 36b) yields also $H_{\leq d}$ and $H_{>d}$ effectively benign in G. So by Lemma 36e+d), Theorem 39 follows.

Definition 41. *Let C denote the infinite (in fact uncountable) HNN extension*

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

with base G and stable letters $a_{(i,t)}$, $m_{(i,t)}$ as above. Here, $\phi_{(i,t)}, \psi_{(i,t)} : G \to G$ denote the isomorphisms[8]

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

Intuitively in C, commuting a stable letter $a_{(i,t)}$ 'causes' a real addition in the sense that $a_{(i,t)} \cdot x_{(i,s)} \cdot a_{(i,t)}^{-1} = x_{(i,s+t)}$. Furthermore, since $a_{(i,t)}$ commutes with all $x_{(j,s)}$, $j \neq i$, it holds

$$a_{(i,t)} \cdot \bar{w}_{(r_1,\ldots,r_i,\ldots,r_D)} \cdot a_{(i,t)}^{-1} \quad = \quad \bar{w}_{(r_1,\ldots,r_i+t,\ldots,r_D)} \ ; \tag{7}$$

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

Lemma 42. *For each operation o and its corresponding subgroup L_o of C as in Figure 1, it holds $W_o = G \cap L_o$, and W_o is effectively benign in G.*

Proof. $x_i \leftarrow \alpha$[9]**:** The inclusion $W_{(x_i \leftarrow \alpha)} \subseteq G \cap L_{(x_i \leftarrow \alpha)}$ holds because the generators $a_{(j,s)}$ may be used according to (7) to attain, starting from $\bar{w}_{(0,\ldots,\alpha,\ldots,0)}$, any desired value r_j for the symbols $x_{(j,r_j)}$ in $\bar{w}_{\bar{r}}$, $j \neq i$, while $r_i = \alpha$ cannot be affected. Conversely, a representative of an element from $L_{(x_i \leftarrow \alpha)}$ belonging to G must by Fact 27 have all stable letters $a_{(\ell,s)}$ removed by means of repeated applications of (7); these leave $r_i = \alpha$ unaffected, thus establishing membership to $W_{(x_i \leftarrow \alpha)}$.
$x_i \leftarrow x_j$**:** Similarly as above, the $a_{(\ell,s)}$ yield, starting from $\bar{w}_{\bar{0}}$, $\bar{w}_{\bar{r}}$ with any value for r_ℓ, $\ell \neq i, j$; while the (by definition of $L_{(x_i \leftarrow x_j)}$ necessarily simultaneous) application of both $a_{(i,s)}$ and $a_{(j,s)}$ preserves the property "$r_i = r_j$".
$x_i \leftarrow x_j + x_k$**:** Similarly, now preserving "$r_i = r_j + r_k$".
The other cases proceed analogously and establish $W_o = G \cap L_o$ for all o.

Knowing o, the generators of $L_o \subseteq C$ are obviously decidable. Hence, L_o is effectively benign in algebraically presented C according to Lemma 36b). Since the same applies to G, too, Lemma 36d) yields also W_o to be effectively benign in C; and thus in G as well by virtue of Lemma 36a). □

[8] Notice that $\psi_{(i,t)}$ has $t \neq 0$. In fact, we take into account only BSS computations which do not multiply with 0. This is no loss of generality because any multiplication command may be preceded with a test whether any of the factors equals 0 and, if so, a direct assignment of 0.

[9] This is the only place where real constants occur; however those that do belong to the finitely many already present in $\mathbb{M}$.

o	$W_o \subseteq G$	$L_o \subseteq C$
"$x_i \leftarrow x_j$", $1 \le j < i$	$\langle \overline{w_r} : r_i = r_j \rangle$	$\langle \overline{w_0}\ ;\ a_{(i,s)} \cdot a_{(j,s)} : s \in \mathbb{R}\ ;$ $;\ a_{(\ell,s)} : s \in \mathbb{R}, \ell \neq i, j \rangle$
"$x_i \leftarrow \alpha$", $\alpha \in \mathbb{R}$ fixed[9]	$\langle \overline{w_r} : r_i = \alpha \rangle$	$\langle \overline{w}_{(0,\ldots,0,\alpha,0,\ldots,0)}\ ;\ a_{(\ell,s)} : s \in \mathbb{R}, \ell \neq i \rangle$
"$x_i \leftarrow x_j + x_k$", $1 \le j,k < i$	$\langle \overline{w_r} : r_i = r_j + r_k \rangle$	$\langle \overline{w_0}\ ;\ a_{(\ell,s)} : s \in \mathbb{R}, \ell \neq i, j, k\ ;$ $;\ a_{(i,s)} \cdot a_{(k,s)},\ a_{(j,s)} \cdot a_{(k,s)} : s \in \mathbb{R} \rangle$
"$x_i \leftarrow -x_j$", $1 \le j < i$	$\langle \overline{w_r} : r_i = -r_j \rangle$	$\langle \overline{w_0}\ ;\ a_{(\ell,s)} : s \in \mathbb{R}, \ell \neq i, j\ ;$ $;\ a_{(i,s)} a_{(j,-s)} : s \in \mathbb{R} \rangle$
"$x_i \leftarrow x_j \times x_k$", $1 \le j,k < i$	$\langle \overline{w_r} : r_i = r_j \cdot r_k \rangle$	$\langle \overline{w}_{\overline{e}_{\{i,j,k\}}}\ ;\ a_{(\ell,s)} : s \in \mathbb{R}, \ell \neq i, j, k\ ;$ $;\ m_{(i,s)} \cdot m_{(k,s)},\ m_{(j,s)} \cdot m_{(k,s)} : s \in \mathbb{R} \rangle$
"$x_i \leftarrow 1/x_j$", $1 \le j < i$	$\langle \overline{w_r} : r_i = \frac{1}{r_j}, r_j \neq 0 \rangle$	$\langle \overline{w}_{\overline{e}_{\{i,j\}}}\ ;\ a_{(\ell,s)} : s \in \mathbb{R}, \ell \neq i, j\ ;$ $;\ m_{(i,s)} \cdot m_{(j,1/s)} : 0 \neq s \in \mathbb{R} \rangle$
"$x_j \ge 0$", $1 \le j < i$	$\langle \overline{w_r} : r_j \ge 0 \rangle$	$\langle \overline{w_0}\ ;\ a_{(j,s)} : 0 < s \in \mathbb{R}\ ;$ $;\ a_{(\ell,s)} : s \in \mathbb{R}, \ell \neq j \rangle$
"$x_j < 0$", $1 \le j < i$	$\langle \overline{w_r} : r_j < 0 \rangle$	$\langle \overline{w}_{(0,\ldots,0,-1,0,\ldots,0)}\ ;\ m_{(j,s)} : 0 < s \in \mathbb{R}\ ;$ $;\ a_{(\ell,s)} : s \in \mathbb{R}, \ell \neq j \rangle$

We abbreviate $\overline{0} = (0,\ldots,0)$ and, for $I = \{i_1 < i_2 < \ldots < i_p\} \subseteq \{1,\ldots,D\}$,
$\overline{e_I} := (0,\ldots,0,\underbrace{1}_{i_1},0,\ldots,0,\underbrace{1}_{i_2},0,\ldots\ldots\ldots,0,\underbrace{1}_{i_p},0,\ldots,0)$.

Fig. 1. Operations and their induced subgroups.

4.5 Putting It All Together

So far, the index n of the computational path γ_n had been fixed. It will now run over $\mathbb{N}$, so that

- $n \mapsto \mathbb{A}_n \subseteq \mathbb{R}^{d(n)}$ denotes an enumerable and uniformly decidable decomposition of $\mathbb{H} = \bigcup_{n\in\mathbb{N}} \mathbb{A}_n$;
- $U_n := \langle \overline{w}_{n,\overline{r}} : \overline{r} \in \mathbb{A}_n \rangle \subseteq G$, $n \in \mathbb{N}$, where
- $G = \langle y; (x_{(i,s)})_{s\in\mathbb{R}, i\in\mathbb{N}}; (x_{(0,n)})_{n\in\mathbb{N}} \rangle$ denotes a free algebraically presented group; and
- $\overline{w}_{(n,r_1,\ldots,r_d)} = x_{(d,r_d)}^{-1} \cdots x_{(1,r_1)}^{-1} \cdot x_{(0,n)}^{-1} \cdot y \cdot x_{(0,n)} \cdot x_{(1,r_1)} \cdots x_{(d,r_d)}$.

Observe how the index n of the path γ_n accepting $\mathbb{A}_n$ is now encoded into the words generating U_n. Theorem 39 obviously carries over to this minor modification, hence

- U_n is effectively benign in G.

For given n, $\mathbb{A}_n$ is decidable: simply evaluate γ_n on a given $\overline{r}$. This amounts to *uniform* decidability (Remark 31). A brief review of Section 4.4 reveals all constructions to hold uniformly in n so that in fact

- U_n is *uniformly* effectively benign in G in the sense of Definition 34c).

It now follows from Lemma 36f) that $\langle \bigcup_n U_n \rangle \subseteq G$ is effectively benign in G, too; and so is

$$U \quad := \quad \left\langle \left\langle \bigcup_n U_n \right\rangle \cup \left\langle (x_{(0,n)})_{n\in\mathbb{N}} \right\rangle \right\rangle \cap \left\langle y; (x_{(i,s)})_{s\in\mathbb{R}, i\ge 1} \right\rangle$$

by Lemma 36b+d+e). According to Remark 35, membership to U can thus be reduced to the word problem of some algebraically presented group K. But, similar to the arguments in Lemmas 40 and 42, U arises from $\bigcup_n U_n$ by eliminating $x_{(0,n)}$ and replacing it with an existential quantifier over n. Hence, U equals $\left\langle \{\overline{w_r} : \exists n : \overline{r} \in \mathbb{A}_n\} \right\rangle$ by virtue of Fact 38. This concludes the proof of Theorem 20. □

More precisely, regarding Observation 29 and Footnote 9, one arrives at the following

Scholium[10] **43** *To every BSS machine $\mathbb{M}$ semi-deciding some language $\mathbb{P} \subseteq \mathbb{R}^\infty$, there exists an algebraically presented real group $G = \langle X|R\rangle$ (in fact with $X \subseteq \mathbb{R} \times \mathbb{N}$) to whose word problem the membership in $\mathbb{P}$ is reducible to.*

The computation of this reduction requires no real constants. Moreover, deciding X and R is possible uniformly in (that is, given) $\mathbb{M}$. In particular, the description of G requires no real constants other than those present already in $\mathbb{M}$. □

Since a Universal BSS Machine does not need constants, it follows

Corollary 44. *The real Halting Problem $\mathbb{H}$ is reducible to the word problem of an algebraically presented group over $\mathbb{Q}$!*

5 Conclusions and Perspectives

In this paper we have 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?

As main result of the paper it has been established that, on the one hand, the word problem for an algebraically presented group is always semi-decidable; while, on the other hand, there are algebraically presented groups for which the above word problem is not only undecidable but exactly as hard as the real Halting Problem.

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 are located in the heart of computational group theory; their connection to semi-algebraic geometry is visible in the background only.

There are clearly a bunch of interesting questions to be investigated. We conclude by mentioning a few of them. They might hopefully serve as starting point for a fruitful further research related to the topics studied in this paper.

Our construction yields a BSS-complete group with both generators X and relations R being BSS-decidable.

Question 1. *Can we require the set of generators to be* semi-algebraic *rather than decidable?*

Over complex numbers, every decidable set in some $\mathbb{C}^N$ is also algebraic [CR93]; however our proof makes heavy use of $\mathbb{Z}$ as a discrete component of X and does not comply with complex decidability.

Question 2. *How about a group with word problem BSS-complete over $\mathbb{C}$?*

In our approach, the relations R seem crucial to live in $\mathbb{R}^\infty$; for instance in view of U_{γ_n} (Definition 37) which includes words $\bar{w}_{n;\bar{r}}$ of length $1+2d(n)$ unbounded in n.

Question 3. *Can one restrict (not only the set of generators but also) the set of relations to some finite-dimensional $\mathbb{R}^M$?*

To this end, it might be worth while exploiting that a BSS machine references data in fact not globally but through copy registers which change by at most one in each step; cf. Definition 2.

It would furthermore be nice to have a real counterpart to the famous Higman Embedding Theorem (Fact 7):

[10] A scholium is "*a note amplifying a proof or course of reasoning, as in mathematics*" [Mor69].

Question 4. *Does every recursively presented real group admit a (BSS-computable) embedding into an effectively presented one?*

Special classes of discrete groups with *decidable* word problem have been investigated with respect to the computational *complexity* of this decision [MS83, HRRT06]. This looks promising to carry over to the reals; for instance in form of

Question 5. *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 by Miller [Mil92] in which a lot of related issues are discussed.

References

[BCSS98] L. BLUM, F. CUCKER, M. SHUB, S. SMALE: "*Complexity and Real Computation*", Springer (1998).

[BSS89] 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", pp.1–46 in *Bulletin of the American Mathematical Society* (AMS Bulletin) vol.**21** (1989).

[Boo58] W.W. BOONE: "*The word problem*", pp. 265–269 in *Proc. Nat. Acad. Sci. U.S.A*, vol.**44** (1958).

[Bou01] M. BOURGADE: "*Séparations et transferts dans la hiérarchie polynomiale des groupes abéliens infinis*", pp. 493–502 in *Mathematical Logic Quarterly*, vol.**47 (4)** (2001).

[CC00] J.W. CANNON, G.R. CONNER: "The combinatorial structure of the Hawaiian earring group", pp.225–271 in *Topology and its Applications* vol.106 (2000).

[CR93] F. CUCKER, F. ROSSELLÓ: "Recursiveness over the Complex Numbers is Time-Bounded", pp.260–267 in *Proc. 13th Conference on Foundations of Software Technology and Theoretical Computer Science* (FSTTCS'93), Springer LNCS vol.**761**.

[Cuc92] F. CUCKER: "The arithmetical hierarchy over the reals", pp.375–395 in *Journal of Logic and Computation*, vol.**2(3)** (1992).

[DJK05] H. DERKSEN, E. JEANDEL, P. KOIRAN: "Quantum automata and algebraic groups", pp.357–371 in *J. Symbolic Computation* vol.**39** (2005).

[FK91] L. FINKELSTEIN, W.M. KANTOR (Edts.): "*Groups and Computation*", vol.**11** in the DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS (1991).

[FK95] L. FINKELSTEIN, W.M. KANTOR (Edts.): "*Groups and Computation II*", vol.**28** in the DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS (1995).

[Gas01] C. GASSNER: "The $\mathcal{P} = \mathcal{DNP}$ problem for infinite abelian groups", pp. 574–583 in *Journal of Complexity*, vol.**17** (2001).

[HEB05] D.F. HOLT, B. EICK, E. O'BRIEN "*Handbook of Computational Group Theory*", Chapman&Hall/CRC (2005).

[Hig61] G. HIGMAN "Subgroups of finitely presented groups", pp. 455–475 in *Proc. Royal Society*, Ser. A 262 (1961).

[HNN49] G. HIGMAN, B.H. NEUMANN, H. NEUMANN "Embedding theorems for groups", pp. 247–254 in *J. London Math. Society*, vol.**24** (1949).

[HRRT06] D.F. HOLT, S. REES, C.E. RÖVER, R.M. THOMAS: "Groups with Context-Free Co-Word Problem", to appear in the *Journal of the London Mathematical Society*.

[Lan85] S. LANG: "$SL_2(\mathbb{R})$", Springer (1985).

[LS77] R.C. LYNDON, P.E. SCHUPP: "Combinatorial Group Theory", Springer (1977).

[Mat70] Y. MATIYASEVICH: "Enumerable sets are Diophantine", pp.354-358 *Soviet Mathematics. Doklady* vol.**11:2** (1970).

[Mic91] C. MICHAUX: "*Ordered rings over which output sets are recursively enumerable*", pp. 569–575 in *Proc. Amer. Math. Soc.*, vol.**112** (1991).

[Mil92] C.F. MILLER III:"Decision problems for groups – survey and reflections", pp. 1–59 in *Algorithms and classification in combinatorial group theory*, G. Baumslag and C.F. Miller III eds., Springer Verlag, Math. sci. res. inst. publ., vol.**1** (1992).

[Mor69] W. MORRIS (Editor): "*American Heritage Dictionary of the English Language*", American Heritage Publishing (1969).

[MS83] D.E. MULLER, P.E. SCHUPP: "Groups, the Theory of Ends, and Context-Free Languages", pp.295–310 in *J. Comp. System Sci*. vol.**26** (1983).

[MZ05] K. MEER, M. ZIEGLER: "An Explicit Solution to Post's Problem over the Reals", pp. 456–467 in *Proc. 15th Symposium on Fundamentals of Computation Theory (FCT)*, Springer LNCS, vol.**3623** (2005); see also `arXiv:cs.LO/0603071`

[Nov59] P.S. NOVIKOV: "*On the algorithmic unsolvability of the word problem in group theory*", pp. 1–143 in *Trudy Mat. Inst. Steklov*, vol.**44** (1959).

[Pru02] M. PRUNESCU: "*A model-theoretic proof for* $\mathcal{P} \neq \mathcal{NP}$ *over all infinite abelian groups*", pp. 235–238 in *The Journal of Symbolic Logic*, vol.**67** (2002).

[Rot95] J.J. ROTMAN: "*An Introduction to the Theory of Groups*" 4th Edition, Springer (1995).

[Tuc80] J.V. TUCKER: "Computability and the algebra of fields",

[Tur36] TURING, A.M.: "On Computable Numbers, with an Application to the Entscheidungsproblem", pp.230–265 in *Proc. London Math. Soc.* vol.**42(2)** (1936).

[Val69] M.K. VALIEV "On the complexity of word problem for finitely presented groups", pp. 5–43 in *Algebra and logic*, vol.**7** (1969).

[Wei00] K. WEIHRAUCH: "*Computable Analysis*", Springer (2000).