Real Computational Universality:
The Word Problem for a Class of Groups
with Infinite Presentation
(Extended Abstract)

Klaus Meer[1,*] and Martin Ziegler[2,**]

[1] IMADA, Syddansk Universitet, Campusvej 55,
5230 Odense M, Denmark
`meer@imada.sdu.dk`
[2] 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 *to*) but also reducible *from* 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.

1.1   Real Computability

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 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]. 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 whose registers can hold arbitrary real numbers; its inputs are thus finite sequences over $\mathbb{R}$ of possibly unbounded length. This model bears many structural similarities to the discrete setting like for example the existence of a Universal Machine, the notion of (e.g. $\mathcal{NP}$–) completeness, or undecidable problems:

Definition 1.1. *The* real Halting Problem $\mathbb{H}$ *is the following decision problem. Given the code* $\langle \mathbb{M} \rangle \in \mathbb{R}^\infty$ *of a BSS machine* $\mathbb{M}$, *does M terminate its computation (on empty input) ?*

Both the existence of a coding $\langle \cdot \rangle$ for BSS machines and the undecidability of $\mathbb{H}$ in the BSS model were shown in [BSS89]. 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 1.2. 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 [Mati70]. For reals $R = \mathbb{R}$ however, it *is* (BSS-)decidable by virtue of TARSKI's Quantifier Elimination [BCSS98, top of p.97].   □

1.2   Subsumption of Our Results

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 [MeZi05] *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 [Cuck92, 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. (Such a result had been envisioned in Section 4 of [MeZi06].) 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 [CaCo00] 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.

1.3   Further Related Work

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 [Bour01, Gass01, Prun02] treat such G as underlying structure of the computational model, that is, not over the reals $\mathbb{R}$ and its arithmetic. [Tuck80] considers the question of computational realizing G and its operation, not of deciding properties of (elements of) G. An exception, [DJK05] does consider BSS-decidability (and complexity) of properties of a real group; however without completeness results. There also the group is not fixed nor presented but given by some matrix generators.

1.4   Overview

Section 2 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. (Guiding examples of mathematical groups that fit into this framework can be found in the full version...) 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 proves our main result: The real Halting Problem can be reduced to the word problem of algebraically presented real groups.

2   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* [FiKa91, FiKa95, HEoB05]. 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 [Novi59] and Boone [Boon58]. In the BSS 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.

2.1   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 3.

Definition 2.1. *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*

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

where $x^1 := x$ and where 1 denotes the empty word, that is, the unit element.
b) For a group H and $W \subseteq H$, denote by

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

the subgroup of H generated by W. *The* normal *subgroup of H generated by W is $\langle W \rangle_{Hn} := \langle \{ h \cdot w \cdot h^{-1} : h \in H, w \in W \} \rangle_H$. For $h \in H$, we write h/W for its W–coset $\{ h \cdot w : w \in \langle W \rangle_{Hn} \}$ 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 $\langle R \rangle$–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.

---

[1] We remark that in the other major and complementary model of *real* (as opposed to rational or algebraic [KMPSY04]) number computation, the concept of decidability is inapplicable because, there, discontinuous functions are generally uncomputable due to the so-called Main Theorem of Recursive Analysis [Weih00, Theorem 4.3.1].

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

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 "$w_1^{\epsilon_1} \cdots w_n^{\epsilon_n} = 1$" 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 2.1 (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 2.2. *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 from the discrete Halting Problem* H. $\qquad\square$

For the nontrivial Claim b), see e.g. one of [Boon58, Novi59, LySc77, Rotm95].

Example 2.3. $\mathcal{H} := \left\langle \{a, b, c, d\} \,\middle|\, \{a^{-i}ba^i = c^{-i}dc^i : i \in H\} \right\rangle$ is a *recursively* presented group with word problem reducible from H; compare the proof of [LySc77, THEOREM §IV.7.2]. $\qquad\square$

Fact 2.2b) requires the group to be *finitely* presented group. This step is provided by the remarkable

Fact 2.4 (Higman Embedding Theorem). *Every recursively presented group can be embedded in a finitely generated one.*

Proof. See, e.g., [LySc77, SECTION §IV.7] or [Rotm95, THEOREM 12.18]. $\qquad\square$

Fact 2.4 asserts the word problem from Example 2.3 to be in turn reducible to that of the finitely presented group $\mathcal{H}$ is embedded into, because any such embedding is automatically effective:

Observation 2.5. *Let* $G = \langle X \rangle / \langle R \rangle_n$ *and* $H = \langle Y \rangle / \langle S \rangle_n$ *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* $\psi'(\bar{x}) \in \langle S \rangle_n$ *whenever* $\bar{x} \in \langle R \rangle_n$; *that is,* ψ' *maps R-cosets to S-cosets and makes Diagram (2) commute.*

$$
\begin{array}{ccc}
\langle X \rangle & \xrightarrow{\;\;\psi'\;\;} & \langle Y \rangle \\
\downarrow & & \downarrow \\
\langle X \rangle / \langle R \rangle_n & \xrightarrow{\;\;\psi\;\;} & \langle Y \rangle / \langle S \rangle_n
\end{array} \qquad (2)
$$

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 $\psi(x_i) = \bar{w}_i / \langle S \rangle_n$ where $\bar{w}_i \in \langle Y \rangle$. Setting (and storing in the machine) $\psi'(x_i) := \bar{w}_i$ yields the claim.

2.2   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 2.1c+d):

Definition 2.6. *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.*

CLASSICAL DISCRETE AND OUR NEW REAL NOTIONS:

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

Remark 2.7. a) Although X inherits from $\mathbb{R}$ algebraic structure such as addition $+$ and multiplication $\times$, the Definition 2.1a) 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 $\bar{a}$: $x_5^{-1} \neq x_{1/5}$.

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'). Even when $R = R'$, X need not be unique! Nevertheless we adopt from literature such as [LySc77] the convention 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 2.1d) 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 $(w_1, \epsilon_1, \ldots, w_n, \epsilon_n) \in (\mathbb{R}^N \times \mathbb{N})^n$. In this sense, the Rules (1) implicit in the free group are obviously decidable and may w.l.o.g. be included in R.

We first show that, parallel to Fact 2.2a), the word problem for any algebraically enumerated real group is not harder than the BSS Halting Problem:

Theorem 2.8. *Let $G = \langle X | R \rangle$ denote a algebraically enumerated real group. Then the associated word problem is BSS semi-decidable.*

This and all further proofs will be available in the full version.

---

[3] R is a set of *vectors of vectors* of varying lengths. By suitably encoding delimiters we shall regard R as effectively embedded into *single* vectors of varying lengths.

3   Reduction *from* the Real Halting Problem

This section proves the main result of the paper and continuous counterpart to Fact 2.2b): The word problem for algebraically presented real groups is in general not only undecidable (cmp. [MeZi05]) in the BSS model but in fact as hard as the real Halting Problem.

Theorem 3.1. *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 $\mathcal{H}$.*

Our proof has been guided by, and borrows concepts from, that of the discrete case [LySc77, SECTION §IV.7]. However a simple transfer fails because 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 3.2). 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 [Mati70], which is infeasible for $\mathbb{H}$ (recall Example 1.2).

3.1   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 [LySc77, Rotm95].

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 3.2. *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, $\langle \psi'(X)|S \rangle$ is a presentation of the subgroup $\psi(G)$ of H. For an embedding ψ, G is classically isomorphic to $\psi(G)$; Lemma 3.14 below contains a computable variation of this fact.

Remark 3.3. 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 3.4 (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* $G * H := \langle X \cup Y \mid R \cup S \rangle$. *Similarly for the free product* $\underset{i \in I}{*} G_i$ *with* $G_i = \langle X_i | R_i \rangle$, *$I$ an arbitary index set.*

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 [LySc77, Rotm95] and in particular the nice illustration [Rotm95, FIGURE 11.9].

Definition 3.5 (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*

$$\langle G * H \mid \phi(a) = a \forall a \in A \rangle \quad := \quad \langle X \cup Y \mid R \cup S \cup \{\phi'(\bar{v})\bar{v}^{-1} : \bar{v} \in V\} \rangle \ . \ (3)$$

Definition 3.6 (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*

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

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 [LySc77, CHAPTER IV] or [Rotm95, CHAPTER 11].

Fact 3.7 (Higman-Neumann-Neumann). *Let $G^* := \langle G; t | ta = \phi(a)t \forall a \in A \rangle$ be a HNN extension of G. Then,* id $: g \mapsto g$ *is an embedding of G into G^*.*   □

Fact 3.8 (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 it holds $g_0 \cdot t^{\epsilon_1} \cdot g_1 \cdots t^{\epsilon_n} \cdot g_n \neq 1$ in G^*.*   □

Fact 3.9 (Normal Form). *Let $P = \langle G * H | \phi(a) = a \forall A \rangle$ denote a free product with amalgamation. Consider $c_1, \ldots, c_n \in G * H$, $2 \leq n \in \mathbb{N}$, such that i) each c_i is either in G or in H; ii) consecutive c_i, c_{i+1} come from different factors; iii) no c_i is in A nor B. Then $c_1 \cdots c_n \neq 1$ in P.*   □

3.2 First Effectivity Considerations

Regarding finitely generated groups, the cardinalities of the sets of generators (that is their *ranks*) add under free products [LySc77, 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 2.6:

Observation 3.10. *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 $\textstyle\bigstar_{i \in I} G_i = \langle \bigcup_{i \in I}(X \times \{i\}) \mid \bigcup_{i \in I}(R \times \{i\}) \rangle$ 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 3.11. *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 $\textstyle\bigstar_{i \in I} G_i$.*
  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 $G^* := \langle G; (t_i)_{i \in I} \mid t_i a = \phi_i(a) t_i \forall a \in A_i \forall i \in I \rangle$ w.r.t. 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 the free product with amalgamation (3) is algebraically enumerated/presented whenever G and H are.

Remark 3.12. 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) [Cuck92, 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. $\square$

Recall (Observation 2.5) 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 3.11b+c), we explicitly have to specify the following

Definition 3.13. *An homomorphism* $\psi : \langle X|R \rangle \rightarrow \langle Y|S \rangle$ *of presented real groups is called an* effective homomorphism *if it admits a BSS-computable realization* $\psi' : X \rightarrow \langle Y \rangle$ *in the sense of Definition 3.2.*

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* $\chi' : \psi'(X) \subseteq \langle Y \rangle \rightarrow X$.

Effective embeddings arise in Lemmas 3.14 and 3.17. For an injective effective homomorphism ϕ as in Lemma 3.11c) 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.

Lemma 3.14. *Let* $\psi : G = \langle X|R \rangle \rightarrow \langle Y|S \rangle = K$ *denote an effective embedding.*

a) *There is an effective embedding* $\chi : \psi(G) \rightarrow G$ *(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.*

3.3   Benign Embeddings

The requirement in Lemma 3.11b+c) that the subgroup(s) A be recursively enumerable or even decidable, is of course central but unfortunately violated in many cases. This suggests the notion of *benign* subgroups, in the classical case (below, Item a). Recall that there, effectivity of an embedding drops off automatically.

Definition 3.15.   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 3.12, there are groups* K_i *uniformly algebraically presented and uniformly effective embeddings* $\phi_i : \langle G; t_i | t_i a_i = a_i t_i \forall a_i \in A_i \rangle \rightarrow K_i$.

The benefit of benignity is revealed in the following

Remark 3.16. In the notation of Definition 3.15b), if A is effectively benign in G then the word problem for A is reducible to that for K: Fact 3.7.
Moreover in this case, the *membership problem* for A in G — that is the question whether given $\bar{x} \in \langle X \rangle$ is equivalent (w.r.t. R) to an element of A — is also reducible to the word problem for K: According to Fact 3.8, $a := \bar{x}/R$ satisfies $t \cdot a \cdot t^{-1} \cdot a^{-1} = 1 \Leftrightarrow a \in A$. □

The following fundamental properties extend corresponding results from the finite framework. Specifically, Lemma 3.17b) generalizes [LySc77, Lemma §IV.7.7(i)] and Claims d+e) generalize [LySc77, Lemma §IV.7.7(ii)].

Lemma 3.17. *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 (possibly different from $\langle V \cup W|R \rangle$) effectively benign in G.

f) Let $(A_i)_{i \in I}$ be uniformly effectively benign in G (Definition 3.15c). Then $\langle \bigcup_{i \in I} A_i \rangle$ admits a presentation effectively benign in G.

The above claims hold uniformly, corresponding effective embeddings do not introduce new real constants.

3.4   Putting It All Together

Let $\mathbb{H} \subseteq \mathbb{R}^\infty$ denote the real Halting Problem, 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 $\mathbb{M}$, $\mathbb{A}_n \subseteq \mathbb{H} \cap \mathbb{R}^{d(n)}$ the set of inputs accepted at path γ_n. Let $X := \{x_r : r \in \mathbb{R}\} \uplus \{k_n : n \in \mathbb{N}\} \uplus \{s\}$, $G := \langle X \rangle$, and $U := \langle k_n^{-1} \cdot w_{\vec{r}} \cdot k_n : n \in \mathbb{N}, \vec{r} \in \mathbb{A}_n \rangle$ where $\bar{w}_{r_1,\ldots,r_d} := x_{r_d}^{-1} \cdots x_{r_1}^{-1} \cdot s \cdot x_{r_1} \cdots x_{r_d}$. Finally let $V := \langle U; (k_n) \rangle \cap \langle s; x_r : r \in \mathbb{R} \rangle$. Based on Lemma 3.17 we can show

Proposition 3.18. *a) U is decidable.   b) U and V are effectively benign in G. c) The words $k_n^{-1} \cdot w_{\vec{r}} \cdot k_n$ freely generate U.   d) $V = \langle \bar{w}_{\vec{r}} : \exists n \in \mathbb{N} : \vec{r} \in \mathbb{A}_n \rangle$.*

Proof (Theorem 3.1). Let K denote the algebraically presented group which the HNN extension $\langle G; t|tv = vt \forall v \in V \rangle$ effectively embeds into (Proposition 3.18b) by some effective embedding ψ. Then, according to Fact 3.8 and by Proposition 3.18d), $\bar{v} := \psi(t \cdot \bar{w}_{\vec{r}} \cdot t^{-1} \cdot \bar{w}_{\vec{r}}^{-1})$ equals 1 in K iff $\vec{r} \in \mathbb{H} = \bigcup_n \mathbb{A}_n$.   □

References

[BCSS98]   Blum, L., Cucker, F., Shub, M., Smale, S.: Complexity and Real Computation. Springer, Heidelberg (1998)

[BSS89]   Blum, L., Shub, M., Smale, S.: On a Theory of Computation and Complexity over the Real Numbers: $\mathcal{NP}$-Completeness, Recursive Functions, and Universal Machines. Bulletin of the American Mathematical Society (AMS Bulletin), vol. 21, pp. 1–46 (1989)

[Boon58]   Boone, W.W.: The word problem. Proc. Nat. Acad. Sci. 44, 265–269 (1958)

[Bour01]   Bourgade, M.: Séparations et transferts dans la hiérarchie polynomiale des groupes abéliens infinis. Mathematical Logic Quarterly 47 (4), 493–502 (2001)

[CaCo00]   Cannon, J.W., Conner, G.R.: The combinatorial structure of the Hawaiian earring group. Topology and its Applications 106, 225–271 (2000)

[Cuck92]   Cucker, F.: The arithmetical hierarchy over the reals. Journal of Logic and Computation 2(3), 375–395 (1992)

[DJK05]   Derksen, H., Jeandel, E., Koiran, P.: Quantum automata and algebraic groups. J. Symbolic Computation 39, 357–371 (2005)

[FiKa91]   Finkelstein, L., Kantor, W.M. (eds.): Groups and Computation. The DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, vol. 11. AMS, Providence, RI (1991)

[FiKa95]   Finkelstein, L., Kantor, W.M. (eds.): Groups and Computation II. The DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, vol. 28. AMS, Providence, RI (1995)

[Gass01]   Gassner, C.: The $\mathcal{P} = \mathcal{DNP}$ problem for infinite abelian groups. Journal of Complexity 17, 574–583 (2001)

[HEoB05]   Holt, D.F., Eick, B., O'Brien, E.: Handbook of Computational Group Theory. Chapman&Hall/CRC (2005)

[KMPSY04]   Kettner, L., Mehlhorn, K., Pion, S., Schirra, S., Yap, C.K.: Classroom Examples of Robustness Problems in Geometric Computations. In: Albers, S., Radzik, T. (eds.) ESA 2004. LNCS, vol. 3221, pp. 702–713. Springer, Heidelberg (2004)

[LySc77]   Lyndon, R.C., Schupp, P.E.: Combinatorial Group Theory. Springer, Heidelberg (1977)

[Mati70]   Matiyasevich, Y.: Enumerable sets are Diophantine. Soviet Mathematics. Doklady 11(2), 354–358 (1970)

[MeZi05]   Meer, K., Ziegler, M.: An Explicit Solution to Post's Problem over the Reals. In: Liśkiewicz, M., Reischuk, R. (eds.) FCT 2005. LNCS, vol. 3623, pp. 456–467. Springer, Heidelberg (2005), full version to appear in the journal of complexity, see also `arXiv:cs.LO/0603071`

[MeZi06]   Meer, K., Ziegler, M.: Uncomputability Below the Real Halting Problem. In: Beckmann, A., Berger, U., Löwe, B., Tucker, J.V. (eds.) CiE 2006. LNCS, vol. 3988, pp. 368–377. Springer, Heidelberg (2006)

[Novi59]   Novikov, P.S.: On the algorithmic unsolvability of the word problem in group theory. Trudy Mat. Inst. Steklov 44, 1–143 (1959)

[Prun02]   Prunescu, M.: A model-theoretic proof for $\mathcal{P} \neq \mathcal{NP}$ over all infinite abelian groups. The Journal of Symbolic Logic 67, 235–238 (2002)

[Rotm95]   Rotman, J.J.: An Introduction to the Theory of Groups 4th Edition. Springer, Heidelberg (1995)

[Tuck80]   Tucker, J.V.: Computability and the algebra of fields. J. Symbolic Logic 45, 103–120 (1980)

[Turi36]   Turing, A.M.: On Computable Numbers, with an Application to the Entscheidungsproblem. Proc. London Math. Soc. 42(2), 230–265 (1936)

[Weih00]   Weihrauch, K.: Computable Analysis. Springer, Heidelberg (2000)