Descriptive Complexity Theory over the Real Numbers

Erich Grädel*   Klaus Meer†

RWTH Aachen

Abstract

We present a logical approach to complexity over the real numbers with respect to the model of Blum, Shub and Smale.

The logics under consideration are interpreted over a special class of two-sorted structures, called $\mathbb{R}$-*structures*: They consist of a finite structure together with the ordered field of reals and a finite set of functions from the finite structure into $\mathbb{R}$. They are a special case of the *metafinite structures* introduced recently by Grädel and Gurevich. We argue that $\mathbb{R}$-structures provide the right class of structures to develop a descriptive complexity theory over $\mathbb{R}$. We substantiate this claim by a number of results that relate logical definability on $\mathbb{R}$-structures with complexity of computations of BSS-machines.

1 Introduction

Computations with real numbers. In 1989 Blum, Shub, and Smale [1] introduced a model for computations over the real numbers (and other rings as well) which is now usually called a BSS machine. The important difference with, say, the Turing model is that real numbers are treated as basic entities and that arithmetic operations on the reals are performed in a single step, independently of the magnitude or complexity of the involved numbers. In particular, the model abstracts from the problems that in actual computers real numbers have to be approximated by bit-sequences, that the complexity of arithmetic operations depends on the length of these approximate representations, from rounding errors and from the problem that exact testing for 0 is impossible in practice. Similar notions of computations over arbitrary fields or rings had been investigated earlier in *algebraic complexity theory* (see [20, 24, 26] for survey articles and the forthcoming book [2] for a comprehensive treatment). A novelty of the approach of Blum, Shub and Smale is that their model is uniform (for all input-lengths) whereas the notions explored in algebraic complexity (straight-line programs, arithmetic circuits, decision trees) are typically nonuniform. One of the main purposes of the BSS approach was to create a uniform complexity theory dealing with problems having an analytical and topological background, and to show that certain problems remain hard even if arbitrary reals are treated as basic entities.

Many basic concepts and fundamental results of classical computability and complexity theory reappear in the BSS model: the existence of universal machines, the classes $\mathrm{P}_{\mathbb{R}}$ and $\mathrm{NP}_{\mathbb{R}}$ (real analogues of P and NP) and the existence of $\mathrm{NP}_{\mathbb{R}}$-complete problems. Of course these notions appear in a different form, with a strong analytic flavour: typical examples of undecidable, recursively enumerable sets are complements of certain Julia sets, and the first problem that was shown to be $\mathrm{NP}_{\mathbb{R}}$-complete is the question whether a given multivariate polynomial of degree four has a real root [1]. Like in the Boolean setting all problems in the class $\mathrm{NP}_{\mathbb{R}}$ are decidable within single exponential time (but this is not as trivial as in the classical case) and the $\mathrm{P}_{\mathbb{R}}$ versus $\mathrm{NP}_{\mathbb{R}}$ question is one of the major open problems .

However, there also are many differences between Boolean and real complexity theory. Just to mention a few we note that the meaning of space resources seems to be very different (cf. [22] and section 6 below), that certain separation results can be established (like $\mathrm{NC}_{\mathbb{R}} \subsetneq \mathrm{P}_{\mathbb{R}}$ and $\mathrm{NP}_{\mathbb{R}} \subsetneq \mathrm{EXP}_{\mathbb{R}}$ [3]) which are open in the Boolean theory, and that some discrete problems seem to change their complexity behaviour when considered in the BSS model (cf. [21]). Nevertheless even from the discrete point of view the continuous approach provides interesting results; in particular, Boolean parts of real complexity classes bear a strong relationship to the classical theory (see [19, 4] and the references given there).

Logics that capture complexity classes. While

*Lehrgebiet Mathematische Grundlagen der Informatik, RWTH Aachen, D-52056 Aachen, graedel@informatik.rwth-aachen.de

†Lehrstuhl C für Mathematik, RWTH Aachen, D-52056 Aachen, meer@rwth-aachen.de. Partially supported by EC-Project NeuroCOLT.

STOC ' 95, Las Vegas, Nevada, USA
© 1995 ACM 0-89791-718-9/95/0005..$3.50

computational complexity theory is concerned with the amount of resources like time or space that are neccessary to solve a problem, *descriptive complexity theory* is a branch of finite model theory, that considers the logical complexity of defining a property or query, and relates computational complexity with logical definability.

One of the most important results is Fagin's theorem [8] which provides a purely logical, machine-independent characterization of NP: Let L be an isomorphism-closed class of finite structures of a fixed, nonempty signature. Then L is in NP if and only if there exists an existential second-order sentence ψ such that L is precisely the class of finite models of ψ. Some years later, Immerman and Vardi [15, 25] proved that, on ordered structures, the problems solvable in polynomial time are exactly those definable in least fixed-point logic. Immerman [15]–[18] systematically studied the problem of capturing complexity classes by logical languages and came up with logical characterizations for most of the major complexity classes. The most important results in this field are surveyed in [14, 18].

These logical characterizations of complexity are model theoretic and based either on fragments of second-order logic [8, 10] or on extensions of first-order logic by additional means to construct new relations (such as fixed point operators). There also is a different, functional approach which draws more on recursion theory than model theory. Gurevich proved that interpreting the classical calculus of primitive recursive functions (resp. recursive functions) over finite successor structures gives precisely the log-space (resp. polynomial time) computable global functions [13, 14]. A variant of the latter result was also obtained by Sazonov [23].

It should be noted, that for complexity classes below NP, precise logical characterizations have been obtained only on ordered structures. The problem whether there exists a logic capturing precisely the polynomial-time computable queries on arbitrary finite structures is still open.

Metafinite models and a descriptive complexity theory over $\mathbb{R}$. In many areas of computer science (e.g. databases, optimization, fault-tolerant networks) there arise objects that consist of a finite structure together with a collection of numbers from an infinite numerical domain, on which arithmetical operations are performed. To reason about such objects in an adequate way, Grädel and Gurevich have recently introduced *metafinite structures* [12]. Metafinite model theory should be viewed as a possibility for going beyond finite models, in order to integrate logical queries to finite structures with arithmetical operations on numbers from an infinite structure like, e.g., the ring of integers or the ordered field of reals. To avoid problems pertinent to typical infinite numerical structures — e.g. the undecidability of arithmetic — Grädel and Gurevich have investigated a number of logics for metafinite models that extend the usual logics on finite structures by *restricted access* to the infinite numerical domain. The relationship of metafinite model theory with other proposal (most notably from database theory) for combining finite structures with infinite numerical domains is also discussed in [12].

In this paper we exploit metafinite models to develop a logical approach to complexity over $\mathbb{R}$ for the BSS model, and obtain results that parallel those of descriptive complexity theory in the Boolean case. Indeed, the first problem for such an approach is to define the right class of structures to model in a convincing way the computational problems that we are interested in, and to admit logical reasoning about computations of BSS machines within natural logical languages. Since we are dealing with the ordered field of reals, we are not in the realm of finite model theory anymore. On the other side, the model theory of real closed fields, or of the ring $\mathbb{R}^\infty$ do not provide the right framework either. What is needed is a clear separation between the finite, discrete aspects of problems and computations (like indices of tuples, time, indices of registers, the finite control of the machines) on one side and the arithmetic of real numbers on the other side.

This can be achieved by $\mathbb{R}$-structures, which are a special case of metafinite models. They consist of a finite structure $\mathfrak{A}$, together with the ordered field of reals and a finite set of functions from $\mathfrak{A}$ into $\mathbb{R}$. We discuss a number of logical languages on $\mathbb{R}$-structures and investigate their expressive power. We argue that $\mathbb{R}$-structures provide the right class of structures to develop a desciptive complexity theory over $\mathbb{R}$. We substantiate this claim by the following results:

- An appropriate variant of existential second order logic on $\mathbb{R}$-structures, denoted $(\mathrm{SO}\ \exists)_{\mathbb{R}}$, with existential quantification over functions from the finite part of the structure into $\mathbb{R}$, captures $\mathrm{NP}_{\mathbb{R}}$. This is the analogue over $\mathbb{R}$ to Fagin's Theorem.

- We design a fixed-point logic for *partial functions* from finite domains into $\mathbb{R}$ and show that on ordered $\mathbb{R}$-structures, this logic captures $\mathrm{P}_{\mathbb{R}}$. We thus also have a real analogue to the theorem of Immerman and Vardi.

- We investigate appropriate variants of the calculus of primitive recursive and recursive functions over ordered $\mathbb{R}$-structures. The recursive global functions capture precisely polynomial-time, whereas the primitive recursive global functions coincide with the functions computable by BSS machines in polynomial-time with constant space. As a consequence, there exist primitive recursive global functions which are not in $\mathrm{NC}_{\mathbb{R}}$.

- We exhibit problems that are complete for $\mathrm{P}_{\mathbb{R}}$ and $\mathrm{NP}_{\mathbb{R}}$ under first-order reductions.

We believe that these results give sufficient evidence that metafinite model theory provides the right framework for a descriptive complexity over $\mathbb{R}$.

2 Computability and complexity theory over the real numbers

Let $\mathbb{R}^\infty := \bigcup_{k\in\mathbb{N}}\mathbb{R}^k$, or equivalently, the set of functions $X : \mathbb{N} \rightarrow \mathbb{R}$ with $X(n) = 0$ for all but finitely many n. For any $X \in \mathbb{R}^\infty$, we call $|X| := \max\{n : X(n) \neq 0\}$ the *length* of X. Note that $\mathbb{R}^\infty \times \mathbb{R}^\infty$ can be identified with $\mathbb{R}^\infty$ in a natural way by concatenation. A *decision problem* is a pair (F, F^+) where $F^+ \subseteq F \subseteq \mathbb{R}^\infty$.

A *Blum-Shub-Smale machine* — in the sequel called a BSS-machine — is essentially a Random Access Machine over $\mathbb{R}$ which can evaluate rational functions at unit cost and whose registers can store arbitrary real numbers.

Definition 2.1 [1] A *BSS-machine* M over $\mathbb{R}$ is given by a finite set I of instructions labelled by $0, \ldots, N$. The input and output spaces are subsets of $\mathbb{R}^\infty$. A configuration is a quadruple $(k, r, w, x) \in I \times \mathbb{N} \times \mathbb{N} \times \mathbb{R}^\infty$, where k is the instruction currently executed, r and w are the numbers of the so called "copy registers" (see below) and x describes the content of the registers of the machine. On input $x \in \mathbb{R}^\infty$, the computation is started with configuration $(0, 0, 0, x)$. If $k = N$ the computation stops; in that case the value of x is the output computed by the machine. The instructions are of the following types:

computation: $k : x_0 \leftarrow g_k(x)$ where g_k is a rational function on $\mathbb{R}^\infty$. The next instruction will be $k+1$, the copy-registers are updated according to either $r \leftarrow r+1$ or $r \leftarrow 0$ and similarly for w. The other registers remain unchanged.

branch: k: **if** $x_0 \geq 0$ **goto** $\beta(k)$ **else goto** $k+1$. The contents of the registers remain unchanged.

copy: $k : x_w \leftarrow x_r$, i.e. the content of the "read-register" is copied into the "write-register". The next instruction is $k+1$; all other registers remain unchanged.

Remarks. The rational function g_k evaluated by instruction k depends on a fixed finite collection $x_{i_1}, \ldots, x_{i_s}$ of components of x. The finite set of real constants appearing in the functions g_k are called the *machine constants* of M. Up to an increase of running times by a constant factor, the power of BSS-machines does not change if one restricts the computation-instructions to the basic operations $+, -, \cdot, /$ and assignments $x_0 \leftarrow \alpha$ where α belongs to a fixed finite set of reals (the machine-constants of M).

Definition 2.2 $\mathrm{P}_{\mathbb{R}}$ is the class of all decision problems (F, F^+) for which there exists a polynomial-time machine over $\mathbb{R}$ which decides, for every given $X \in F$, whether $X \in F^+$. The analogue of NP is the class $\mathrm{NP}_{\mathbb{R}}$ of decision problems (F, F^+) for which there exists a decision problem $(G, G^+) \in \mathrm{P}_{\mathbb{R}}$ and a constant k such that $G = \{(X, Y) \in F \times \mathbb{R}^\infty : |Y| \leq |X|^k\}$ and

$$F^+ = \{X \in F : (\exists Y \in \mathbb{R}^\infty)(X, Y) \in G^+\}.$$

Equivalently, $\mathrm{NP}_{\mathbb{R}}$ can be defined as the class of decision problems decided in polynomial time by a *nondeterministic* BSS-machine, i.e. a BSS-machine that can nondeterministically guess tuples $Y \in \mathbb{R}^\infty$ at cost $|Y|$. In particular, during a polynomial-time computation on input X, the concatenation of the tuples guessed by a nondeterministic BSS-machine gives a tuple $Y \in \mathbb{R}^\infty$ with $|Y| \leq |X|^k$ for some fixed $k \in \mathbb{N}$.

3 Logic on $\mathbb{R}$-structures

Let $\mathfrak{R} = (\mathbb{R}, +, -, \cdot, /, \mathrm{sgn}, <, (c_r)_{r\in\mathbb{R}})$ be the ordered field of real numbers. We include subtraction and division as primitive operations and assume that every element $r \in \mathbb{R}$ is named by a constant c_r in order to write every rational function $g : \mathbb{R}^k \longrightarrow \mathbb{R}$ as a term (without quantifiers). In addition we have included the function

$$\mathrm{sgn}(x) := \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases}$$

which clearly is efficiently computable, but is not a rational function. It turns out, that for logical descriptions it is often more convenient to use the sign function rather than the ordering relation.

$\mathbb{R}$-structures consist of a finite structure $\mathfrak{A}$ together with a finite set of functions from $\mathfrak{A}$ into $\mathbb{R}$. They are special kinds of the *metafinite structures* introduced by Grädel and Gurevich. For developping a descriptive complexity theory for computions over the reals it is appropriate to model inputs by $\mathbb{R}$-structures, viewing the finite part as an (ordered) set of indices.

Let Υ_a, Υ_w be finite vocabularies where Υ_a may contain relation and function symbols, and Υ_w contains function symbols only.

Definition 3.1 An $\mathbb{R}$-*structure* of vocabulary (Υ_a, Υ_w) is a triple $\mathfrak{D} = (\mathfrak{A}, \mathfrak{R}, W)$ consisting of *(i)* a finite structure $\mathfrak{A}$ of vocabulary Υ_a, called the primary part of $\mathfrak{D}$;

(ii) the (infinite) structure $\mathfrak{R}$, called the secondary part of $\mathfrak{D}$;

(iii) a finite set W of functions: $X : A^k \rightarrow \mathbb{R}$ interpreting the function symbols in Υ_w. Here A is the universe of $\mathfrak{A}$.

We let $|\mathfrak{D}|$ be the cardinality of A, i.e. of the primary part of $\mathfrak{D}$. A simple class of $\mathbb{R}$-structures is obtained by letting $\mathfrak{A} = (\{1, \ldots, k\}, <)$ be a finite ordered set and W consists of a single unary function $X : \{1, \ldots, k\} \rightarrow \mathbb{R}$. Obviously this class models $\mathbb{R}^\infty$.

Definition 3.2 An $\mathbb{R}$-structure $\mathfrak{D} = (\mathfrak{A}, \mathfrak{R}, W)$ is called *ranked* if W contains a function $E : A \rightarrow \mathbb{R}$ which is a bijection from A to $\{0, \ldots, |A| - 1\}$. In this case, E is called a *ranking*. It defines a linear order on A. An *m-ranking* is a bijection E_m from A^m to $\{0, \ldots, |A|^m - 1\} \subseteq \mathbb{R}$. Every ranking induces lexicographic m-rankings, for all $m \in \mathbb{N}$.

First-order logic. Fix a countable set $V = \{t_0, t_1, \ldots,\}$ of variables. These variables range only over the primary part; we don't use element variables taking values in the secondary part.

The language $\mathrm{FO}_\mathbb{R}$ contains, for each vocabulary $\Upsilon = (\Upsilon_a, \Upsilon_w)$, a set $\mathrm{FO}_\mathbb{R}(\Upsilon)$ of formulae and terms. Each term takes, when interpreted in some $\mathbb{R}$-structure, values in either the primary part, in which case we call it an *index term*, or in $\mathbb{R}$, in which case we call it a *number term*. Terms are defined inductively as follows

- The set of index terms is the closure of the set V of variables under applications of function symbols of Υ_a.
- Every constant c_r is a number term.
- If $s_1, \ldots, s_k$ are index terms and X is a k-ary function symbol of Υ_w then $X(s_1, \ldots s_k)$ is a number term.
- If f, g are number terms, then so are $f + g$, $f - g$, $f \cdot g$, f/g and $\mathrm{sgn}(f)$.

Atomic formulae are equalities $s = s'$ of index terms, equalities $f = g$ of number terms, expressions $Ps_1 \cdots s_k$ where P is a k-ary predicate symbol in Υ_a and $s_1, \ldots, s_k$ are index terms, and inequalities $f < g$ of number terms.

The set of formulae of $\mathrm{FO}_\mathbb{R}$ is the smallest that contains all atomic formulae and is closed under Boolean connectives and quantification $(\exists t)\psi$ and $(\forall t)\psi$. Note that we do *not* build formulae $(\exists x)\psi$ where x ranges over $\mathbb{R}$.

Second-order logic. Second order-logic on $\mathbb{R}$-structures is the logic $\mathrm{SO}_\mathbb{R}$ obtained by adding to $\mathrm{FO}_\mathbb{R}$ the possibility to quantify over function symbols.

We say that ψ is an *existential second-order sentence* (of vocabulary (Υ_a, Υ_w)) if $\psi = \exists Y_1 \ldots \exists Y_r \varphi$ where φ is a first-order sentence in $\mathrm{FO}_\mathbb{R}$ of vocabulary $(\Upsilon_a, \Upsilon_w \cup \{Y_1, \ldots, Y_r\})$.

4 $\mathrm{NP}_\mathbb{R}$ and existential second-order logic

Encodings. We showed that $\mathbb{R}^\infty$ can be modelled by $\mathbb{R}$-structures in a natural way. Conversely every $\mathbb{R}$-structure $\mathfrak{D} = (\mathfrak{A}, \mathfrak{R}, W)$ can be encoded by a tuple $e(\mathfrak{D}) \in \mathbb{R}^\infty$ in the following way:

Choose a ranking on A and replace all functions and relations in the primary part by the apprioriate characteristic functions $\chi : A^k \rightarrow \{0, 1\} \subseteq \mathbb{R}$. This gives a structure whose primary part is a plain set A, with functions $X_1, \ldots, X_t$ of the form $X_i : A^k \rightarrow \mathbb{R}$ and with the ranking $E : A \rightarrow \mathbb{R}$. Each of the functions X_i can be represented by a tuple $x_0, \ldots, x_{m-1} \in \mathbb{R}^m$ where $m = |A|^k$ and $x_i = X(\bar{a}(i))$ where $\bar{a}(i)$ is the i-th tuple in A^k with respect to the k-ranking induced by E. The concatenation of these tuples gives the encoding $e(\mathfrak{D})$. Note that $e(\mathfrak{D})$ depends on the ranking that was chosen.

Obviously, for structures $\mathfrak{D}$ of a fixed finite signature, the length of $e(\mathfrak{D}) \in \mathbb{R}^\infty$ is bounded by some polynomial n^ℓ where $n = |\mathfrak{D}|$ and ℓ depends only on the signature. Thus we can also view $e(\mathfrak{D}) = (x_0, \ldots, x_{n^\ell - 1})$ as a single function $X_\mathfrak{D} : A^\ell \rightarrow \mathbb{R}$ where $X(\bar{a}(i)) = x_i$ for all $i < n^\ell$. This means that encoding an $\mathbb{R}$-structure in $\mathbb{R}^\infty$ basically means representing the whole structure by a single function (of appropriate arity) from $\{0, \ldots, n-1\}$ into $\mathbb{R}$.

Furthermore this encoding is first-order definable in the following sense:

Lemma 4.1 *For every signature (Υ_a, Υ_w), there exists a first-order formula $code(X, E)$ of signature $(\Upsilon_a, \Upsilon_w \cup \{X, E\})$ such that for all $\mathbb{R}$-structures $\mathfrak{D}$ of signature Υ, for all rankings E and for all functions X*

$$(\mathfrak{D}, X, E) \models code(X, E) \quad \textit{iff} \quad X = e(\mathfrak{D}).$$

Without loss of generality we view a decision problem as a pair (F, F^+) where F and F^+ are sets of $\mathbb{R}$-structures (of some fixed vocabulary) which are closed under isomorphisms, and where $F^+ \subseteq F$. When we say, that a decision problem (F, F^+) of $\mathbb{R}$-structures is in $\mathrm{P}_\mathbb{R}$ or $\mathrm{NP}_\mathbb{R}$, we actually mean that $(e(F), e(F^+))$ are in $\mathrm{P}_\mathbb{R}$ or $\mathrm{NP}_\mathbb{R}$, where $e(F) = \{e(\mathfrak{D}) : \mathfrak{D} \in F\} \subseteq \mathbb{R}^\infty$ and similarly for F^+.

When $(F, F^+) \in \mathrm{NP}_{\mathbb{R}}$ we have a decision problem $(G, G^+) \in \mathrm{P}_{\mathbb{R}}$, and we can view the structures in G as expansion of the structures $\mathfrak{D} \in F$ by a k-ary function $Y : A^k \rightarrow \mathbb{R}$.

The following theorem is the analogous result in the real setting to Fagin's Theorem.

Theorem 4.2 *Let (F, F^+) be a decision problem of $\mathbb{R}$-structures. Then the following two statements are equivalent.*

(i) $(F, F^+) \in \mathrm{NP}_{\mathbb{R}}$;

(ii) there exists an existential second-order sentence ψ such that $F^+ = \{\mathfrak{D} \in F : \mathfrak{D} \models \psi\}$.

Proof. It is easy to see that *(ii)* implies *(i)*. For the converse, let $(F, F^+) \in \mathrm{NP}_{\mathbb{R}}$ and let (G, G^+) be the corresponding problem in $\mathrm{P}_{\mathbb{R}}$, with $G = \{(\mathfrak{D}, Y) : \mathfrak{D} \in F,\ Y$ a k-ary function$\}$ and $F^+ = \{\mathfrak{D} \in F : \exists Y((\mathfrak{D}, Y) \in G^+)\}$.

Let M be a polynomial-time BSS-machine deciding (G, G^+), and m be a natural number such that M stops on $(\mathfrak{D}, Y)$ after less than n^m steps and uses at most $n^m - 3$ registers where $n = |\mathfrak{D}|$.

We first suppose that we have a ranking $E : A^m \rightarrow \mathbb{R}$ available. From E, the induced m-ranking E_m is first-order definable: we can identify the element in A of maximal rank and thus have the number term n available; we then can use $E_m(\bar{t})$ as an abbreviation for

$$E(t_1)n^{m-1} + \cdots E(t_{m-1})n + E(t_m).$$

We can then identify A^m with the initial subset $\{0, \ldots, n^m - 1\}$ of $\mathbb{N}$. Thus, in the formulae to be constructed below, m-tuples $\bar{t} = t_1, \ldots, t_m$ of variables are considered to range over natural numbers $t < n^m$. Conditions like $\bar{t} = 0$ or $\bar{t} = \bar{s} + \bar{s}'$ can then be expressed by $\mathrm{FO}_{\mathbb{R}}$-formulae of vocabulary $\{E\}$.

The computation of M on a given input $(\mathfrak{D}, Y)$ can be represented by a function $Z : A^{2m} \rightarrow \mathbb{R}$, as follows.

- $Z(0, \bar{t})$ is the instruction executed by M at time $\bar{t}$.
- $Z(1, \bar{t})$ and $Z(2, \bar{t})$ are the indices of the read and the write-registers of M at time $\bar{t}$.
- $Z(\bar{j} + 3, \bar{t})$ is the content of register $\bar{j}$ at time $\bar{t}$.

We construct a first-order formula ψ with the property that for all ranked structures $(\mathfrak{D}, Y) \in G$ and all Z, we have that $(\mathfrak{D}, Y, Z) \models \psi$ iff Z represents an accepting computation of M on $e(\mathfrak{D}, Y)$.

We first have to express that for time $t = 0$, the function Z encodes the input configuration of M on $(\mathfrak{D}, Y)$. Thus we need a subformula, stating that $Z(i, 0) = 0$ for $i = 0, 1, 2$ and that the values $Z(\bar{j} + 3, 0)$ encode the input $(\mathfrak{D}, Y)$. By Lemma 4.1 this can be expressed in first-order logic.

Second, we have to ensure that for every $t < n^m - 1$, if the sequence $\langle Z(\bar{j}, \bar{t}) : \bar{j} = 0, \ldots, n^m - 1 \rangle$ represents a configuration of M, then the sequence of values $Z(\bar{j}, \bar{t} + 1)$ represents the successor configuration. The formula asserting this has the form

$$\forall \bar{t} \bigwedge_{k=0}^{N} (Z(0, \bar{t}) = k \ \rightarrow \ \varphi_k)$$

where φ_k describes transitions performed by instruction k.

Consider for example a computation instruction of the form $k : x_0 \leftarrow g(x_0, \ldots, x_\ell)$, and assume in addition that it increases the index of the read-register by 1 and sets back the index of the write register to 0.

The formula φ_k then has to express the following

- $Z(0, \bar{t} + 1) = k + 1$ (the next instruction is $k + 1$);
- $Z(1, \bar{t} + 1) = Z(1, \bar{t}) + 1$ (the read-register index is increased by 1);
- $Z(2, \bar{t} + 1) = 0$ (the write-register index is set back to 0);
- $Z(3, \bar{t} + 1) = g(Z(3, \bar{t}), Z(4, \bar{t}), \ldots, Z(\ell + 3, \bar{t}))$ (into register 0, M writes the result of applying the rational function g to the register contents at time $\bar{t}$).
- $Z(\bar{j}, \bar{t} + 1) = Z(\bar{j}, \bar{t})$ for all $\bar{j} > 3$ (the other registers remain unchanged).

Clearly, these conditions are first-order expressible. It should be noted that whenever $f_0, \ldots, f_\ell$ are number terms and $g : \mathbb{R}^\ell \rightarrow \mathbb{R}$ is a rational function, then $g(f_0, \ldots, f_\ell)$ is also a number term.

For another example illustrating the explicit use of the embbeding function, consider a copy instruction $k : x_w \leftarrow x_r$. Here the formula has to express (besides update of the instruction number etc. which are done as above), that the content of the register $Z(2, \bar{t})$ at time $\bar{t} + 1$ is the same as the content of the register $Z(1, \bar{t})$ at time $\bar{t}$. This is expressed by the formula

$$\forall \bar{j} \forall \bar{j}'([Z(1, \bar{t}) = E_m(\bar{j}) \wedge Z(2, \bar{t}) = E_m(\bar{j}')]$$
$$\rightarrow Z(\bar{j}' + 3, \bar{t} + 1) = Z(\bar{j} + 3, \bar{t})).$$

To express that M accepts its input, we just have to say that $Z(3, n^m - 1) = 1$ (by convention, the result of the computation, if it is a single number, is stored in register 0).

Combining all these subformulae in the appropriate way, we obtain the desired formula ψ. It then follows that for all structures $\mathfrak{D} \in F$

$$\mathfrak{D} \in F^+ \quad \text{iff}\ \mathfrak{D} \models (\exists Y)(\exists Z)\psi$$

which proves the theorem for the case of ranked structures.

Finally, we do away with the assumption that the input structures be ranked. Indeed, if no ranking is given on structures $\mathfrak{D} \in F$ we can introduce one by existentially quantifying over the function E and adding a conjunct $\alpha(E)$ which asserts that E is one-one and that for all t with $E(t) \neq 0$ there exists an element s such that $E(s) + 1 = E(t)$. It follows that

$$F^+ = \{\mathfrak{D} \in F : \mathfrak{D} \models (\exists E)(\exists Y)(\exists Z)(\alpha \wedge \psi).$$

■

Example: An NP$_\mathbb{R}$-complete problem and its logical description. Let F^4 denote the set of all degree four polynomials in n unknowns (where $n \in \mathbb{N}$ is arbitrary) and F^4_{zero} those having a real zero. The problem (F^4, F^4_{zero}) is $NP_\mathbb{R}$-complete [1]. Consider an $\mathbb{R}$-structure $\mathfrak{D} = (\mathfrak{A}, \mathfrak{R}, W)$ where $A = (\{0, \ldots, n\}, <, 0, n)$ and W consists of a function $C : A^4 \rightarrow \mathbb{R}$. $\mathfrak{D}$ defines a *homogenous* polynomial $g \in \mathbb{R}[X_0, \ldots, X_n]$ of degree four, namely

$$g = \sum_{i,j,k,\ell} C(i,j,k,\ell) X_i X_j X_k X_\ell.$$

We obtain an arbitrary (i.e., not necessarily homogenous) polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$ of degree four by setting $X_0 = 1$ in g.

An (SO $\exists$)$_\mathbb{R}$ sentence for (F^4, F^4_{zero}) quantifies two functions $X : A \rightarrow \mathbb{R}$ and $Y : A^4 \rightarrow \mathbb{R}$ where $X(1), \ldots, X(n)$ describes the zero and $Y(u)$ is the partial sum of all monomials up to $u \in A^4$ in $f(X_1, \ldots, X_n)$ (according to the lexicographical order on A^4). Thus (F^4, F^4_{zero}) is described by the following sentence ψ:

$$(\exists X)(\exists Y)\Big(Y(\bar{0}) = C(\bar{0}) \wedge Y(\bar{n}) = 0 \wedge$$
$$\forall \bar{u}(\bar{u} \neq \bar{0} \rightarrow Y(\bar{u}) = Y(\bar{u} - 1) + C(\bar{u}) \prod_{i=1}^{4} X(u_i))\Big).$$

Indeed, $\mathfrak{D} \models \psi$ if and only if the polynomial f of degree four defined by $\mathfrak{D}$ has a real zero.

5 A fixed point logic for $\mathbb{R}$-structures

For simplicity, we restrict attention now to *functional* $\mathbb{R}$-structures, or $\mathbb{R}$-*algebras*, whose primary part is a plain set A, i.e. $\Upsilon_a = \varnothing$. This is no loss of generality, since we can replace any relation $P \subseteq A^k$ by its characteristic function, considered as a function $\chi_P : A^k \rightarrow \mathbb{R}$.

Furthermore we will allow *partially defined* functions from the primary part into $\mathbb{R}$. Formally we define a *partial* $\mathbb{R}$-*algebra* as an $\mathbb{R}^*$-algebra where $\mathbb{R}^*$ is the extension of $\mathbb{R}$ to $\mathbb{R}^* = \mathbb{R} \cup \{\text{undef}\}$. The basic operations on $\mathbb{R}$ are extended to $\mathbb{R}^*$ by

$$a + \text{undef} = a - \text{undef} = \text{undef}$$
$$a \cdot \text{undef} = a/\text{undef} = \begin{cases} 0 & \text{if } a = 0 \\ \text{undef} & \text{if } a \neq 0 \end{cases}$$
$$\text{sgn}(\text{undef}) = \text{undef}$$

We define a *functional fixed-point calculus of number terms* by closing the set of first-order number terms, as defined in section 3, under a *maximization rule* and a *fixed point rule.*

Maximization rule: If $F(s, \bar{t})$ is a number term with free variables $s, \bar{t}$, then

$$\max_s F(s, \bar{t})$$

is also a number term with free variables $\bar{t}$, and the obvious semantic. Maximization may be seen as a functional substitute for existential quantifiers.

The notion of a functional fixed point is more complicated. Fix a signature Υ_w and a function symbol Z not contained in this signature. Let $F(Z, \bar{t})$ be a number term of signature $\Upsilon_w \cup \{Z\}$ and free variables $\bar{t} = t_1, \ldots, t_r$ where r is the arity of Z. We write $F^{\mathfrak{D},Z}(\bar{t})$ for the value of $F(Z, \bar{t})$ for a given interpretation $(\mathfrak{D}, Z)$.

For every $\mathbb{R}^*$-algebra $\mathfrak{D}$ of signature Υ_w, the term $F(Z, \bar{t})$ gives rise to an operator $F^\mathfrak{D}$ which updates *partially defined* functions Z as follows:

$$(F^\mathfrak{D} Z)(\bar{t}) := \textbf{if } Z(\bar{t}) = \text{undef } \textbf{then } F^{\mathfrak{D},Z}(\bar{t}) \textbf{ else } Z(\bar{t})$$

This gives an inductive definition of a sequence of partial functions $Z^j : A^r \rightarrow \mathbb{R}$.

$$\begin{aligned} Z^0(\bar{t}) &= \text{undef} \quad (\text{for all } \bar{t}) \\ Z^{j+1} &= F^\mathfrak{D} Z^j. \end{aligned}$$

Since the operator $F^\mathfrak{D}$ updates Z only at points where Z is undefined, this process becomes saturated after polynomially many iterations: $Z^j = Z^{j+1}$ for some $j < |A|^r$. We denote this fixed point by Z^∞ and call it the *fixed point of* $F(Z, \bar{t})$ *on* $\mathfrak{D}$.

Fixed point rule: Given a number term $F(Z, \bar{t})$ of signature $\Upsilon_w \cup \{Z\}$, a tuple $\bar{t} = t_1, \ldots, t_r$ of variables (where r is the arity of Z), and a tuple $\bar{u} = u_1, \ldots, u_r$ of number terms, we build a new number term

$$\textbf{fp}[Z(\bar{t}) \leftarrow F(Z, \bar{t})](\bar{u})$$

of signature Υ_w. Its semantic, on a given $\mathfrak{R}^*$-algebra $\mathfrak{D}$, is $Z^\infty(\bar{u})$.

Definition 5.1 *Functional fixed point logic for* $\mathbb{R}$-*algebras*, denoted $\mathrm{FFP}_{\mathbb{R}}$, is obtained by closing the set of first-order number terms under the maximization rule, under the basic operations $+, -, \cdot, /$, sgn of $\mathbb{R}$ and under the fixed point rule.

Proposition 5.2 $\mathrm{FFP}_{\mathbb{R}} \subseteq \mathrm{P}_{\mathbb{R}}$.

The same techniques (e.g. Ehrenfeucht-Fraïssé games) that apply to fixed point logic on finite structures show that $\mathrm{FFP}_{\mathbb{R}}$ does not capture the full power of polynomial-time BSS-machines. For instance, there is no number term of $\mathrm{FFP}_{\mathbb{R}}$ defining the cardinality of the primary part. However, as in finite model theory, fixed-point logic captures polynomial-time on such structures where we have a ranking (or ordering) available so that the fixed point construction can simulate the cycling of an algorithm through all elements.

Let $\varphi(t_1, \ldots, t_r)$ be any formula. We write $\chi[\varphi(t_1, \ldots, t_r)]$ for the characteristic function of φ, with the understanding that $\chi[F = G]$ and $\chi[F < G]$ are undefined, if at least one of the terms F, G is undefined.

Lemma 5.3 *The characteristic function of every* $\mathrm{FO}_{\mathbb{R}}$-*formula is* $\mathrm{FFP}_{\mathbb{R}}$-*definable.*

Proof. This is a simple induction. The only point worth mentioning is that the characteristic functions of equalities $F = G$ or inequalities $F < G$ of two number terms can be defined by

$$\begin{aligned} \chi[F = G] &= 1 - [\mathrm{sgn}(F - G)]^2 \\ \chi[F < G] &= ([\mathrm{sgn}(G - F)]^2 + \mathrm{sgn}(G - F))/2. \end{aligned}$$

■

Note that given a ranking E, the induced m-ranking E_m is definable; we will use the abbreviation $\underline{t}$ for $E_m(\bar{t})$. Also we will use $0, 1, \ldots,$ for the tuples—which are of course definable—which are mapped to $0, 1, \ldots,$ by E_m. Thus, strictly speaking, we use a term $F(i)$ (where $i \in \mathbb{N}$) as an abbreviation for $\max_{\bar{t}} \chi[E_m(\bar{t}) = i]F(\bar{t})$.

Theorem 5.4 *On ranked* $\mathbb{R}$-*structures,* $\mathrm{FFP}_{\mathbb{R}} = \mathrm{P}_{\mathbb{R}}$.

Proof. Only the inclusion $\mathrm{P}_{\mathbb{R}} \subseteq \mathrm{FFP}_{\mathbb{R}}$ remains to be shown. We represent a computation of a polynomial-time BSS-machine M by a function $Z : A^{2m} \to \mathbb{R}$ in precisely the same way as in the proof of Theorem 4.2, and prove that this function is inductively definable in the form

$$\mathbf{fp}[Z(\bar{j}, \bar{t}) \leftarrow F(Z, \bar{j}, \bar{t})].$$

We use the fact that there is a $\mathrm{FFP}_{\mathbb{R}}$-term defining the characteristic function of every first-order predicate. The term $F(Z, \bar{j}, \bar{t})$ describes the updates for Z at every step of the computation. It has the form

$$\begin{aligned} F(Z, \bar{j}, \bar{t}) := \chi[\underline{t} = 0]F_{\text{input}}(\bar{j}) + \\ + \max_{\bar{s}} \chi[\underline{t} = \underline{s} + 1] \sum_{k=0}^{N} \chi[Z(0, \bar{s}) = k]F_k(Z, \bar{j}, \bar{s}) \end{aligned}$$

where F_{input} and F_k are terms describing the encoding of the input and the updates made by instruction k.

The first-order definability of input encodings (Lemma 4.1) yields that F_{input} is definable in $\mathrm{FFP}_{\mathbb{R}}$.

As an example for a term F_k we consider a computation instruction $k : x_0 \leftarrow g(x_0, \ldots, x_\ell)$, that increases the index of the read- and write-registers by 1. The associated term $F_k(Z, \bar{j}, \bar{s})$ is

$$\begin{aligned} \chi[\underline{j} = 0](k + 1) + \chi[\underline{j} = 1 \vee \underline{j} = 2](Z(\bar{j}, \bar{s}) + 1) + \\ + \chi[\underline{j} = 3]g(Z(3, s), \ldots, Z(\ell + 3, \bar{s})) + \\ + \chi[\underline{j} > 3]Z(\bar{j}, \bar{s})). \end{aligned}$$

Similarly, for a copy instruction $k : x_w \leftarrow x_r$ we have the following term $F_k(Z, \bar{j}, \bar{s})$:

$$\begin{aligned} \chi[\underline{j} = 0](k + 1) + \chi[\underline{j} \neq 0 \wedge \underline{j} \neq Z(2, \bar{s}) + 3]Z(\bar{j}, \bar{s}) + \\ + \chi[\underline{j} = Z(2, \bar{s}) + 3] \max_{\bar{j}'} \chi[\underline{j'} = Z(1, \bar{s}) + 3]Z(\bar{j}', \bar{s}). \end{aligned}$$

■

6 Primitive recursive and recursive functions on $\mathcal{R}$-structures

As mentioned in the introduction, it was proved by Gurevich that the calculus of primitive recursive functions defines, when interpreted over finite successor structures, precisely the global functions computable in logspace. However, there are important differences between Boolean and real complexity theory with respect to space-resources: it is a result of Michaux [22] that every BSS-decidable problem over $\mathbb{R}^\infty$ can actually be solved in constant space. Thus it is not obvious what type of functions will play the part of logspace computable ones. A closer analysis reveals that there seems to be an enourmous time trade off in applying Michaux' reduction to get constant space computations. It is not known whether the same can be done loosing only a polynomial amount of time. We show that this question is closely related to the relationship between the recursive and the primitive recursive global functions.

We extend the calculi of primitive recursive and recursive functions in a natural way to global functions on $\mathbb{R}$-structures and prove the main result of this section: the primitive recursive global functions are exactly those being computable in polynomial time and constant space whereas the recursive functions are those computable in polynomial time.

Definition 6.1 A *global function* F of vocabulary Υ with arity (ℓ, s) is a function that assigns to each $\mathbb{R}$-structure $\mathfrak{D} = (\mathfrak{A}, \mathfrak{N}, W)$ a function $F^{\mathfrak{D}} : A^{\ell} \times \mathbb{R}^s \to \mathbb{R}$. For an argument $(\bar{a}; \bar{x})$ of $F^{\mathfrak{D}}$ we call $\bar{a}$ the *index part* and $\bar{x}$ the *number part* of that argument.

Definition 6.2 A global function F is *computable in time* $t(n)$ if there exists a BSS-machine M which, given $\mathfrak{D}$ and $(\bar{a}, \bar{x})$, computes $F^{\mathfrak{D}}(\bar{a}, \bar{x})$ in at most $t(|\mathfrak{D}|)$ steps.

In the following we consider only ranked $\mathbb{R}$-structures.

Definition 6.3 The *initial functions* (of vocabulary Υ) are

(i) the embedding function $E : A \to \mathbb{R}$;

(ii) the functions of vocabulary Υ and the characteristic functions of relations in Υ.

(iii) the constants 0 and *last*, considered as $(0,0)$-ary global functions into $\mathbb{R}$, whose values on $\mathfrak{D}$ are, respectively, 0 and $|A| - 1$.

(iv) for every $c \in \mathbb{R}$, the constant function c.

(v) the sign function and the basic arithmetic operations $+, -, \cdot, /$

(vi) the projections.

The class of *primitive recursive global functions* on $\mathbb{R}$-structures is the closure of the initial functions under composition and (simultaneous) primitive recursion:

If $G_i, \ldots, G_r$ and $H_1, \ldots, H_r$ are primitive recursive, then so are the functions $F_1, \ldots, F_r$ defined by

$$\begin{aligned} F_i(0, \bar{a}; \bar{x}) &= H_i(\bar{a}; \bar{x}) \\ F_i(\bar{t}+1, \bar{a}; \bar{x}) &= G(\bar{t}, \bar{a}; F_1(\bar{t}, a; x), \ldots, F_r(\bar{t}, \bar{a}; \bar{x})) \end{aligned}$$

(where $\bar{t}+1$ is the successor of $\bar{t}$ with respect to the lexicographic ordering on tuples over A). A predicate is primitive recursive iff its characteristic function is.

Lemma 6.4 *Every number term in* $\mathrm{FO}_{\mathbb{R}}$ *and the characteristic function of every first-order property is primitive recursive. Furthermore, if the functions* $G_1, \ldots, G_k$ *and the predicates* $\varphi_1, \ldots, \varphi_k$ *are primitive recursive then so is the function* $F = \sum_{i=1}^{k} \chi[\varphi_i] G_i$.

In order to speak about BSS-machines working in constant space we have to modify the machines (since at least n registers are needed to represent a structure $\mathfrak{D}$ with $|\mathfrak{D}| = n$).

Definition 6.5 A *BSS-machine with separated input and output device*, shortly a SIO-BSS-machine, is a BSS-machine M having besides its working registers two more blocks of registers, for the input and the output. In addition to the usual operations on the working registers M can read values from input registers or write into output registers (with unit cost). A SIO-BSS machine M works in space $t(n)$ if the number of working registers used on inputs of size n does not exceed $t(n)$.

Theorem 6.6 *A global function is computable by a SIO-BSS machine in polynomial time and constant space iff it is primitive recursive.*

Proof. A simple induction shows that every primitive recursive global function is computable in polynomial-time with constant space by a SIO-BSS machine.

Conversely, assume that F is a global function computed by an SIO-BSS machine M with k working registers in time n^m. Similarly to the proof of Theorem 4.2 we describe the behaviour of M by a collection $\bar{Z} = Z_0, \ldots, Z_{k+2}$ and X, Y of global functions. Here, for $i = 0, \ldots, k-1$, the value $Z_i^{\mathfrak{D}}(\bar{t}, \bar{a}; \bar{x})$ is the content of working register i at time $\bar{t}$ during the computation of M while calculating $F^{\mathfrak{D}}(\bar{a}; \bar{x})$. The remaining three functions Z_k, Z_{k+1} and Z_{k+2} encode the instruction and the indices of the read and write registers, whereas X, Y encodes the content of the input and output registers. Obviously the values $Z_i(\bar{t}+1, \bar{a}; \bar{x})$ depend in a simple way from the values $\bar{Z}(\bar{t}, \bar{a}; \bar{x})$ and from the content of the input registers.

Using Lemma 6.4 and the fact that the encoding of the input is first-order definable, it is not diffcult (although a bit lengthy) to write down a primitive recursive function describing this update. Finally, it is obvious that content of the output registers, and thus the function F too, can be calculated from $\bar{Z}$ by primitive recursion and projection. ∎

Since the primitive recursive global functions on finite successor structures are logspace computable, they are in NC^2. Over the reals the situation is different. As shown in [3], $\mathrm{NC}_{\mathbb{R}} \subsetneq \mathrm{P}_{\mathbb{R}}$, where $\mathrm{NC}_{\mathbb{R}}$ consists of all problems decidable by a polynomial number of BSS-machines working in parallel in time $log^k(n)$ (we refer to [3] for the exact definition). Exploiting Cucker's argument, we get the following result.

Theorem 6.7 *There exists a primitive recursive global function which is not computable in polylogarithmic parallel time by a polynomial number of BSS machines.*

In the literature, there are a number of different calculi of partial recursive functions that give, when they are interpreted over ordered finite structures, precisely the polynomial-time computable global functions.

Gurevich presented several such algebras for PTIME in [13], and we refer to [23, 14, 11] for other similar algebras that achieve the same goal.

Many of these algebras can be extended to algebras of global functions on ordered $\mathbb{R}$-structures that characerize polynomial-time computability in the sense of Blum, Shub and Smale. Due to space limitations we just sketch one example.

Following Gurevich we introduce the concept of global recursive functions on ordered $\mathcal{R}$-structures by adapting the classical Herbrand–Gödel–Kleene equation language, cf. [13]. Let Υ be a vocabulary and consider a set E of finitely many equations $t_1 = s_1, \ldots, t_k = s_k$, Here, t_i are terms $F_j(\bar{h}; \bar{r})$ where $F_1, \ldots, F_q$ are function symbols not contained in Υ and $\bar{h}$ and $\bar{r}$ are tuples of, respectively, index terms and number terms. The s_i are number terms over vocabulary $\Upsilon \cup \{F_1, \ldots, F_q\}$. For instance, one can reformulate the schema for primitive recursion as such a system.

Definition 6.8 Let $\mathfrak{D}$ be an ordered $\mathbb{R}$-structure of vocabulary Υ. A system E as above *defines a function $F_i : A^\ell \times \mathbb{R}^s \rightarrow \mathbb{R}$ recursively in $\mathfrak{D}$* iff for all $(\bar{a}; \bar{x}) \in A^\ell \times \mathbb{R}^s$ there exists at most one $w \in \mathbb{R}$ such that $F_i(\bar{a}; \bar{x}) = w$ can be derived from the identities of the form $g(\bar{b}; \bar{y}) = v$ holding in $\mathfrak{D}$, where g is initial primitive recursive, by finite applications of the following steps:

(i) substituting elements from A for individual variables j and closed number terms for real variables x_i.

(ii) if t is a closed term, $u \in \mathbb{R}$ and $t = u$ has already been proved, then occurences of t can be replaced by u.

E recursively defines a global function F if it recursively defines $F^{\mathfrak{D}}$ for every $\mathfrak{D}$.

Remark. Note that we don't require the existence of a total function F such that E is satisfied for all values. Thus, checking values of functions defined by E at points $(\bar{a}; \bar{x})$ does not mean to decide the existential first order theory of the reals.

Theorem 6.9 *Let F be a global function of vocabulary Υ. Then F is recursively defined by a system E iff it is computable in polynomial time by a BSS-machine.*

In the full paper, we will also discuss other algebraic characterizations of polynomial-time over $\mathbb{R}$.

7 First-order reductions

It is known, that there exist problems which are NP-complete under first-order reductions or even quantifier-free reductions [7, 9]. On ordered structures, the even weaker so-called projection reductions suffice [16, 17].

We introduce here the notion of a $\text{FO}_\mathbb{R}$-reduction among (classes of) $\mathbb{R}$-structures, and show that both $\text{NP}_\mathbb{R}$ and $\text{P}_\mathbb{R}$ contain complete problems under these reductions. To do this we find it convenient to generalize the notion of a number term in $\text{FO}_\mathbb{R}$ in the following way: Let $T(\text{FO})$ be the set of expressions $t_1\chi[\varphi_1] + \cdots + t_k\chi[\varphi_k]$ where t_i are number terms of $\text{FO}_\mathbb{R}$ and $\chi[\varphi_i]$ are the characteristic functions of $\text{FO}_\mathbb{R}$-formulae φ_i.

Definition 7.1 Let Υ, Υ' be two vocabularies for $\mathbb{R}$-structures with $\Upsilon = (\Upsilon_a, \Upsilon_w)$. We assume for simplicity that Υ_a is relational. Let $k \in \mathbb{N}$ be a constant. A *first-order interpretation* (of width k) from $\mathbb{R}$-structures of vocabulary Υ' to $\mathbb{R}$-structures of vocabuary Υ is given by a collection Φ of first-order formulae and terms:

- for every m-ary relation $R \in \Upsilon_a$, Φ contains a formula φ_R of signature Υ', with free variables t_{ij} where $i = 1, \ldots, m$, $j = 1, \ldots, k$.
- for every function $X \in \Upsilon_w$ of arity m, there is a number term $F_X \in T(\text{FO})$ of signature Υ' in Φ, depending on km variables t_{ij}.

Such an interpetation Φ maps a structure $\mathfrak{D}$ of signature Υ' to a structure $\Phi\mathfrak{D}$ of signature Υ in the obvious way.

Definition 7.2 Let K and K' be sets of $\mathbb{R}$-structures of signatures Υ, Υ', respectively. We say that K' is $\text{FO}_\mathbb{R}$-*reducible* to K iff there exists a first-order interpretation Φ such that for every $\mathbb{R}$-structure $\mathfrak{D}$

$$\mathfrak{D} \in K' \text{ iff } \Phi\mathfrak{D} \in K.$$

In [1] it is shown that the problem of deciding the existence of a real zero for a degree four polynomial is $\text{NP}_\mathbb{R}$-complete. It follows that the problem AC whether a given algebraic circuit evaluates at least one input to 1 is $\text{NP}_\mathbb{R}$-complete, too. (For the definition of an algebraic circuit cf. [26]). We can show that the circuit-problem is $\text{NP}_\mathbb{R}$-complete even under $\text{FO}_\mathbb{R}$-reductions. The proof extends a similar result for the discrete setting, which was established by Gács and Lovász [9].

Theorem 7.3 *The algebraic-circuit problem is complete for class $NP_\mathbb{R}$ under $\text{FO}_\mathbb{R}$-reductions.*

Remark. First-order reductions can be computed in *weak polynomial time* in the sense of Koiran (cf. [19, 5]). Thus, Theorem 7.3 generalizes the result of Cucker, Shub and Smale [5] that $\text{NP}_\mathbb{R}$ contains complete problems with respect to weak polynomial reductions.

It is easy to see that first-order reductions can be computed by algebraic circuits of polynomial size and constant depth (if the gates allow an unbounded fan-in; for bounded fan-in one gets polylogarithmic depth). Cucker and Torecillas [6] proved that the problem of deciding whether a given algebraic circuit evaluates a given real input to a given value is $\mathrm{P}_{\mathbb{R}}$-complete under $\mathrm{NC}_{\mathbb{R}}$-reductions. In fact the $\mathrm{NC}_{\mathbb{R}}$-reductions given there can be refined to first-order reductions, establishing the following result.

Theorem 7.4 *The algebraic circuit evaluation problem is* $\mathrm{P}_{\mathbb{R}}$*-complete under* $\mathrm{FO}_{\mathbb{R}}$*-reductions.*

References

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

[2] P. Bürgisser, M. Clausen, A. Shokrollahi, *Algebraic Complexity Theory*, forthcoming.

[3] F. Cucker, $\mathrm{P}_{\mathbb{R}} \neq \mathrm{NC}_{\mathbb{R}}$, Journal of Complexity **8** (1992), 230–238.

[4] F. Cucker, D. Grigoriev, *On the Power of real Turing Machines over Binary Inputs*, NeuroCOLT Technical Report NC-TR-94-7, 1994, ESPRIT Working Group 8556.

[5] F. Cucker, M. Shub, S. Smale, *Separation of Complexity Classes in Koiran's weak model*, Theoretical Computer Science **133** (1994), 3–14.

[6] F. Cucker, A. Torrecillas, *Two P-complete Problems in the Theory of the Reals*, Journal of Complexity **8** (1992), 454–466.

[7] E. Dahlhaus, *Reductions to NP-Complete Problems by Interpretations*, in: E. Börger et al. (Eds.), Logic and Machines: Decision Problems and Complexity, Lecture Notes in Computer Science Nr. 171, Springer (1983), 357–366.

[8] R. Fagin, *Generalized first-order spectra and polynomial-time recognizable sets*, SIAM-AMS Proc. **7** (1974), 43–73.

[9] P. Gács, L. Lovász, *Some Remarks on generalized Spectra*, Zeitschrift für mathematische Logik und Grundlagen der Mathematik **23** (1977), 547–554.

[10] E. Grädel, *Capturing Complexity Classes by Fragments of Second Order Logic*, Theoretical Computer Science **101** (1992), 35–57.

[11] E. Grädel, Y. Gurevich, *Tailoring recursion for complexity*, Proceedings of 21st Colloquium on Automata, Languages and Programming, ICALP 94, Lecture Notes in Computer Science Nr. 820, Springer (1994), 118–129.

[12] E. Grädel, Y. Gurevich, *Metafinite Model Theory*, in preparation. [Preliminary versions have been presented at the Logic Colloquium 94 in Clermont-Ferrand in July 1994 (by E. Grädel), and at the Conference on Logic and Complexity, Indianapolis, in October 1994 (by Y. Gurevich).]

[13] Y. Gurevich, *Algebras of feasible functions*, Proc. of 24th IEEE Symposium on Foundations of Computer Science (1983), 210–214.

[14] Y. Gurevich, *Logic and the Challenge of Computer Science*, in: E. Börger (Ed.), Trends in Theoretical Computer Science, Computer Science Press (1988), 1–57.

[15] N. Immerman, *Relational queries computable in polynomial time*, Information & Control 68 (1986), 86-104.

[16] N. Immerman, *Languages that Capture Complexity Classes*, SIAM J. Comput. **16** (1987), 760–778.

[17] N. Immerman, *Expressibility as a Complexity Measure, Results and Directions*, Proc. of 2nd IEEE Conference on Structure in Complexity Theory (1987), 194–202.

[18] N. Immerman, *Descriptive and Computational Complexity*, in: J. Hartmanis (Ed.), Computational Complexity Theory, Proc. of AMS Symposia in Appl. Math. **38** (1989), 75–91.

[19] P. Koiran, *A weak version of the Blum-Shub-Smale model*, Proc. 34th IEEE Symposium on Foundations of Computer Science (1993), 486–495.

[20] T. Lickteig, *On semialgebraic decision complexity*, ICSI Tech.Rep. TR-90-052 and Habilitationsschrift, Universität Tübingen (1990).

[21] K. Meer, *On the Complexity of Quadratic Programming in Real Number Models of Computation*, Theoretical Computer Science **133** (1994), 85–94.

[22] C. Michaux, *Une remarque à propos des machines sur* $\mathbb{R}$ *introduites par Blum, Shub et Smale*, C.R.Acad.Sc. Paris, t 309, série I (1989), 435-437.

[23] V. Sazonov, *Polynomial computability and recursivity in finite domains*, Elektronische Datenverarbeitung und Kybernetik **16** (1980), 319–323.

[24] V. Strassen, *Algebraic Complexity Theory*, in: J. van Leeuwen (Ed.), Handbook of Theoretical Computer Science, vol. A, Elsevier, Amsterdam 1990, pp. 633–672.

[25] M. Vardi, *Complexity of relational query languages*, Proceedings of 14th ACM Symposium on Theory of Computing (1982), 137-146.

[26] J. von zur Gathen, *Algebraic Complexity Theory*, Ann. Reviews of Computer Science **3** (1988), 317-347.