An Explicit Solution to Post's Problem over the Reals

Klaus Meer and Martin Ziegler

Department of Mathematics and Computer Science,
Syddansk Universitet, Campusvej 55, 5230 Odense M,
FAX: 0045 6593 2691, Denmark
{meer, ziegler}@imada.sdu.dk

Abstract. In the BSS model of real number computations we prove a concrete and explicit semi-decidable language to be undecidable yet not reducible from (and thus strictly easier than) the real Halting Language. This solution to Post's Problem over the reals significantly differs from its classical, discrete variant where advanced diagonalization techniques are only known to yield the existence of such intermediate Turing degrees.

Then we strengthen the above result and show as well the existence of an uncountable number of incomparable semi-decidable Turing degrees below the real Halting problem in the BSS model. Again, our proof will give concrete such problems representing these different degrees.

1 Introduction

Is every super-Turing computer capable of solving the discrete Halting Problem H? More formally, does each undecidable, recursively enumerable language $P \subseteq \mathbb{N}$, when serving as oracle to some appropriate Turing Machine M, enable this M^P to decide H? That question of E.L. Post from 1944 was answered to the negative in 1956/57 independently by Muchnik and Friedberg [8][1]. Devising the *finite injury priority* sophistication of diagonalization, they proved the existence of r.e. Turing degrees strictly between those of $\emptyset$ and $\emptyset' = H$; cf. [21, Chapters V to VII].

While the diagonal language is also based on a mere existence proof, its reduction to H reveals this as well as many other explicit and practical problems in automatized software verification undecidable. In contrast, problems like P are until nowadays only known to exist but have resisted any explicit — not to mention intuitive — description.

It turns out that for real number problems the situation is quite different. More precisely, for the $\mathbb{R}$-machine model due to Blum, Shub, and Smale [2,3], we *explicitly* present a semi-decidable language (specifically, the set $\mathbb{Q}$ of rationals) and prove it to neither be reducible from the real Halting Problem $\mathbb{H}_\mathbb{R}$

[1] The existence of intermediate Turing degrees that need not to be r.e. follows from a result by Kleene and Post from 1954, see [21, Chapter VI].

M. Liśkiewicz and R. Reischuk (Eds.): FCT 2005, LNCS 3623, pp. 467–478, 2005.

nor from the set $\mathbb{A}$ of algebraic reals. The proof exploits that real computability theory, apart from logic as in the discrete case, has also algebraic and topological aspects.

Section 1.2 recalls the basics of real number computation in the BSS model as well as the recursion-theoretic notions of reducibility and degrees; Section 2 contains the first main result of our work; we show $\mathbb{Q} \precneqq \mathbb{A}$, i.e. the real algebraic numbers cannot be decided using a BSS oracle machine which has access to the (undecidable!) set of rationals as oracle set. Section 2.1 proves the '$\preceq$'-part, Section 2.2 the '$\precneqq$'-part. In Section 3 the results are generalized in order to get an uncountable number of incomparable semi-decidable problems below the real Halting problem. We conclude in Section 4 with some general remarks on hypercomputation.

1.1 Related Work

Our contribution adds to other results, indicating that many (separation-) problems which seem to require non-constructive (e.g., diagonalization) techniques in the discrete case, admit an explicit solution over the reals. For instance, a problem neither in $\mathcal{VP}$ nor $\mathcal{VNP}$-complete (provided that $\mathcal{VP} \neq \mathcal{VNP}$, of course) was presented explicitly in [4, SECTION 5.5].

CUCKER's work [7] is about the Arithmetic Hierarchy over $\mathbb{R}$, that is, degrees beyond the real Halting Problem $\mathbb{H}_\mathbb{R}$.

HAMKINS and LEWIS considered Post's Problem over the reals for *Infinite Time* Turing Machines, that is, with respect to arguments $x \in \mathbb{R}$ given by their binary expansion and for hypercomputers performing an ordinal number of steps like $1, 2, 3, \ldots, n, \ldots, \omega, \omega+1, \ldots, 2\omega, \ldots$ They showed in [9] that in this model,

- for sets of reals the answer is "no" just like in the classical discrete case.
- for *single* real numbers x on the other hand, considered as sets $L_x \subseteq \mathbb{N}$ of those indices where the binary expansion of x has a 1, there is no undecidable degree below that of the Halting Problem (of Infinite Time Machines). POST's Problem therefore is to be answered to the *positive* in this latter setting!

The existence of different *complexity degrees* below $\mathcal{NP}$ in the BSS model both for real and for complex numbers was studied in a series of papers [1,6,16] and related to classical results (cf. [13,20]) for the Turing model.

1.2 The BSS Model of Real Number Computation

This section summarizes very briefly the main ideas of real number computability theory. For a more detailed presentation see [3].

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.

Definition 1. *([2])*

a) Let $Y \subseteq \mathbb{R}^\infty := \bigoplus_{k\in\mathbb{N}} \mathbb{R}^k$, i.e. the set of finite sequences of real numbers. A BSS-machine M over $\mathbb{R}$ with admissible input set Y *is given by a finite set*

I of instructions labeled by $1, \ldots, N$. A configuration of M is a quadruple $(n, i, j, x) \in I \times \mathbb{N} \times \mathbb{N} \times \mathbb{R}^\infty$. Here, n denotes the currently executed instruction, i and j are used as addresses (copy-registers) and x is the actual content of the registers of M. The initial configuration of M's computation on input $y \in Y$ is $(1, 1, 1, y)$. If $n = N$ and the actual configuration is (N, i, j, x), the computation stops with output x .

The instructions M is allowed to perform are of the following types :

computation: $n : x_s \leftarrow x_k \circ_n x_l$, *where* $\circ_n \in \{+, -, \times, \div\}$ *or* $n : x_s \leftarrow \alpha$ *for some constant* $\alpha \in \mathbb{R}$.
The register x_s will get the value $x_k \circ_n x_l$ 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** $x_0 \geq 0$ **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: $n : x_i \leftarrow x_j$, *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.*

b) *A set $A \subseteq \mathbb{R}^\infty$ is a* decision problem *or a* language. *We call a function $f : A \to \mathbb{R}^\infty$ (BSS-)* computable *iff it is realized by a BSS machine over admissible input set A. Similarly, a set $A \subseteq \mathbb{R}^\infty$ is* decidable *in $\mathbb{R}^\infty$ iff its characteristic function is computable. It is* semi-decidable *(synonymously:* r.e.*) iff there is a BSS algorithm which takes inputs from $\mathbb{R}^\infty$ and halts precisely on the elements belonging to A.*

c) *A BSS oracle machine using an* oracle *set $B \subseteq \mathbb{R}^\infty$ 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 $x \in \mathbb{R}^\infty$ belongs to B. The oracle gives the correct answer at unit cost.*

Several further concepts and notions now emerge as in the discrete setting.

Definition 2. *The* real Halting Problem $\mathbb{H}_\mathbb{R}$ *is the following decision problem. Given the code $c_M \in \mathbb{R}^\infty$ of a BSS machine M together with an $x \in \mathbb{R}^\infty$, does M terminate its computation on input x?*

Both the existence of such a coding for BSS machines and the undecidability of $\mathbb{H}_\mathbb{R}$ in the BSS model were shown in [2].

Next, oracle reductions are defined as usual.

Definition 3. *a) A real number decision problem A is* reducible *to another decision problem B if there is a BSS oracle machine that decides membership in A by using B as oracle set. We denote this reducibility by $A \preceq B$ and write $A \precneqq B$ when A is reducible to B, but B is not reducible to A.*

b) *If A is reducible to B and vice versa, we write $A \equiv B$. This defines equivalence classes $\{B : A \equiv B\}$ among real number decision problems called* (real) Turing degrees *or* BSS degrees.

c) *If none of two problems is reducible to the other, they are said to be incomparable.*

The main question treated in this paper is: Are there incomparable Turing degrees strictly between the degree $\emptyset$ of decidable problems in $\mathbb{R}^\infty$ and the degree $\emptyset'$ of the real Halting problem $\mathbb{H}_\mathbb{R}$?

2 Explicit Solution to Post's Problem over the Reals

Consider the sets $\mathbb{Q}$ of all rational numbers and $\mathbb{A}$ of all algebraic reals, that is, of real zeros of polynomials with rational coefficients, only. $\mathbb{Q}$ is obviously semi-decidable (upon input of $x \in \mathbb{R}$, simply check for all pairs of integers $r, s \in \mathbb{Z}$ whether $x = r/s$) but well-known not to be decidable [10,17]. In fact the same holds for $\mathbb{A}$: Given $x \in \mathbb{R}$, try for all polynomials $p \in \mathbb{Q}[X]$ whether $p(x) = 0$.

Our first main result states that, even given oracle access to $\mathbb{Q}$, $\mathbb{A}$ remains undecidable: $\mathbb{A} \not\preceq \mathbb{Q}$. Since oracle access to the Halting Problem $\mathbb{H}_\mathbb{R}$ of BSS machines allows to decide $\mathbb{A}$ by querying whether the above search for $p \in \mathbb{Q}[X]$ terminates, $\mathbb{Q}$ thus constitutes an explicit example of a real BSS degree strictly between the decidable one and that of the Halting Problem.

We also show $\mathbb{Q} \preceq \mathbb{A}$.

Theorem 4. *In the BSS model of real number computation it holds* $\mathbb{Q} \precneqq \mathbb{A}$. *In particular, transcendence is not semi-decidable even when using* $\mathbb{Q}$ *as an oracle.*

This result is, in spite of the notational resemblance to $\mathbb{Q} \subsetneq \mathbb{A}$, by no means obvious.

2.1 Deciding $\mathbb{Q}$ in $\mathbb{R}$ by Means of an $\mathbb{A}$–Oracle

In this section, we prove

Lemma 5. $\mathbb{Q} \preceq \mathbb{A}$.

Proof. Consider some input $x \in \mathbb{R}$. By querying the $\mathbb{A}$-oracle, identify and rule out the case that x is not in $\mathbb{A}$ (and hence not in $\mathbb{Q}$ either). So it remains to distinguish $x \in \mathbb{Q}$ from $x \in \mathbb{A} \setminus \mathbb{Q}$. To this end, calculate $d := \deg(x)$ according to Lemma 6 below and test whether $d = 1$ $(x \in \mathbb{Q})$ or $d \geq 2$ $(x \notin \mathbb{Q})$. □

Recall that the *degree* of an algebraic $a \in \mathbb{R}$ is defined to be

$$\deg(a) = \dim_\mathbb{Q} \mathbb{Q}(a) = [\mathbb{Q}(a) : \mathbb{Q}],$$

that is, the dimension of the rational extension field generated by a. It is well known, for example in [14, Proposition V.§1.2], that finite field extensions $M \subset K \subset L$ satisfy

$$[L : M] = [L : K] \cdot [K : M] \ . \tag{1}$$

A non-algebraic number is *transcendental*, the set of which we denote by $\mathbb{T}$.

Lemma 6. *The function* $\deg : \mathbb{A} \to \mathbb{N},\ a \mapsto \deg(a)$ *is BSS computable.*

We point out that the restriction of deg to algebraic numbers is essential here; in other words: While for reasons of mathematical convenience one can *define* $\deg(x) := \infty$ for transcendental x, a BSS machine cannot *compute* it.

Proof. Exploit that an alternative yet equivalent definition for $\deg(a)$ is given by the degree of a minimal polynomial of a, that is, of an irreducible non-zero $p \in \mathbb{Z}[X]$ with $p(a) = 0$ [14, Proposition V.§1.4].

Therefore we enumerate all non-zero $p \in \mathbb{Z}[X]$ and, for each one, plug in a to test whether $p(a) = 0$. If so, check p for irreducibility — a property in classical $\mathcal{NP}$ by virtue of [5] and thus BSS decidable. If this test succeeds as well, return $\deg(p)$ and terminate; otherwise continue with the next $p \in \mathbb{Z}[X]$. □

Remark 7. An alternative way for deciding irreducibility in $\mathbb{Z}[X]$ — although not within nondeterministic polynomial time — proceeds as follows:

Given $p \in \mathbb{Z}[X]$ of degree $n-1$, choose some n arbitrary distinct arguments $x_1, \ldots, x_n \in \mathbb{Z}$ and multi-evaluate $y_i := p(x_i)$. Observe that, if $q \in \mathbb{Z}[X]$ is a non-trivial divisor of p, then $z_i := q(x_i)$ divides y_i for each $i = 1, \ldots, n$. This suggests to go through all (finitely many) choices for $(z_1, \ldots, z_n) \in \mathbb{Z}^n$ with $z_i | y_i$, to calculate the interpolation polynomial $q \in \mathbb{Q}[X]$ to data (x_i, z_i) and check whether its coefficients are integral.

2.2 Undecidability of $\mathbb{A}$ in $\mathbb{R}$ with Support of a $\mathbb{Q}$–Oracle

In this section, we prove $\mathbb{A} \not\preceq \mathbb{Q}$.

The undecidability of $\mathbb{A}$ *without* further oracle assistance follows similarly to that of $\mathbb{Q}$ from a continuity argument, observing that each, $\mathbb{A}$ and $\mathbb{Q}$ as well as their complements, are dense in $\mathbb{R}$. In fact, algebraic numbers remain dense even when restricting to arbitrary high degree:

Lemma 8. *Let* $x \in \mathbb{R}$, $\varepsilon > 0$, *and* $N \in \mathbb{N}$.
Then, there exists an algebraic real a *of* $\deg(a) = N$ *with* $|x - a| < \varepsilon$.

Proof. Take some arbitrary algebraic real b of degree N, such as $b := 2^{1/N}$. Since $\mathbb{Q}$ is dense in $\mathbb{R} \ni y := x - b$, there exists some rational $r \in \mathbb{Q}$ with $|r - y| < \varepsilon$. Then $a := r + b$ has the desired property. □

Of course, total discontinuity does not prevent a problem to be BSS decidable under the support of a $\mathbb{Q}$–oracle any more as, for example, $\mathbb{Q}$ now is decidable. More precisely a putative algorithm might try distinguishing algebraic from transcendental reals by mapping a given x through some rational function $f \in \mathbb{R}(X)$, then querying the oracle whether the value $f(x)$ is rational or not, and proceeding adaptively depending on the answer.

The following observation basically says that in any sensible such approach, for transcendental x, $f(x)$ will be irrational rather than rational.

Lemma 9. *Let* $f : \mathrm{dom}(f) \subseteq \mathbb{R} \to \mathbb{R}$ *be analytic and non-constant,* $T \subseteq \mathrm{dom}(f)$ *uncountable. Then,* f *maps some* $x \in T$ *to a transcendental, that is,* $f(x) \notin \mathbb{A}$.

Proof. Consider an arbitrary $y \in \mathbb{A}$; by uniqueness of analytic functions [19, THEOREM 10.18], f can map at most countably many different $x \in \mathrm{dom}(f)$ to that single value y. Hence, if $f(x) \in \mathbb{A}$ for all $x \in T$, $f^{-1}(\mathbb{A}) = \bigcup_{y\in\mathbb{A}} f^{-1}(\{y\})$ is a countable union of countable sets and thus countable, too — contradicting the prerequisite that $T \subseteq f^{-1}(\mathbb{A})$ is uncountable. □

So it remains the case of an algorithm trying to map algebraic x to rationals $f(x)$ and transcendental x to irrational $f(x)$. The final ingredient formalizes the intuition that this approach cannot distinguish transcendentals from algebraic numbers of sufficiently high degree:

Proposition 10. *Let $f \in \mathbb{R}(X)$, $f = p/q$ with polynomials p, q of $\deg(p) < n$, $\deg(p) < m$. Let $a_1, \ldots, a_{n+m} \in \mathrm{dom}(f)$ be distinct real algebraic numbers with $f(a_1), \ldots, f(a_{n+m}) \in \mathbb{Q}$.*

a) There are co-prime polynomials $\tilde{p}, \tilde{q}$ of $\deg(\tilde{p}) < n$, $\deg(\tilde{q}) < m$ with coefficients in the algebraic field extension $\mathbb{Q}(a_1, \ldots, a_{n+m})$ such that, for all $x \in \mathrm{dom}(f) = \{x : q(x) \neq 0\} \subseteq \mathbb{R}$, it holds $f(x) = \tilde{f}(x) := \tilde{p}(x)/\tilde{q}(x)$.
b) Let $d := \max_i \deg(a_i)$. Then $f(x) \notin \mathbb{Q}$ for all transcendental $x \in \mathrm{dom}(f)$ as well as for all $x \in \mathbb{A}$ of $\deg(x) > D := d^{n+m} \cdot \max\{n-1, m-1\}$.

Notice that p and q themselves in general do not satisfy claim a); e.g. $p = \pi \cdot \tilde{p}$ and $q = \pi \cdot \tilde{q}$.

Proof. a) Without loss of generality take p and q to be co-prime. Let $y_i := f(a_i)$. The idea is to solve the rational interpolation problem for (a_i, y_i). Already knowing that is *has* a solution (namely p, q) avoids many of the difficulties discussed in [15].

More precisely, observe that the coefficients $p_0, \ldots, p_{n-1}, q_0, \ldots, q_{m-1} \in \mathbb{R}$ of p and q satisfy the homogeneous $(n+m) \times (n+m)$-size system of linear equations

$$\left(\begin{array}{ccccc|cccc} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} & -y_1 & -y_1a_1 & \ldots & -y_1a_1^{m-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} & -y_2 & -y_2a_2 & \ldots & -y_2a_2^{m-1} \\ 1 & a_3 & a_3^2 & \ldots & a_3^{n-1} & -y_3 & -y_3a_3 & \ldots & -y_3a_3^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{array}\right) \cdot \begin{pmatrix} p_0 \\ \vdots \\ p_{n-1} \\ q_0 \\ \vdots \\ q_{m-1} \end{pmatrix} = 0 .$$

In particular, this system has $(p_0, \ldots, q_{m-1}) \in \mathbb{R}^{n+m}$ as non-zero solution.

The coefficients of the matrix live in $\mathbb{Q}(a_1, \ldots, a_{n+m})$. Therefore, GAUSSian Elimination yields a (possibly different) non-zero solution $(\bar{p}_0, \ldots, \bar{q}_{m-1})$, also with entries in $\mathbb{Q}(a_1, \ldots, a_{n+m})$. Now apply the EUCLIDEAN Algorithm to the thus obtained polynomials $\bar{p}, \bar{q}$ and calculate their greatest common divisor $\bar{h}$ which, again, has coefficients in $\mathbb{Q}(a_1, \ldots, a_{n+m})$.

Thus, $\tilde{p} := \bar{p}/\bar{h}$ and $\tilde{q} := \bar{q}/\bar{h}$ are co-prime polynomials over $\mathbb{Q}(a_1, \ldots, a_{n+m})$ of $\deg(\tilde{p}) < n$ and $\deg(\tilde{q}) < m$ such that $\tilde{p} \cdot q$ coincides with $p \cdot \tilde{q}$ on arguments $a_1, \ldots, a_{n+m}$. This implies the latter polynomials of degree less than $n + m$ to be identical: $\tilde{p} \cdot q = p \cdot \tilde{q}$.

It follows that q divides both sides; and co-primality of (p, q) in the factorial ring $\mathbb{R}[X]$ requires that q divides $\tilde{q}$. Similarly, $\tilde{q}$ divides q, yielding $\tilde{q} = \lambda q$ for some $\lambda \in \mathbb{R}$. Analogously, $\tilde{p} = \lambda p$ for the same λ.

b) Consider $x \in \mathbb{R}$ with $y := f(x) \in \mathbb{Q}$ and suppose x is algebraic of $\deg(x) > d^{n+m} \cdot \max\{n-1, m-1\}$ or transcendental. Being, by virtue of a), a zero of the polynomial $\tilde{p} - y \cdot \tilde{q}$ with coefficients from $\mathbb{Q}(a_1, \ldots, a_n)$, x lies in an algebraic extension of the latter field, hence ruling out the case that it is transcendental. More precisely, the degree of x over $\mathbb{Q}(a_1, \ldots, a_n)$ is bounded by $\deg(\tilde{p} - y \cdot \tilde{q})$; and $\deg(x)$, its degree over $\mathbb{Q}$, is at most $\deg(\tilde{p} - y \cdot \tilde{q}) \cdot \deg(a_1) \cdots \deg(a_{n+m}) \leq \max\{n-1, m-1\} \cdot d^{n+m}$ by Equation (1) — contradiction. □

We are finally in the position for the

Proof (of Theorem 4). Suppose some BSS algorithm semi-decides $\mathbb{T}$ in $\mathbb{R}$ with oracle $\mathbb{Q}$ according to Definition 1; in other words, it proceeds by repeatedly evaluating a given $x \in \mathbb{R}$ at functions $f \in \mathbb{R}(X)$ and continuing adaptively according to whether $f(x)$ is positive/zero/negative and rational/irrational, such as to terminate iff $x \in \mathbb{T}$.

Consider this process unrolled into an (infinite yet countable) Decision Tree, each internal node u of which is labeled with an according $f_u \in \mathbb{R}(X)$ and has five successors according to the cases

$0 > f_u(x) \in \mathbb{Q}$ $\quad$ $0 > f_u(x) \notin \mathbb{Q}$ $\quad$ $0 = f_u(x)$ $\quad$ $0 < f_u(x) \in \mathbb{Q}$ $\quad$ $0 < f_u(x) \notin \mathbb{Q}$

with leafs corresponding to terminating computations, that is, to $x \in \mathbb{T}$. Observe that the sets T_v of $x \in \mathbb{T}$ terminating in leaf v give rise to a partition of $\mathbb{T}$. In fact, the at most countably many leafs — as opposed to $\mathbb{T}$ having cardinality of the continuum — require that T_v is uncountable for at least one v.

Consider the path leading from the root to that leaf. W.l.o.g. it contains no branches of type "$0 = f_u(x)$" nor of type "$f_u(x) \in \mathbb{Q}$" that are answered "yes"; for if it does, then the uncountable set T_v of transcendentals x passing through this branch implies that f_u is constant (Lemma 9) and node u thus is dispensable. By possibly changing from $+f_u$ to $-f_u$, we may finally suppose that every branch on the path to leaf v is of type $0 < f_u(x)$.

Summarizing, $T_v \neq \emptyset$ is the set of exactly those $x \in \mathbb{R}$ satisfying $0 < f_u(x) \notin \mathbb{Q}$ for the (finitely many) internal nodes u on the path from the root to v; in particular, $T_v \subseteq \mathrm{dom}(f_u)$. Now take some $t \in T_v \subseteq \mathbb{R}$. Due to continuity of rational functions, there exists $\varepsilon > 0$ such that $f_u(x) > 0$ on all nodes u on that path for any $x \in \mathbb{R}$ satisfying $|x - t| < \varepsilon$. In particular, $f_u(a) > 0$ holds for infinitely many algebraic numbers a of unbounded degree according to Lemma 8. Since by presumption, none of them completes the (terminating) computational path to leaf v, they must branch off somewhere, that is, satisfy $f_u(a) \in \mathbb{Q}$ for some of the finitely many nodes u. However by Proposition 10b), each single f_u can sort out only algebraics of degree up to some finite $D = D(u)$ — a contradiction. □

3 More Undecidable and Incomparable Real Degrees

A further achievement of the works of FRIEDBERG and MUCHNIK was the proof of existence of incomparable r.e. degrees below the Halting problem. In this section, we extend the used techniques to establish in the real case explicit such problems.

More precisely, we shall construct natural incomparable subsets of $\mathbb{A}$. They are given as certain algebraic, infinite extensions of $\mathbb{Q}$ obtained by adjunction of all n-th roots of a fixed prime.

Here, we shall explicitly construct two incomparable problems, only. However, it will then be obvious from the presentation that an uncountable number of incomparable real Turing degrees exist.

3.1 Some Auxiliary Results from Algebra

Let $\mathbb{P} := \{2, 3, 5, 7, \ldots\}$ denote the set of prime numbers. We define the following infinite algebraic extensions of $\mathbb{Q}$:

$$\mathbb{Q}_{\sqrt{2}} := \mathbb{Q}(\{2^{\frac{1}{p}} | p \in \mathbb{P}\}) \quad \text{and} \quad \mathbb{Q}_{\sqrt{3}} := \mathbb{Q}(\{3^{\frac{1}{p}} | p \in \mathbb{P}\}),$$

where the corresponding roots are taken as the smallest positive real that is such a root. Thus, $\mathbb{Q}_{\sqrt{2}}$ results from $\mathbb{Q}$ by field adjunction of all p-th roots of $2, p \in \mathbb{P}$. It is easy to see that $[\mathbb{Q}_{\sqrt{2}} : \mathbb{Q}] = \infty$ and $[\mathbb{Q}_{\sqrt{3}} : \mathbb{Q}] = \infty$. In order to apply the techniques from Section 2 we need the following two results.

Theorem 11. *Let $n \in \mathbb{P}$ and let k be a field. If $a \in k$ is not the n-th power of an element in k, then the field extension $k(\sqrt[n]{a})$ has degree n over k.*

Proof. See [14], Chapter 6, Theorem 9.1.

We would like to guarantee that the elements $2^{\frac{1}{p}}, p \in \mathbb{P}$ do not only have degree p over $\mathbb{Q}$, but as well over $\mathbb{Q}_{\sqrt{3}}$ (and vice versa for elements $3^{\frac{1}{p}}$ and $\mathbb{Q}_{\sqrt{2}}$). In view of the previous theorem it thus suffices to show that $2^{\frac{1}{p}} \notin \mathbb{Q}_{\sqrt{3}}$. Though we strongly assume this to be known we could not find a suitable reference; therefore we add a proof.

Lemma 12. *For all $p \in \mathbb{P}$ it holds $2^{\frac{1}{p}} \notin \mathbb{Q}_{\sqrt{3}}$. Similarly, $3^{\frac{1}{p}} \notin \mathbb{Q}_{\sqrt{2}}$ for all $p \in \mathbb{P}$. Thus $[\mathbb{Q}_{\sqrt{3}}(2^{\frac{1}{p}}) : \mathbb{Q}_{\sqrt{3}}] = p$ and $[\mathbb{Q}_{\sqrt{2}}(3^{\frac{1}{p}}) : \mathbb{Q}_{\sqrt{2}}] = p$ for all $p \in \mathbb{P}$.*

Proof. Suppose to the opposite that $2^{\frac{1}{p}} \in \mathbb{Q}_{\sqrt{3}}$. Then $2^{\frac{1}{p}}$ is already element of a finite extension of $\mathbb{Q}$ with elements $3^{\frac{1}{2}}, 3^{\frac{1}{3}}, \ldots, 3^{\frac{1}{q}}$ for some $q \in \mathbb{P}$. Define $N := \prod_{\substack{i \in \mathbb{P} \\ i \leq q}} i$; it follows that $2^{\frac{1}{p}} \in \mathbb{Q}(3^{\frac{1}{N}})$. We can now proceed almost as in the classical proof of irrationality of $\sqrt{2}$. Suppose $2^{\frac{1}{p}}$ has a representation as $\frac{f(3^{\frac{1}{N}})}{g(3^{\frac{1}{N}})}$ for some polynomials $f, g \in \mathbb{Z}[x]$ such that the integer coefficients of f and g

have 1 as their joint greatest common divisor and such that the occurring powers of $3^{\frac{1}{N}}$ are non-integral. The usual arguments together with $p > 1$ result in the contradiction that 2 divides all those coefficients. The final claim now follows from Theorem 11. □

Since any rational can be incorporated into any minimal polynomial of an element in $\mathbb{Q}_{\sqrt{2}}$ over $\mathbb{Q}_{\sqrt{3}}$ it follows

Corollary 13. *Let $n \in \mathbb{N}$ and let $x \in \mathbb{Q}_{\sqrt{3}}$; for each $\epsilon > 0$ there are infinitely many $y \in \mathbb{Q}_{\sqrt{2}}$ of degree at least n over $\mathbb{Q}_{\sqrt{3}}$ such that $|x - y| < \epsilon$.*

3.2 Existence of Incomparable Degrees

The results from the previous subsection allow to generalize our results to obtain

Theorem 14. *The sets $\mathbb{Q}_{\sqrt{2}}$ and $\mathbb{Q}_{\sqrt{3}}$ are incomparable.*

To prove the theorem we need the following generalization of Proposition 10.

Proposition 15. *Let $f \in \mathbb{R}(X), f = \frac{p}{q}$ with polynomials p, q of degree less than n and m, respectively. Let $a_1, \ldots, a_{n+m} \in \mathbb{Q}_{\sqrt{2}} \cap \mathrm{dom}(f)$ be distinct with $f(a_i) \in \mathbb{Q}_{\sqrt{3}}$.*

a) There are co-prime polynomials $\tilde{p}, \tilde{q}$ of $\deg(\tilde{p}) < n$, $\deg(\tilde{q}) < m$ with coefficients in the algebraic field extension $\mathbb{Q}_{\sqrt{3}}(a_1, \ldots, a_{n+m})$ such that, for all $x \in \mathrm{dom}(f) = \{x : q(x) \neq 0\} \subseteq \mathbb{R}$, it holds $f(x) = \tilde{f}(x) := \tilde{p}(x)/\tilde{q}(x)$.

b) Let d be the maximal degree of an a_i over the field $\mathbb{Q}_{\sqrt{3}}$. Then $f(x) \notin \mathbb{Q}_{\sqrt{3}}$ for all transcendental $x \in \mathrm{dom}(f)$ as well as for all $x \in \mathbb{Q}_{\sqrt{2}}$ of degree $> D := d^{n+m} \cdot \max\{n-1, m-1\}$ over $\mathbb{Q}_{\sqrt{3}}$.

Proof. Follows the same way as Proposition 10. □

Proof (of Theorem 14). We only fill in the missing arguments for showing $\mathbb{Q}_{\sqrt{2}} \not\preceq \mathbb{Q}_{\sqrt{3}}$. Incomparability then follows obviously from that proof.

Assume M to be a machine semi-deciding $\mathbb{R} \setminus \mathbb{Q}_{\sqrt{2}}$ by means of an $\mathbb{Q}_{\sqrt{3}}$-oracle. Follow the proof of Theorem 4 to obtain in just the same way a leaf v together with the related path set $T_v \subseteq \mathbb{R} \setminus \mathbb{Q}_{\sqrt{2}}$. Since T_v is uncountable it contains a transcendental x and in each neighborhood of x by virtue of Lemma 12 and Corollary 13 elements of $\mathbb{Q}_{\sqrt{2}}$ of arbitrarily high degree over the field $\mathbb{Q}_{\sqrt{3}}$. Thus, applying Proposition 15 there exist elements in $\mathbb{Q}_{\sqrt{2}}$ that are branched along v, contradicting the assumed semi-decidability of $\mathbb{R} \setminus \mathbb{Q}_{\sqrt{2}}$. □

As an easy consequence of the above proof we obtain the related result for other extensions of $\mathbb{Q}$ such as $\mathbb{Q}_{\sqrt{p}}$ for $p \in \mathbb{P}$. Clearly, there exist uncountably many sequences of reals that we could attach to $\mathbb{Q}$ in order to get even more incomparable problems (which, however, may be less explicit than $\mathbb{Q}_{\sqrt{p}}$). Thus, we have proven

Theorem 16. *There are uncountably many real recursively enumerable Turing degrees below the real Halting problem.* □

3.3 Some Open Problems

The previous arguments lead to some other problems concerning the relation between some natural subsets of $\mathbb{R}$ that we consider to be interesting.

For $d \in \mathbb{N}$ let $\mathbb{A}_d := \{x \in \mathbb{A} : \deg(x) \le d\} \subset \mathbb{R}$ denote the set of algebraic numbers that have degree at most d over $\mathbb{Q}$.

Problem 1. *Is it true that each step in the following chain is strict?*

$$\mathbb{Q} \preceq \mathbb{A}_2 \preceq \mathbb{A}_3 \preceq \ldots \preceq \mathbb{A} \preceq \mathbb{H}_{\mathbb{R}} \,?$$

We have defined $\mathbb{A}_d$ to consist of numbers of degree *less or* equal to d but point out that considering, rather than $\mathbb{A}_2 =: \mathbb{A}_{\le 2}$, the set $\mathbb{A}_{=2} := \{x \in \mathbb{A} : \deg(x) = 2\}$ of numbers of degree *exactly* 2, in fact makes no difference:

Lemma 17. *It holds* $\mathbb{A}_{=2} \equiv \mathbb{A}_{\le 2}$.

Proof. Based on oracle access to $\mathbb{A}_{\le 2}$, decide $\mathbb{A}_{=2}$ in $\mathbb{R}$ as follows: Upon input of $x \in \mathbb{R}$, query $\mathbb{A}_{\le 2}$ to find out whether $\deg(x) \le 2$. If not, reject; otherwise $x \in \mathbb{A}$ and we may apply Lemma 6 to compute $\deg(x)$.

Conversely, given $\mathbb{A}_{=2}$ as an oracle, decide whether $x \in \mathbb{A}_{\le 2}$ by querying both x and $y := x + \sqrt{2}$. If at least one of them belongs to $\mathbb{A}_{=2}$, then x is surely algebraic and thus applicable to Lemma 6. If $x, y \in \mathbb{R} \setminus \mathbb{A}_{=2}$, we may reject immediately because $\deg(x) < 2$ would imply $x \in \mathbb{Q}$ and thus $y = x + \sqrt{2} \in \mathbb{A}_{=2}$. □

But what about this question for general degrees $d \in \mathbb{N}$?

Problem 2. *Is it true that for all $d \ge 2$ it holds $\mathbb{A}_{=d} \equiv \mathbb{A}_{\le d}$?*

Another interesting question kindly pointed out to us by an anonymous referee would yield, in addition to $\mathbb{Q}$, a vast number of further problems strictly below $\mathbb{H}_{\mathbb{R}}$.

Problem 3. *Does $\mathbb{H}_{\mathbb{R}} \preceq A \subseteq \mathbb{R}^\infty$ imply that A is uncountable?*

Currently we do not see such a proof. And even if, the stronger result $\mathbb{A} \not\preceq \mathbb{Q}$ still would remain.

4 Conclusion

We have shown that oracle access to the set of rational numbers $\mathbb{Q}$ gives a BSS machine additional power but still prevents it from solving the real Halting Problem $\mathbb{H}_{\mathbb{R}}$ (of BSS machines). In addition we proved that there is an uncountable number of incomparable recursively enumerable degrees in the real number setting.

Our proofs do not rely on the ordering available over the real numbers. Thus with small corrections (for example a slightly changed definition of the characteristic path in a potential decision tree) it also yields corresponding results over the complex numbers.

We close with some (necessarily speculative) remarks concerning the raising field of super-Turing computation, that is, concerning hypercomputers of various sorts. While their realizability is questionable and in fact denied by the Church-Turing Hypothesis, recent works put in turn this hypothesis into question [22,11,12]. Since a super-Turing computer capable of solving some problem P can also solve any $L \preceq P$, hypercomputers for higher (Turing-) degrees are necessarily more difficult to realize than for lower ones. Therefore, rather than trying to solve the Halting Problem, it seems more promising to go for some strictly easier yet undecidable one for a start. FRIEDBERG and MUCHNIK's solution P to Post's Problem would be a candidate for this approach, were it not for its inherent non-constructivity. In contrast and over the reals, we have explicitly revealed $\mathbb{Q}$ as an undecidable problem strictly easier than the Halting problem.

One might object that, since '*Natura non facit saltus*' according to LEIBNIZ, the discontinuity inherent in deciding $\mathbb{Q}$ in $\mathbb{R}$ (i.e., of distinguishing fractions from general reals) makes an according hypercomputing device physically impossible. However we point out that for example the Fractional Quantum Hall Effect (Nobel Prize Physics 1998) shows that nature does exhibit exactly this kind of discontinuous behavior.

Acknowledgments. K.MEER is 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). M.ZIEGLER's stay in Odense was made possible by project 21-04-0303 of SNF. We thank the unknown referees for some useful comments.

References

1. 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).
2. 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).
3. L. BLUM, F. CUCKER, M. SHUB, S. SMALE: "*Complexity and Real Computation*", Springer (1998).
4. P. BÜRGISSER: "*Completeness and Reduction in Algebraic Complexity Theory*", Springer (2000).
5. D.G. CANTOR: "Irreducible Polynomials with Integral Coefficients have Succinct Certificates", pp.385–392 in *J. Algorithms* vol.**2** (1981).
6. 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).
7. F. CUCKER: "The arithmetical hierarchy over the reals", pp.375–395 in *Journal of Logic and Computation* vol.**2(3)** (1992).
8. R.M. FRIEDBERG: "Two recursively enumerable sets of incomparable degrees of unsolvability", pp.236–238 in *Proc. Natl. Acad. Sci.* vol.**43** (1957).
9. J.D. HAMKINS, A. LEWIS: "Post's Problem for supertasks has both positive and negative solutions", pp.507–523 in *Archive for Mathematical Logic* vol.**4(6)** (2002).

10. G.T. Herman, S.D. Isard: "Computability over arbitrary fields", pp.73–79 in *J. London Math. Soc.* vol.**2** (1970).
11. M.L. Hogarth: "Non-Turing Computers and Non-Turing Computability", pp.126–138 in *Proc. Philosophy of Science Association* vol.**1** (1994).
12. T. Kieu: "Hypercomputation with Quantum Adiabatic Processes", pp.93–104 in *Theoretical Computer Science* **317** (2004).
13. R. Ladner: "On the structure of polynomial time reducibility", pp.155–171 in *Journal of the ACM*, vol. **22** (1975).
14. S. Lang: "*Algebra*", 3rd Edition Addison-Wesley (1993).
15. N. Macon, D.E. Dupree: "Existence and Uniqueness of Interpolating Rational Functions", pp.751–759 in *The American Mathematical Monthly* vol.**69** (1962).
16. G. Malajovich, K. Meer: "On the Structure of $NP_{\mathbb{C}}$", pp.27–35 in *SIAM Journal on Computing*, vol. **28**, no.1 (1999).
17. K. Meer: "Real Number Models under Various Sets of Operations", pp.366–372 in *J. Complexity* vol.**9** (1993).
18. E.L. Post: "Recursively enumerable sets of positive integers and their decision problems", pp.284–316 in *Bull. Amer. Math. Soc.* vol.**50** (1944).
19. W. Rudin: "*Real and Complex Analysis*", McGraw-Hill (1966).
20. U. Schöning: "A uniform approach to obtain diagonal sets in complexity classes", pp.95–103 in *Theoretical Computer Science*, vol.**18** (1982).
21. R.I. Soare: "*Recursively Enumerable Sets and Degrees*", Springer (1987).
22. A. C.-C. Yao: "Classical Physics and the Church-Turing Thesis", pp.100–105 in *J. ACM* vol.**50(1)** (2003).