Uncomputability Below the Real Halting Problem*

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, 33095 Germany
ziegler@upb.de

Abstract. Most of the existing work in real number computation theory concentrates on complexity issues rather than computability aspects. Though some natural problems like deciding membership in the Mandelbrot set or in the set of rational numbers are known to be undecidable in the Blum-Shub-Smale (BSS) model of computation over the reals, there has not been much work on different degrees of undecidability. A typical question into this direction is the real version of Post's classical problem: Are there some explicit undecidable problems below the real Halting Problem?

In this paper we study three different topics related to such questions: First an extension of a positive answer to Post's problem to the linear setting. We then analyze how additional real constants increase the power of a BSS machine. And finally a real variant of the classical word problem for groups is presented which we establish reducible to and from (that is, complete for) the BSS Halting problem.

1 Introduction

We consider the model of real number computation introduced by Blum, Cucker, Shub, and Smale [BSS89, BCSS98]. As opposed to Type-2 machines [Wei01], these so-called BSS machines treat each real (or complex) number as an entity which can be processed (read, stored, compared, added, and so on) exactly and in a single step. They are thus sometimes referred to as algebraic model of real number computation.

It seems fair to state that most of the research in this model so far has been on complexity issues. We on the other hand are interested in associated computability questions. It is well known that the real version $\mathbb{H}$ of the Halting Problem, i.e.

* Part of this work was done while K. Meer visited the Forschungsinstitut für Diskrete Mathematik at the University of Bonn, Germany. The hospitality during the stay is gratefully acknowledged. He was 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.
M. Ziegler is supported by DFG (project Zi1009/1-1) and by JSPS (ID PE 05501).

A. Beckmann et al. (Eds.): CiE 2006, LNCS 3988, pp. 368–377, 2006.

asking whether a given BSS machine terminates on a given input, is undecidable in this model. Other undecidable decision problems such as membership to the Mandelbrot set or to the rational numbers have been established, basically by taking into account structural properties of semi-algebraic sets and their close relation to decidable sets in the BSS model over the reals. A few more results of that type where given in [Cuc92], namely an investigation of the real counterpart to the classical arithmetical hierarchy, that is an infinite sequence of (classes of) problems of strictly increasing difficulty extending beyond $\mathbb{H}$. Our present focus is on undecidable real number problems below (and up to) $\mathbb{H}$:

- Regarding the question (raised by Emil Post in 1944) whether there actually *are* undecidable problems strictly easier than the Halting problem, Section 2 reviews and extends classical and recent affirmative results.
- The capability of a BSS machine to store a finite number of real constants in its code makes it more powerful than a Turing machine. Section 3 proves that the power of the BSS model indeed increases strictly with the number of constants it is allowed to store.
- As opposed to classical recursion theory, undecidability proofs in the BSS framework (of the Mandelbrot set, say) typically do not (and, at least for the rationals, cannot) proceed by reduction from $\mathbb{H}$. Section 4 presents a natural problem reducible both to and from (that is, equivalent to) $\mathbb{H}$.

2 Post's Problem in the Linear BSS Model

In 1944 Emil Post [Pos44] asked whether there exist problems in the Turing machine model which are undecidable yet strictly easier than the discrete Halting Problem H. Here a problem P is considered easier than H if H cannot be solved by a Turing machine having access to an oracle for P. Post's question was answered in the affirmative independently by Muchnik [Muc58] and Friedberg [Fri57]. However, so far there are no *explicit* problems with this behaviour known.

In [MZ05] the authors began to study Post's problem over the real numbers. The real Halting problem $\mathbb{H}$ is known to be BSS-undecidable [BSS89]. Thus Post's question makes perfect sense here as well, asking for the existence of BSS–undecidable problems which are semi-decidable but strictly easier than the real Halting Problem. It has turned out that the answer is not only positive, as in the discrete case, but even constructively witnessed by an explicitly statable problem. In fact, the following can be shown:

Fact 1 ([MZ05]). *No BSS algorithm can decide the real Halting Problem, even given access to an oracle for membership to the (undecidable) set $\mathbb{Q}$ of rationals.*

Since the rationals are easily shown to be semi- yet undecidable over $\mathbb{R}$ we thus have an explicit problem which is easier than $\mathbb{H}$. In [MZ05] it is also explicitly given an infinite number of incomparable problems below $\mathbb{H}$.

Remark[1] **2.** *BSS- or, more generally, algebraic* [TZ00, Sections 6.3+6.4] *computability, reducibility, and particularly degree theory are of course sensitive to the class of operations—including the (number of) constants, cf. Section 3—permitted.*

In the last ten years, the linearly restricted version $(\mathbb{R}, +, -, 0, 1, <)$ of the full BSS model over $\mathbb{R}$ has received increasing interest [Koi94, CK95] due to its relation with the classical (i.e., discrete) "$\mathcal{P}$=$\mathcal{NP}$?" question [FK00]. Here only additions, subtractions and comparisons as well as the constants 0 and 1 are allowed but no multiplication × nor division ÷. Thus, all computed intermediate results on inputs $x \in \mathbb{R}$ have the form $ax + b$ for some $a, b \in \mathbb{Z}$. Analogously to the full model, the Halting Problem $\mathbb{H}^\ell$ for linear machines is undecidable by a linear machine; and Post's problem as well makes sense in the linear version. The main result of the present section is an explicit solution to it.

Theorem 3. *Let* $\mathbb{SQ} := \{q^2 : q \in \mathbb{Q}\}$ *denote the set of quadratic rationals. Then* $\mathbb{SQ} \precneq^\ell \mathbb{Q} \preceq^\ell \mathbb{H}^\ell$*, where "*$\preceq^\ell$*" and all similar notions refer to Turing reducibility in the linear model.*

We have space to handle the easy claims: Both $\mathbb{Q}$ and $\mathbb{SQ}$ are undecidable in the linear model since this already holds in the full model. Both sets are semi-decidable: For input $x \in \mathbb{R}$ enumerate all pairs $(r, s) \in \mathbb{Z} \times \mathbb{N}$ and check for each pair whether $x \cdot s = r$. Note that both the enumeration and the 'multiplication' $x \cdot s$ can be performed in $(\mathbb{R}, +, -, 0, 1, <)$; similarly for semi-deciding $\mathbb{SQ}$ by enumerating all pairs (r^2, s^2) based for instance on the recursion $(r + 1)^2 = r^2 + r + r + 1$. Next, $\mathbb{SQ} \preceq^\ell \mathbb{Q}$: On input $x \in \mathbb{R}$, first check $x \geq 0$ and ask the $\mathbb{Q}$-oracle whether $x \in \mathbb{Q}$. If this is the case use the above enumeration to find $(r, s) \in \mathbb{N}^2$ with $xs = r$. Then test whether some of the (finitely many) pairs $(\tilde{r}^2, \tilde{s}^2) \leq (r, s)$ satisfies $x \cdot \tilde{s}^2 = \tilde{r}^2$ or not.

Note that in the full BSS model the converse relation $\mathbb{Q} \preceq \mathbb{SQ}$ is also valid: Having access to a $\mathbb{SQ}$–oracle one can decide $\mathbb{Q}$ by simply squaring the input $x \in \mathbb{R}$. By the nontrivial claim of Theorem 3, this reduction does not hold in the linear model.

Question 1. *In the linear setting, is* $\mathbb{Q}$ *as hard as the Halting Problem?*

In the full BSS model, Question 1 has a negative answer according to Fact 1.

3 The Benefit of Additional Real Constants

Already the paper [BSS89] revealed that the capability of BSS machines to store a finite number of arbitrary real constants gives it super-recursive power. Specifically, *any* $A \subseteq \mathbb{N}$ and in particular the discrete Halting Problem H can be encoded into some $r \in \mathbb{R}$ and thus decided by a BSS machine.

This raises the question whether and to what extent real or complex constants may be exploited in terms of complexity as well, that is, in order to accelerate

[1] We gladly follow an anonymous referee's suggestion to point this out explicitly.

solution of computational problems. We briefly mention some interesting results in that respect. In the complex BSS model for rational decision problems one can eliminate complex constants in potential decision algorithms with a polynomial slow down only, see [BCSS98, Koi96]. For the real number model it is an important open question whether real constants can be eliminated without too a high increase of the running time. Some aspects of this question are discussed in [Cha99, BMM00]. In certain restrictions of the BSS model, however, it was shown that the use of real constants introduces non-uniformity, see [Koi93]. Similar results where obtained for several complexity classes, for example in [CG97].

The present section deals with the *computational* power of BSS machines. We want to gauge the *degree* of super-recursiveness yielded by one, two, or more real constants. In the discrete realm, a pairing function like $\langle x, y\rangle := (2x+1)\cdot 2^y$ admits a computable en- and decoding of several integers into a single one. This significantly differs from the real case where, as a consequence to the *domain-invariance theorem* in Algebraic Topology [Dei85, THEOREM 4.3], a bijection $\mathbb{R}\times\mathbb{R}\to\mathbb{R}$ cannot be locally continuous, not to mention BSS-computable[2]. Thus the impossibility to effectively en- and decode two reals into a single one should, at least intuitively, imply that two constants yield strictly more power than a single one.

Our first result is based on a tool related to [TZ00, SECTIONS 6.3+6.4]:

Lemma 4. *For $A \subseteq \mathbb{R}^\infty$ and $c_1,\dots,c_i \in \mathbb{R}$, consider the following claims:*

a) A is semi-decidable by a BSS Machine with constants $c_1,\dots,c_i\in\mathbb{R}$.
b) There is an integer sequence $(d_n)_n$ such that A is a countable union $A = \bigcup_n A_n$ of sets $A_n \subseteq \mathbb{R}^{d_n}$ semi-algebraic over the field extension $\mathbb{Q}(c_1,\dots,c_i)$.
c) There exists $c_{i+1}\in\mathbb{R}$ such that A is semi-decidable by a BSS Machine with constants $c_1,\dots,c_i,c_{i+1}$.

Then a) implies b) from which in turn c) follows.

Proof. implicit in [Cuc92, THEOREM 2.4 and REMARK 2.5]; cf. also [Mic90]. □

Theorem 5. *a) Let $(p_i)_i = (2,3,5,7,11,\dots)$ denote the sequence of primes and $c_i := \exp(\sqrt{p_i})\in\mathbb{R}$. Then, $c_1,\dots,c_i$ are algebraically independent.*
b) Let $c_1,\dots,c_i$ be algebraically independent. The finite set $A := \{c_1,\dots,c_i\}\subseteq\mathbb{R}$ is decidable with i real constants but not semi-decidable with $i-1$ real constants.

In other words, the computational power of the BSS model strictly increases with every further admitted constant.

Proof. a) Apply Lindemann-Weierstraß [Bak75, THEOREM 1.4] to the linearly independent numbers $\sqrt{p_i}$ (`math.niu.edu/~rusin/known_math/00_incoming/sqrt_q`).
b) Suppose A is semi-decidable by a machine with $i-1$ real constants. By Lemma 4 (a⇒b), it is semi-algebraic over some rational field extension $K = \mathbb{Q}(\tilde{c}_1,\dots,\tilde{c}_{i-1})$. A finite discrete set, *in*equalities can be eliminated revealing

[2] Although $(x,n)\mapsto\langle\lfloor x\rfloor, n\rangle + (x-\lfloor x\rfloor)$ is a bi-computable bijection $\mathbb{R}\times\mathbb{N}\to\mathbb{R}$.

that A is even algebraic over K—contradicting that A's transcendence degree exceeds that of K. □

Next, let $\mathbb{H}_i$ denote the real Halting Problem for BSS-machines with i constants. Obviously $\mathbb{H}_i$ is no harder than $\mathbb{H}_{i+1}$—simply choose $c_{i+1} = c_i$. We want to show that $\mathbb{H}_i$ is in fact *strictly* easier than $\mathbb{H}_{i+1}$. This claim does not follow from Theorem 5 because the (anyway a bit artificial) sets A_i constructed there are neither reducible to nor from any $\mathbb{H}_j$. Formally:

Definition 6. *Let different versions of the Halting Problem be defined as*
$H := \{\langle M\rangle : M$ *is a Turing machine that terminates on input* $0\}$
$\mathbb{H}_0 := \{\langle M\rangle : M$ *is a constant-free BSS machine that terminates on input* $0\}$
$\mathbb{H}_1 := \{\langle M, c_1\rangle : M$ *is a BSS machine with constant* c_1 *terminating on* $0\}$
$\mathbb{H}_2 := \{\langle M, c_1, c_2\rangle :$ *BSS machine* M *with constants* c_1, c_2 *terminating on* $0\}$
and so on. Here, $\langle M\rangle \in \mathbb{N}$ *denotes a reasonable encoding of (the discrete, i.e. control part of) machine* M *by an integer number* [BSS89, SECTION 8].

Note that indeed the control part of a BSS machine (except for the machine constants, that is) can easily be coded by a single integer. In particular, the code of an instance for $\mathbb{H}_i$ varies piecewise continuously with the machine constants $c \in \mathbb{R}^i$ used. Since $\mathbb{H}_i \subseteq \mathbb{R}^i$ by virtue of footnote 2, Definition 6 describes the dimensional decomposition of the real BSS Halting Problem $\mathbb{H} = \bigcup_i \mathbb{H}_i \subseteq \mathbb{R}^\infty$. That $\mathbb{H}_i$ is strictly easier than $\mathbb{H}_{i+1}$ has the interesting consequence of yielding, in addition to the set $\mathbb{Q}$ of rationals according to [MZ05], a vast variety of further explicit solutions to Post's Problem over the Reals:

Corollary 7. *Fix* $i \in \mathbb{N}$ *and let* $A \subseteq \mathbb{R}^i$ *be undecidable yet recursively enumerable. Then* A *is strictly easier than* $\mathbb{H} \subseteq \mathbb{R}^\infty$*. In particular, unbounded dimension is unavoidable for any BSS-complete problem.*

For the underlying notion of reducibility to make sense here, the use of real constants must be limited in computing the corresponding reduction function.

Definition 8. *Let* $A, B \subseteq \mathbb{R}^\infty$ *be two real decision problems.* A *is called many-one reducible to* B with i constants *if there exists a BSS machine* M *having constants* $c_1, \ldots, c_i \in \mathbb{R}$ *that reduces* A *to* B *in the usual sense. We denote this by "*$A \preceq_m^i B$*"; similarly for equivalence "*$\equiv_m^i$*". Regarding Turing-reduction, write "*$A \preceq_T^i B$*" if a BSS machine with at most* i *constants can decide* A *given oracle access to* B*.*

It is well-known that the three basic classical characterizations of recursive enumerability of some $A \subseteq \mathbb{N}$—halting set of a Turing machine (semi-decidability), many-one reducibility to H, and range of a computable integer function—carry over to the real setting[3] [Mic91]. The same holds for $\mathbb{H}$'s single 'slices' $\mathbb{H}_i$:

Lemma 9. *For any decision problem* $A \subseteq \mathbb{R}^n$*, the following are equivalent:*

a) A *is the halting set of some BSS machine with* i *real constants;*
b) $A \preceq_m^i \mathbb{H}_{i+n}$*;*

[3] Notice that enumerability of a countable $A \subseteq \mathbb{R}$ does *not* mean $A = \text{range}(f)$ for a computable $f : \mathbb{N} \to \mathbb{R}$; compare Lemma 9c).

c) $A = \mathrm{range}(f)$ *for some partial function* $f :\subseteq \mathbb{R}^n \to \mathbb{R}^n$ *computable by a BSS machine with* i *real constants.*

For the rest of this section, we show that the hierarchy $\mathbb{H}_i$ from Definition 6 is indeed strict. For the lowest two levels it is not hard to show

Proposition 10. $H \equiv^0_m \mathbb{H}_0 \lneq^0_T \mathbb{H}_1$.

The next result applies to all levels of the hierarchy but takes into account only many-one reductions (or, more generally, Turing-reductions permitted only one oracle query).

Theorem 11. *For all* $i \in \mathbb{N}$ *it is* $\mathbb{H}_{i+1} \not\leq^0_m \mathbb{H}_i$ *and* $\mathbb{H}_{i+1} \not\leq^0_{T[1]} \mathbb{H}_i$.

Proof. Suppose that a constant-free machine M^* decides $\mathbb{H}_{i+1}$ making a single oracle call to $\mathbb{H}_i$. Consider an instance $(M, c^*_1, \dots, c^*_{i+1})$ for $\mathbb{H}_{i+1}$, where all c^*_i are algebraically independent. Then in a small ball $U(c^*)$ around $c^* := (c^*_1, \dots, c^*_{i+1})$ the reduction algorithm will use the same path for inputs of the form $(M, c), c \in U(c^*)$ and thus it computes instances of $\mathbb{H}_i$ having the form $(M', \mathcal{P}(c^*))$. Here, M' will be the same machine for all $c \in U(c^*)$ due to the remark preceding the theorem, and $\mathcal{P} : \mathbb{R}^{i+1} \to \mathbb{R}^i$ is a polynomial map, say $\mathcal{P} = (p_1, \dots, p_i)$.

The main task of the proof now is to construct a situation where we can guarantee that both a yes- and a no-instance of the given problem $\mathbb{H}_{i+1}$ have to be reduced to the same instance of $\mathbb{H}_i$. This can be achieved by using the implicit function theorem together with the cylindrical algebraic decomposition of semi-algebraic sets.

The above arguments hold for any machine M having $i+1$ machine constants which are algebraically independent. We now specify M to be a machine that uses machine constants $(c_1, \dots, c_{i+1})$ and halts on input 0 iff all its constants are algebraically independent. There are two cases to analyze:

Case 1. In $U(c^*)$ there exists a point $\tilde{c}$ such that $detD\mathcal{P}(\tilde{c}) \neq 0$. Without loss of generality we can assume that the components of such an $\tilde{c}$ are algebraically independent. Otherwise, continuity of the determinant and of $\mathcal{P}$ together with density of the tuples of algebraically independent numbers in $\mathbb{R}^{i+1}$ would yield a contradiction.

According to the implicit function theorem there exist a neighborhood V of $\tilde{c}_{i+1}$ and an implicit function $g : V \to \mathbb{R}^i$ such that for all $c_{i+1} \in V$ the vector $\mathcal{P}(g(c_{i+1}), c_{i+1})$ is constantly equal to $\mathcal{P}(g(\tilde{c}_{i+1}), \tilde{c}_{i+1})$. It is then clear that there is a rational point c_{i+1} in V such that the yes-instance $(M, \tilde{c})$ and the no-instance $(M, g(c_{i+1}), c_{i+1})$ both are mapped to the same instance of $\mathbb{H}_i$ by the reduction algorithm. Thus the reduction fails.

Case 2. Now suppose that the above matrix is singular in all points of $U(c^*)$. Since $\mathcal{P}$ is a polynomial and since $U(c^*)$ as ball is semi-algebraic the image $\mathcal{P}(U(c^*))$ is semi-algebraic as well. By Sard's theorem the image $\mathcal{P}(U(c^*))$ has measure 0 in $\mathbb{R}^i$ and thus is of dimension m for some $0 \leq m < i$. For notational simplicity below we set $m = i + 1 - j$ for a $j > 1$.

Using the well known properties of semi-algebraic sets, in particular the existence of a cylindrical algebraic decomposition we can find a set $W \subset \mathcal{P}(U(c^*))$ of dimension m such that the following holds:

- W is semi-algebraic in $\mathbb{R}^i$ and its projection onto the, say, m final components is an open ball in $\mathbb{R}^m$;
- thus W is diffeomorphic to a ball $K \subseteq \mathbb{R}^m$ via a map $\phi : W \to K$;
- there exists a $\hat{c} \in \mathcal{P}^{-1}(W)$ such that the matrix $\left\{ \dfrac{\partial(\phi \circ \mathcal{P})_k}{\partial c_\ell}(\hat{c}) \right\}_{\substack{1\le k\le j \\ 1\le \ell\le j}}$ has rank j in a neighborhood of $\hat{c}$. Using the same argument as for Case 1 we can without loss of generality assume all components of $\hat{c}$ to be algebraically independent.

Once again, the implicit function theorem yields existence of a neighborhood $V \subset \mathbb{R}^m$ of $(\hat{c}_{j+1}, \ldots, \hat{c}_{i+1})$ and a function $g : V \to \mathbb{R}^j$ such that

$$\phi \circ \mathcal{P}(g(c_{j+1}, \ldots, c_{i+1}), c_{j+1}, \ldots, c_{i+1}) = \phi \circ \mathcal{P}(g(\hat{c}_{j+1}, \ldots, \hat{c}_{i+1}), \hat{c}_{j+1}, \ldots, \hat{c}_{i+1})$$

for all $(c_{j+1}, \ldots, c_{i+1}) \in V$. Again, this neighborhood V contains a point with a rational component c_{i+1} and the reducing machine will fail on either $\hat{c}$ or that point with rational last component. □

The above proof cannot be applied to yield the same result with respect to Turing reductions. It would only be possible to "fool" as many oracle calls of a reduction machine as the dimension of the image $\mathcal{P}(U)$ is. Thus we have the following open

Question 2. *Does Theorem 11 generalize to arbitrary Turing reductions?*

4 Completeness and the Real Word Problem: An Outline

Classical recursion theory knows a variety of natural problems equivalent (that is, reducible from *and to*) the discrete Halting Problem H: Post's Correspondence Problem, Hilbert's Tenth Problem, and the Word Problem for finitely presented groups [Nov59, Boo58] all are undecidable. The corresponding proofs proceed by reduction from H.

In the real setting of BSS machines on the other hand, most undecidability proofs involve algebraic and/or topological arguments. This is the case with the Mandelbrot set [BCSS98, Theorem 2.4.2], convergence of Newton's iteration [BCSS98, Theorem 2.4.4], and the sets $\mathbb{Q}$ and $\mathbb{A}$ of rationals and of algebraic reals, respectively [MZ05]. And indeed, these problems are (provably for the latter, the others probably as well) *strictly* easier than the real Halting Problem $\mathbb{H}$; cf. Section 2. This raises the question for BSS-complete problems other than $\mathbb{H}$, that is, for further systems capable of universal real number computation. Observe that the above discrete examples all are BSS-decidable by [BSS89, Example 6]. In the present section we present a natural extension of the classical word problem to the reals which is provably many-one reducible to *and from*

$\mathbb{H}$, that is, a new BSS-complete problem in the sense of universal computation. Here we basically only present the formulation of the related problem. It is in full length discussed in [MZ06].

Definition 12. *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 $\bar{w} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $n \in \mathbb{N}$, $x_i \in X$, $\alpha_i \in \{-1, +1\}$, 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 sets X and $R \subseteq \langle X\rangle$, consider the quotient $\langle X\rangle / \langle R\rangle_n =: \langle X|R\rangle$ of $\langle X\rangle$ with respect to the normal *subgroup $\langle R\rangle_n$ of $\langle X\rangle$ generated by R. If both X and R are finite, the tuple (X, R) will be called a* finite presentation *of G.*

c) 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

Fact 13. *a) The word problem for any fixed finitely presented group is semi-decidable by a Turing Machine.*

b) There is a finitely presented group whose associated word problem is many-one reducible by a Turing machine from the discrete Halting Problem H.

Proof. a) is immediate. For b) see e.g. the great textbook [LS77]. □

The word problem for discrete groups is decidable by a BSS-machine. Therefore we now consider *real* groups and their associated word problems. This approach differs significantly from other work dealing with groups G in the BSS setting which treat such G as underlying structure of the computational model, that is, not over the reals $\mathbb{R}$ and its arithmetic structure. [Tuc80] considers the question of computational realizing G and its operation, not of deciding properties of (elements of) G. [DJK05] does consider BSS-decidability (and -complexity) of properties of a real group, but *given* by some matrix generators and lacking completeness results. 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; whereas any *fixed* such group is isomorphic either to $(\mathbb{Z}, +)$ or to some $(\mathbb{Z}_n, +)$, both with easy word problem.

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 12b):

Definition 14. *Let $X \subseteq \mathbb{R}^N$ for some $N \in \mathbb{N}$ and $R \subseteq (X \cup X^{-1})^*$. We call the group $G = \langle X|R\rangle$* effectively presented *if both X and R are BSS-decidable.*

Remark 15. a) Though X inherits from $\mathbb{R}^N$ algebraic structure, Definition 12a) of the free group $G = (\langle X\rangle, \circ)$ considers X as a plain set only. Thus, (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 by writing 'abstract' generators $x_{\bar{a}}$ indexed with real vectors $\bar{a}$; here, 'obviously' $x_5^{-1} \neq x_{1/5}$.

b) BSS-computation of course refers to encoding input (and, if present, also output) as (finite sequences of) vectors of real numbers, that is, of $\bar{w} \in (X \cup X^{-1})^*$ as, e.g., $(w_1, \alpha_1, \dots, w_n, \alpha_n) \in (\mathbb{R}^N \times \mathbb{Z})^n$.
c) While Definition 12c) requires the set X of generators to be finite, it must in the real setting be a finite-*dimensional* subset of $\mathbb{R}^\infty$. Considerable effort in the proof of Theorem 18b) is spent on asserting this condition. □

Example 16. Let $\mathbb{S}$ denote the unit circle in $\mathbb{C}$ with complex multiplication. The following is an effective presentation $\langle X | R_1 \cup R_2 \rangle$ of $\mathbb{S}$ (with decidable word problem):

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

Example 17. (Undecidable) real membership "$t \in \mathbb{Q}$" is reducible to the word problem of an effectively presented real group: Consider $X = \{x_r : r \in \mathbb{R}\}$, $R = \big\{ x_{nr} = x_r, x_{r+k} = x_k : r \in \mathbb{R}, n \in \mathbb{N}, k \in \mathbb{Z} \big\}$; then $x_r = x_0 \Leftrightarrow r \in \mathbb{Q}$. □

The latter example does not establish BSS-*hardness* of the real word problem because $\mathbb{Q}$ is provably easier than the real Halting Problem $\mathbb{H}$ [MZ05]. It is the main result of the present section to provide a BSS counterpart to Fact 13.

Theorem 18. *a) For any effectively presented real group $G = \langle X | R \rangle$, the associated word problem is BSS semi-decidable.*
b) There exists an effectively presented real group $\langle X | R \rangle$ whose associated word problem is many-one reducible from $\mathbb{H}$ by a BSS machine.

Notice that already Claim a) requires Tarski's quantifier elimination. We also point out that, in accordance with Definition 14 and as opposed to X, the set R of relations in b) lives in $\mathbb{R}^\infty$, that is, has unbounded dimension.

References

[Bak75] A. Baker: "*Transcendental Number Theory*", Camb. Univ. Press (1975).

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

[BMM00] S. Ben-David, K. Meer, C. Michaux: "A note on non-complete problems in $NP_\mathbb{R}$", pp.324–332 in *Journal of Complexity* vol. **16**, no. 1 (2000).

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

[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).

[Cha99] O. Chapuis, P. Koiran: "Saturation and stability in the theory of computation over the reals", pp.1–49 in *Annals of Pure and Applied Logic*, vol.**99** (1999).

[CG97] F. Cucker, D.Y. Grigoriev: "On the power of real turing machines over binary inputs", pp.243–254 in *SIAM Journal on Computing*, vol.**26**, no.1 (1997).

[CK95] F. Cucker, P. Koiran: "Computing over the Real with Addition and Order: Higher Complexity Classes", pp.358–376 in *Journal of Complexity* vol.**11** (1995).

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

[Dei85] K. Deimling: "*Nonlinear Functional Analysis*", Springer (1985).

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

[FK00] H. Fournier, P. Koiran: "Lower Bounds Are Not Easier over the Reals", pp.832–843 in *Proc. 27th International Colloqium on Automata, Languages and Programming* (ICALP'2000), vol.**1853** in Springer LNCS.

[Fri57] R.M. Friedberg: "Two recursively enumerable sets of incomparable degrees of unsolvability", pp.236–238 in *Proc. Natl. Acad. Sci.* vol.**43** (1957).

[Koi93] P. Koiran: "A weak version of the Blum-Shub-Smale model", pp. 486–495 in *Proceedings FOCS'93*, (1993).

[Koi94] P. Koiran: "Computing over the Reals with Addition and Order", pp.35–48 in *Theoretical Computer Science* vol.**133** (1994).

[Koi96] P. Koiran: "Elimination of Constants from Machines over Algebraically Closed Fields", pp. 65–82 in *Journal of Complexity*, vol.**13** (1997).

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

[Mic90] C. Michaux: "Machines sur les réels et problèmes $\mathcal{NP}$–complets", *Séminaire de Structures Algébriques Ordonnées*, Prépublications de l'equipe de logique mathématique de Paris 7 (1990).

[Mic91] C. Michaux: "Ordered rings over which output sets are recursively enumerable", pp. 569–575 in *Proceedings of the AMS 111* (1991).

[Muc58] A.A. Muchnik: "Solution of Post's reduction problem and of certain other problems in the theory of algorithms", pp. 391–405 in *Trudy Moskov Mat. Obsc.*, vol.**7** (1958).

[MZ05] K. Meer, M. Ziegler: "An explicit solution to Post's problem over the reals", pp. 456–467 in *Proc. 15th International Symposium on Fundamentals of Computation Theory, Lübeck*, LNCS vol. 3623 (2005).

[MZ06] K. Meer, M. Ziegler: "On the word problem for a class of groups with infinite presentations", Preprint (2006).

[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).

[Pos44] E.L. Post: "Recursively enumerable sets of positive integers and their decision problems", pp.284–316 in *Bull. Amer. Math. Soc.* vol.**50** (1944).

[Tuc80] J.V. Tucker: "Computability and the algebra of fields", pp.103–120 in *J. Symbolic Logic* vol.**45** (1980).

[TZ00] J.V. Tucker, J.I. Zucker: "Computable functions and semicomputable sets on many sorted algebras", pp317–523 in (S. Abramskz, D. Gabbay, T. Maibaum Eds.) *Handbook of Logic for Computer Science* vol.**V** (Logic and Algebraic Methods), Oxford University Press (2000).

[Wei01] Weihrauch K.: "*Computable Analysis*", Springer (2001).