Saturation and Stability in the Theory of Computation over the Reals

Olivier CHAPUIS
Institut Girard Desargues – CNRS, Bâtiment des Mathématiques
Université Lyon I, 43 boulvard du 11 Novembre 1918
F-69622 Villeurbanne Cedex. chapuis@desargues.univ-lyon1.fr

Pascal KOIRAN
Laboratoire de l'Informatique du Parallélisme – CNRS
Ecole Normale Supérieure de Lyon, 46 allée d'Italie
F-69364 Lyon Cedex 07. koiran@lip.ens-lyon.fr

June 10, 1997

Abstract

This paper was motivated by the following two questions which arise in the theory of complexity for computation over ordered rings in the now famous computational model introduced by Blum, Shub and Smale:
(i) is the answer to the question P =? NP the same in every real-closed field ?
(ii) if P $\neq$ NP for $\mathbb{R}$, does there exist a problem of $\mathbb{R}$ which is NP but not NP-complete ?
Some unclassical complexity classes arise naturally in the study of these questions. They are still open, but we could obtain unconditional results of independent interest.
Michaux introduced /const complexity classes in an effort to attack question (i). We show that $\mathrm{A}_{\mathbb{R}}/\mathrm{const} = \mathrm{A}_{\mathbb{R}}$, answering a question of his. Here A is the class of real problems which are algorithmic in bounded time. We also prove the stronger result: $\mathrm{PAR}_{\mathbb{R}}/\mathrm{const} = \mathrm{PAR}_{\mathbb{R}}$, where PAR stands for parallel polynomial time. In our terminology, we say that $\mathbb{R}$ is A-saturated and PAR-saturated. We also prove, at the nonuniform level, the above results for every real-closed field. It is not known whether $\mathbb{R}$ is P-saturated. In the case of the reals with addition and order we obtain P-saturation (and a positive answer to question (ii)). More generally, we show that an ordered $\mathbb{Q}$-vector space is P-saturated at the nonuniform level (this almost implies a positive answer to the analogue of question (i)).
We also study a stronger notion that we call P-stability. Blum, Cucker, Shub and Smale have (essentially) shown that fields of characteristic 0 are P-stable. We show that the reals with addition and order are P-stable, but real-closed fields are not.
Questions (i) and (ii) and the /const complexity classes have some model theoretic flavor. This leads to the theory of complexity over "arbitrary" structures as introduced by Poizat. We give a summary of this theory with a special emphasis on the connections with model theory and we study /const complexity classes with this point of view. Note also that our proof of the PAR-saturation of $\mathbb{R}$ shows that an o-minimal structure which admits quantifier elimination is A-saturated at the nonuniform level.

Contents

1 Introduction

This paper was motivated by the following two questions which arise in the theory of complexity for computation over ordered rings in the now famous computational model introduced by Blum, Shub and Smale [6]:
(i) is the answer to the question P =? NP the same in every real-closed field ?
(ii) if P $\neq$ NP for $\mathbb{R}$, does there exist a problem of $\mathbb{R}$ which is NP but not NP-complete ? (In the standard model of computation the positive answer to this question is known as Ladner's theorem [22].)
Some unclassical complexity classes arise naturally in the study of these questions. They are still open, but we could obtain unconditional results of independent interest. These questions have a model-theoretic flavor. This lead us to work with arbitrary first-order structures in a finite language. The theory of computation and complexity over such structures was developed by Poizat in [14] and [30] as a generalization of the Blum, Shub and Smale model of computation. However, the main results of this paper concern computations over real-closed fields. On the other hand, the model-theoretic setting has some advantages, at least for a better understanding of the results.
Let M be a first-order structure in a finite language (one may think of M as a real-closed field in the language of ordered rings). One of the difficulties of the theory of computation over an infinite structure is that an algorithm over M can use (a finite number of) elements of M, the parameters (or constants) of the algorithm. For example, with the reals, we can encode in the digit of a real number any sequence of 0 and 1 and an algorithm can retrieve these digits. This gives to the reals an algorithmic power that the real-closed field of the real algebraic numbers does not have. Let $M \leq N$ be an elementary extension (or an extension of real-closed fields), then, as the above example shows, there is no reason for M to have the same algorithmic power as N. Conversely, Michaux [26] has noted that if P = NP in M, then P = NP in N. Thus, question (i) above become: (i') does P = NP in N imply P = NP in M ? This question lead Michaux [26] to introduce the complexity class P/const. If M satisfies P/const = P, then for every elementary extension N of M question (i') has a positive answer. The point is that one can sometimes give a "yes-or-no" answer to the question P =? P/const.
Another difficulty is that if M is uncountable we have uncountably many algorithms over M. This can be an obstruction for diagonalization arguments. For example, the uncountability of $\mathbb{R}$ is an obstruction for extending the usual proof of Ladner's theorem to the reals (however, the proof of Ladner's theorem works for the real algebraic numbers). Again, this difficult disappears if M satisfies P/const = P (and has a decidable first-order theory): Ben-David, Meer and Michaux [3] and independently Poizat [31] have shown that under these assumptions, question (ii) has a positive answer for M.
Let us define the complexity classes $\mathcal{C}$/const. If $k \in \mathbb{N}$, and if $\mathcal{C}$ is a class of problems of M, one can define a new class $\mathcal{C}/k$ as follows. A problem $X \subseteq M^{\infty}$ is in $\mathcal{C}/k$ if

there exists $Y \in \mathcal{C}$ (the "corresponding problem"), such that for every $n \geq 0$ there exists $\alpha_n \in M^k$ satisfying

$$\forall x \in M^{\leq n}\ [x \in X \Leftrightarrow \langle x, \alpha_n \rangle \in Y]. \tag{1}$$

Note that the advice α_n must work for all inputs of length *at most* n. Let $\mathcal{C}/\mathrm{const} = \bigcup_{k=0}^{\infty} \mathcal{C}/k$ be the union of these classes. If $l \in \mathbb{N}$ and $\mathcal{C}$ is a classical complexity class, we denote by $\mathcal{C}^l$ the class of problems which are $\mathcal{C}$ with an "algorithm" using l parameters from M. For any M, the inclusions $\mathcal{C}^k \subseteq \mathcal{C}^0/k$ and $\mathcal{C} \subseteq \mathcal{C}/\mathrm{const}$ clearly hold. If $\mathcal{C} = \mathcal{C}/\mathrm{const}$, we say that M is $\mathcal{C}$-saturated.

The main theme of this paper is the study, for real-closed fields and ordered $\mathbb{Q}$-vector spaces, of classes $\mathcal{C}/\mathrm{const}$ where $\mathcal{C}$ is a classical complexity class. We also study from a general point of view classes of the form $\mathcal{C}/\mathrm{const}$ and give counterexamples.

Let us now describe the contents and main results of this paper.

Section 2 is of a preliminary nature. We recall some elementary facts from model theory (such as the notion of saturation and o-minimal structure). We give a summary of the theory of complexity for computation over arbitrary structures. One of the tasks of this summary is to show to a model theorist that computation over a first-order structure is not an alien thing for her or him. Conversely, a number of model theoretic notions and results can be useful. These preliminaries contain a new result: a generalization of Karp-Lipton's theorem. This result allows us to prove (in Section 3) that if $M \leq N$ is an elementary extension and if $\mathrm{P} = \mathrm{NP}$ or $\mathbb{P} = \mathbb{NP}$ in N then the (uniform) polynomial hierarchy over M collapse at the third level.

We need to introduce some notations. As usual we denote by PAR the class of problems solved in parallel polynomial time. In this paper we need to work at the nonuniform level. Following Poizat, we denote by $\mathbb{P}_M$ (respectively, $\mathbb{PAR}_M$) the class of problem of M solved by a sequence of circuits (in the sense of M), using parameters from *a finite* subset of M, of polynomial size (respectively, of polynomial depth). The above classes can be also defined using *boolean* advice functions. For parallel time we need a semi-nonuniform class: $\mathbb{P}\mathrm{AR}_M$ is the class of problems solved in parallel polynomial time with the help of a boolean advice function f from $\mathbb{N}$ into $\{0,1\}^{\infty}$ such that the size of $f(n)$ is polynomial in n. We denote by A_M the class of problems of M solved in *bounded* time. The nonuniform counterpart of A_M is denoted by $\mathbb{A}_M$. This is the class of problems of M solved in bounded time with the help of a boolean advice function. Note that if a real-closed field or an ordered $\mathbb{Q}$-vector spaces contains the reals, then $\mathbb{P} = \mathrm{P}$, $\mathbb{P}\mathrm{AR} = \mathrm{PAR}$ and $\mathbb{A} = \mathrm{A}$ (but $\mathbb{P}\mathrm{AR} \subsetneq \mathbb{PAR}$) .

In Section 3, continuing the work of Michaux, we develop the abstract theory for the classes $\mathcal{C}/\mathrm{const}$. The main ingredient from model theory is saturation (for every reasonable $\mathcal{C}$, $\mathcal{C} = \mathcal{C}/\mathrm{const}$ for an $\aleph_1$-saturated structure). In that section, we are also concerned with counterexamples. We remark that for a number of countable structures (and in particular for countable real-closed fields and countable ordered

$\mathbb{Q}$-vector spaces) there are problems in $P^0/1$ not in A. This implies that we need to work at the nonuniform level. We also construct a structure (with elimination of quantifiers) such that P/const is not included in $\mathbb{A}$ and another one with $\mathbb{A}$/const $= \mathbb{A}$ but where P/const is not included in $\mathbb{P}$.
Section 4 is central and concerns real-closed fields. After recalling some background in the first subsection, we show in subsection 2 that algebraic parameters can be eliminated. In other words, when working with a real-closed field we may assume (without loss of time) that the parameters of the algorithms are algebraically independent. This has some important consequences for the study of /const algorithms. In the third subsection, we prove that $P^0/1 = P^1$ for $\mathbb{R}$. We do not know whether $P^1_{\mathbb{R}}/1 \subseteq P_{\mathbb{R}}$, but $P_{\mathbb{R}}/1$ is contained in Σ_2 over $\mathbb{R}$. We also exhibit a family of problems in $P^1_{\mathbb{R}}/1$ that contains a part of the difficulty of the question $P^1_{\mathbb{R}}/1 \subseteq ?\ P_{\mathbb{R}}$. We conclude this subsection with proofs that A/const = A for the reals. Subsection 4 gives a characterization (in terms of sequences of quantifier-free formulae) of parallel algorithm over real-closed fields. The proof depends on the algorithmic version of the theorem of Milnor-Petrovskii-Olienik-Thom on the number of consistent sign vectors for a family of polynomials as it can be found in [33]. In Subsection 5 we prove that $\mathbb{P}\mathbb{A}\mathbb{R}$/const $= \mathbb{P}\mathbb{A}\mathbb{R}$ and that $\mathbb{P}$AR/const $= \mathbb{P}$AR for every real-closed field (we need to work at the nonuniform level and for $\mathbb{R}$ the second equality implies that PAR/const = PAR). We also give some applications of these results.
We do not know whether $P^0/1 \subseteq \mathbb{P}$ for the real algebraic numbers. We exhibit a family of problems in $P^0/1$ which seems to show that this question is "impossible" (at least before a solution of the question $\mathbb{P} =?\ \mathbb{P}$AR). In the last subsection we use a construction of van den Dries [36] to show that $\mathbb{R}$ has a real-closed extension R with problems Y in P^2 with a restriction to $\mathbb{R}$ not in A, or even with a restriction in A but not in P. In our terminology, $\mathbb{R}$ is not P-stable.
Computation over the reals without multiplication has been also considered. In this setting ordered $\mathbb{Q}$-vector spaces are the structures to consider. We denote by $\mathbb{R}_{ovs}$ the reals without multiplication (i.e, $\mathbb{R}$ in the language of ordered abelian groups). In the last section of this paper we show (using the same kind of arguments as for real-closed fields) that $\mathbb{P}$/const $= \mathbb{P}$ for such structures. It follows that P/const = P for $\mathbb{R}_{ovs}$, that question (ii) has a positive answer for $\mathbb{R}_{ovs}$ and that the question $\mathbb{P} =?\ \mathbb{NP}$ has the same answer in every (nontrivial) ordered $\mathbb{Q}$-vector spaces. Moreover, we show that $\mathbb{R}_{ovs}$ is P-stable: given an extension $\mathbb{R}_{ovs} \leq E$ and a problem Y of E in P, the restriction of Y to $\mathbb{R}_{ovs}$ is P.
One of the main ingredient of the proof that $P^0/1 = P^1$ for $\mathbb{R}$ and that $\mathbb{P}$AR/const $= \mathbb{P}$AR for a real-closed field is the fast algorithm of quantifier elimination of Renegar [33] or Heintz, Roy and Solernó [15] (for the case of ordered $\mathbb{Q}$-vector spaces we use a elimination theorem of Sontag [34]). Another important fact (for $\mathbb{P}$AR/const $= \mathbb{P}$AR) is a result of Pillay [27] on definable equivalence relations in o-minimal structures which applies to real-closed fields and ordered $\mathbb{Q}$-vector spaces (since these structures are o-minimal). In fact, our proof of the equality $\mathbb{P}$AR/const $= \mathbb{P}$AR for

real-closed fields shows that if M is an o-minimal structure which admits elimination of quantifiers, then $\mathbb{A}_M/\mathrm{const} = \mathbb{A}_M$. Moreover, the results of non P-stability of $\mathbb{R}$ and of P-stability of $\mathbb{R}_{ovs}$ are connected with results of van den Dries [35] and of Marker and Steinhorn [25] on definability of types in o-minimal structures (see Section 3.4).

Note that for algebraically closed fields of characteristic 0, questions (i) and (ii) have received positive answers (with $\mathbb{C}$ in place of $\mathbb{R}$ in question (ii)). Blum, Cucker, Shub and Smale proved in [4] that if $K \leq L$ is an extension of fields of characteristic 0 (with K contained in the algebraic closure of $\mathbb{Q}$; but this not essential) and if Y is a problem of L in P_L the restriction of Y is P_K. It follows that $\mathrm{P}/\mathrm{const} = \mathrm{P}$ in K and (independently) that question (i) has a positive answer for algebraically closed fields of characteristic 0. The second author proved in [21] similar results in the case of positive characteristic for $\mathbb{P}$. Note that the above transfer cannot hold in the case of ordered fields (see Section 4.6). In fact, such a result is possible only in the presence of an ω-stable theory or for specific models, such as a Dedekind complete model of an o-minimal theory (see Section 3.4). For question (ii) in the case of $\mathbb{C}$, the first proof of a positive answer is given in [24] by Malajovich and Meer. Using the ω-saturation of $\mathbb{C}$, Ben-David, Meer and Michaux [3] and independently Poizat [31] give a more elementary proof.

2 Preliminaries

2.1 A Word on Model Theory

We assume some familiarity with first-order logic. However, we recall a few definitions and facts. For more details and any unexplained notions we refer the reader to [16] or [29].

In this paper M denotes a first-order structure in a language $\mathcal{L}$ (we always assume that equality is in $\mathcal{L}$). A subset X of M^n is said to be definable if there is some formula $\phi(x_1, \ldots, x_n)$ (of $\mathcal{L}$) *with parameters in* M such that X is the set of elements $a \in M^n$ such that $M \models \phi(a)$. If A is a subset of M we say that X is A-definable if X is definable with a formula with parameters in A only.

Let $M \leq N$ be an extension of $\mathcal{L}$-structures. Such an extension is said to be elementary if every sentence of $\mathcal{L}$ with parameters in M which is true in N is also true in M (this implies that M and N have the same first-order theory). Note that if a first-order theory T admits elimination of quantifiers, then every extension between models of T is elementary.

Let λ be an infinite cardinal. M is said to be λ-saturated if for every subset A of M of cardinal $< \lambda$ and every positive integer n the following holds : every set of formulae with parameters in A and with free variables $x_1, \ldots, x_n$ which is finitely satisfiable in M is satisfiable in M. For example, $\mathbb{R}$ (in the language of ordered ring) is not $\aleph_0$-saturated because the set of (parameter-free) formulae $\{x > n | n \geq 0\}$ is finitely satisfiable in $\mathbb{R}$ but $\mathbb{R}$ is archimedean. On the other hand, it is an easy

exercise (assuming elimination of quantifiers) to show that $\mathbb{C}$ (in the language of ring) is $\aleph_1$-saturated.
The point is that we can found "everywhere" λ-saturated structures. More precisely, if M is a $\mathcal{L}$-structure and λ an infinite cardinal then M has a λ-saturated elementary extension. Moreover, a λ-saturated structure N is λ^+-universal. This means that if M is another $\mathcal{L}$-structure of cardinal $\leq \lambda$ with the same first-order theory as N, then there exists an elementary embedding of M into N (i.e., an injective morphism in the sense of $\mathcal{L}$ of M into N such that the image of M is an elementary restriction of N).
Some of the results of this paper which concern real-closed fields can be generalized to arbitrary o-minimal structures that admit (effective) elimination of quantifiers. For o-minimal structures we refer the interested reader to [28] and [17]. Let M be a $\mathcal{L}$-structure and assume that $\mathcal{L}$ contains a binary relation $<$ that is interpreted as a linear ordering. M is said to be o-minimal if every definable subset of M is a finite union of intervals in M (a usual we assume that $<$ is dense and without extremity). By elimination of quantifiers, real-closed fields (in the language of ordered rings) and ordered $\mathbb{Q}$-vector spaces (in the language of ordered abelian groups) are o-minimal. Let $M \leq N$ be an elementary extension. If M is o-minimal then so is N (this is not obvious). Assume M to be o-minimal. Let a be an element of N, then a defines a cut of M : $(C_a^-; C_a^+)$ where $C_a^- = \{b \in M | b < a\}$ and $C_a^+ = \{b \in M | b > a\}$. The element a is said to be rational over M if C_a^- (and C_a^+) is a definable subset of M. By o-minimality, if a is rational over M then C_a^- and C_a^+ are intervals. Then, the standard part of a is the right extremity of C_a^- ($-\infty$ if C_a^- is empty). We denote this element of $M \cup \{-\infty, +\infty\}$ by $st(a)$. M is said to be Dedekind complete in N if every $a \in N$ is rational over M. M is Dedekind complete if M is Dedekind complete in every elementary extension of M. It is easy to see that M is Dedekind complete iff every nonempty majored (minored) subset of M as a supremum (infimum) in M.

2.2 Models of Computation

This subsection is a summary of the foundation of the theory of complexity for computation over "arbitrary" structures. Of course some knowledge in standard complexity theory is not useless (a classical reference for this subject is [1]). However, if one is mainly interested in nonuniform complexity classes it is not necessary to know what an algorithm is.
Let M be a structure in a finite first-order language $\mathcal{L}$. For simplicity we assume that $\mathcal{L}$ contains two constant symbols denoted by 0 and 1 which are interpreted by two distinct elements of M (if there are no such constants we add them and if possible we choose these two elements in a canonical way). We denote by M^∞ the set of finite sequences of M. A problem X of M is a subset of M^∞. Let $t(n)$ be a function from $\mathbb{N}$ into $\mathbb{N}^*$. $\mathrm{TIME}_M(t)$ denotes the class of problem X which can be recognized in time $O(t(n))$ by a machine over M (essentially a Turing machine which manipulates elements of M and which can apply the functions of $\mathcal{L}$ and the

characteristic functions of the relations of $\mathcal{L}$). Thus $X \in \mathrm{TIME}_M(t)$ if and only if there is a machine over M which, given a finite sequence $(a_1, \ldots, a_n)$ of M, outputs 1 if $(a_1, \ldots, a_n) \in X$ and 0 if $(a_1, \ldots, a_n) \notin X$ after $O(t(n))$ elementary operations. If $\mathcal{M}$ is a machine over M then $\mathcal{M}$ can use a finite number of elements of M not named by constant symbols of $\mathcal{L}$. These elements are the *parameters* of $\mathcal{M}$ (in particular, 0 and 1 are given for free; they are never considered as parameters). If k is a positive integer, we denote by $\mathrm{TIME}^k_M(t)$ the class of problems recognized by a machine working in time $O(t)$ with at most k parameters in its program. Note that the word *constant* has sometimes been used instead of the word *parameter*. We prefer the latter since for us a constant is an element of M named by a constant symbol of $\mathcal{L}$. As usual, we define P_M (respectively, EXP_M) as the class of problem of M which can be recognized by a machine over M working in polynomial (respectively, exponential) time. The corresponding classes for machines with at most k parameters in their programs are denoted by P^k_M and EXP^k_M (throughout the paper, exponentials and logarithms are to the base 2).

If M is infinite, in general (essential if M is not recursively saturated), there exist problems of M which are recognized by a machine over M but without bound on its running time (e.g., $\{(a) | a \in \mathbb{Z}\}$ in $(\mathbb{R}, +, ., -, 0, 1, <)$). Since we are mainly interested in problems solved in bounded time we denote by A_M the class of problems X of M which are recognized in bounded time (i.e., there exists a function t such that $X \in \mathrm{TIME}_M(t)$). The class A_M can be characterized as follows: $X \in \mathrm{A}_M$ if and only if there exists a sequence of quantifier-free formulae $(\phi_n(x_1, \ldots, x_n, y_1, \ldots, y_k))_{n \geq 0}$ (k is fixed) and an element $\alpha \in M^k$ such that (i) there exists an algorithm (in the standard Turing machine model) which produces the ϕ_n and (ii) $X \cap M^n = \{a \in M^n | M \models \phi_n(a, \alpha)\}$. We also define the class $\mathbb{A}_M$ of problem of M which are recognized by "nonuniform algorithm working in bounded time" as above but without imposing condition (i). $\mathbb{A}_M$ can be also defined as $\mathrm{A}_M/\mathcal{F}$, the class of problem recognized by a machine over M which works in bounded time with the help of a boolean advice function $f \in \mathcal{F} = \{f : \mathbb{N} \longrightarrow \{0,1\}^\infty\}$. It is also useful to introduce the class of problems (quantifier-free) definable over M which is defined as $\mathbb{A}_M$ but the ϕ_n can be arbitrary (quantifier-free) formulae with parameters in M. To define the nonuniform counterpart of P (and EXP) we recall from [14] and [30] the notion of circuit in the sense of M. This will be useful for a number of reasons. First we have to add a selector to M. A selector for M is a function $S : M^3 \longrightarrow M$ such that $S(0, y, z) = y$, $S(1, y, z) = z$ and $S(x, y, z) = t(x, y, z)$ for $x \notin \{0, 1\}$ where t is a term of $\mathcal{L}$. Sometimes a structure M has a selector: this means that there exists a conditioned term $s(x, y, z)$ of $\mathcal{L}$ with the above property (for example, if M is a field one can take $s(x, y, z) = (1 - x)z + xy$). If M does not have a selector (e.g., $(\mathbb{R}, +, -, 0, 1, <)$) we add to the language of M a new function symbol S with the above interpretation (one can take $t(x, y, z) = x$; note that since S is $\emptyset$-definable in M without quantifiers, from the point of view of model theory, M with S is the same thing as M without S). we denote by $\mathcal{L}^*$ the new language. A circuit C (in

the sense of M) is a finite acyclic directed graph (where the vertices are called gates and the edges are called arrows) labeled by variables and symbols of $\mathcal{L}^*$ such that:
(i) Since C is acyclic there are gates without incoming arrows: such a gate is labeled by a constant of $\mathcal{L}$ or by a variable $x_1, x_2, ...$; moreover, gates labeled by variables are called input gates and are ordered (we use the notation $C(x_1, \ldots, x_n)$ to say that the input gates are $x_1, \ldots, x_n$).
(ii) A gate with incoming arrows receives r arrows where r is the arity of a symbol of $\mathcal{L}^*$, and it is labeled by such a symbol; moreover, the incoming arrows are ordered and if the gate is labeled by a relation we say that the gate is a test.
(iii) Gates without outgoing arrows are called output gates and they are ordered.
Note that since C is acyclic, there are output gates. The size of C, $size(C)$ is the number of gates of C. Let $C(x_1, \ldots, x_n)$ be a circuit in the sense of M with m output gates. Then $C(x_1, \ldots, x_n)$ computes in an obvious way a function $f_C : M^n \longrightarrow M^m$ (here we see that we need to order the input and output gates and that we need to order incoming arrows since the operations/relations of M are not necessarily commutative/symmetric). Indeed, to each gate we can inductively associate a function of the input variables in the usual way (a test gate labeled by a relation R return 1 if $M \models R(a_1, \ldots, a_n)$ and 0 if not).
In what follows all our circuits are "decisional". This means that there is only one output gate and that this gate is a test. Thus a circuit computes a function $f_C : M^n \longrightarrow \{0, 1\}$. If $C(x_1, \ldots, x_n)$ is a circuit and $a \in M^n$, we say that $M \models C(a)$ if $f_C(a) = 1$. Circuits are compact forms of quantifier-free formulae. If $\phi(x_1, \ldots, x_n)$ is a quantifier-free formula of $\mathcal{L}$, then there exists a circuit $C(x_1, \ldots, x_n)$ of size bounded by the size of ϕ such that for all $a \in M^n$, $M \models C(a)$ if and only if $M \models \phi(a)$. Conversely, if $C(x_1, \ldots, x_n)$ is circuit, then there exists a quantifier-free formula $\phi(x_1, \ldots, x_n)$ such that for all $a \in M^n$, $M \models C(a)$ if and only if $M \models \phi(a)$. Note that the size of ϕ is in general not polynomial in the size of C. However, by quantifying the gates one can construct in polynomial time (in the standard sense) an existential formula $\psi(\bar{x})$ which is equivalent to C.
If X is a problem of M, $(C_n(x_1, \ldots, x_n, y_1, \ldots, y_k))_{n \geq 0}$ is sequence of circuits with k fixed, and $\alpha \in M^k$, we say that $(C_n(x, \alpha))_{n \geq 0}$ solves X if for all $n \geq 0$, for all $a \in M^n$, $a \in X$ iff $M \models C_n(a, \alpha)$. Of course the α are the parameters. Then, we have the following result: if $X \in \mathrm{TIME}_M^k(t)$ then there exists a sequence of circuits $(C_n(x_1, \ldots, x_n, y_1, \ldots, y_k))_{n \geq 0}$ and $\alpha \in M^k$ such that $(C_n(x, \alpha))_{n \geq 0}$ solves X and such that there exists a standard algorithm which outputs circuit $C_n(x, y)$ in time $p(Ot(n))$ where p is a polynomial depending on the model of computation (note that this implies that the size of C_n is at most $p(Ot(n))$). Note that the converse of this result is somewhat obvious. Thus, we can define the class P_M and EXP_M using circuits and the standard notion of polynomial and exponential algorithm. To define nonuniform complexity class we proceed as follows. We say that $X \in \mathrm{SIZE}_M^k(t)$ if there exists a sequences of circuits $(C_n(x_1, \ldots, x_n, y_1, \ldots, y_k))_{n \geq 0}$ and $\alpha \in M^k$ such that $(C_n(x, \alpha))_{n \geq 0}$ solves X and such that $size(C_n) \leq O(t(n))$.

Then, we define $\mathrm{SIZE}_M(t)$, $\mathbb{P}_M^k$, $\mathbb{P}_M$ and $\mathbb{EXP}_M$ in the obvious way. Again, one can define some of these classes using boolean advice functions. For example, $\mathbb{P}_M$ is the class $\mathrm{P}_M/\mathrm{polybool}$ where polybool is the class of function $f : \mathbb{N} \longrightarrow \{0,1\}^\infty$ such that the length of $f(n)$ is polynomial in n.

We turn our attention to nondeterministic classes. One can define the class NP_M as follows. A problem X is in NP_M iff there exist a polynomial p and a problem $Y \in \mathrm{P}_M$ such that for all $n \geq 0$, for all $a \in M^n$, $a \in X$ iff there exists $b \in M^{p(n)}$ such that $\langle a, b\rangle \in Y$. In the same way we can define $\mathrm{N}\mathbb{P}_M$, NA_M and $\mathrm{N}\mathbb{A}_M$ (one has to be a little more carefully for defining, say, NEXP_M). In the standard case, obviously we have $\mathrm{NA} = \mathrm{A}$. This is no longer true in the general case. In fact, it is easy to see that a structure M satisfies $\mathrm{N}\mathbb{A}_M = \mathbb{A}_M$ (respectively, $\mathrm{NA}_M = \mathrm{A}_M$) iff there is an tuple α of elements of M such that the theory of M with new constant symbols for the α admits elimination of quantifiers (respectively, effective elimination of quantifiers). We denote by SAT_M the problem of satisfiability of quantifier-free formulae with parameters in M (SAT_M can be viewed as a problem of M after an adequate coding of quantifier-free formulae). The problem SAT_M is NP_M and $\mathrm{N}\mathbb{P}_M$ complete. This implies that $\mathrm{P}_M = \mathrm{NP}_M$ iff there exist a tuple α of M and a polynomial algorithm in the sense of M which, given an existential formula $\psi(\bar{x})$ computes a circuit $C(\bar{x}, \bar{y})$ such that $\psi(\bar{x})$ is equivalent to $C(\bar{x}, \alpha)$ (for $\mathbb{P}_M = \mathrm{N}\mathbb{P}_M$ it suffices that C be of size polynomial in the size of ψ). Thus, if $\mathrm{P}_M = \mathrm{NP}_M$ or $\mathbb{P}_M = \mathrm{N}\mathbb{P}_M$, there is a tuple α of elements of M such that the theory of M with new constant symbols for the α admits elimination of quantifiers. This leads the theory of complexity over arbitrary structure to consider with a special attention structures M which admit quantifier elimination. However, it seems that the main gap in the theory is that there is no example of a structure M *in a finite language* with $\mathrm{P}_M = \mathrm{NP}_M$ or $\mathbb{P}_M = \mathrm{N}\mathbb{P}_M$. Note also that results of model theory can be applied: (i) if an infinite field K in the language $\{+, -, ., 0, 1, \alpha_1, \dots, \alpha_k\}$ where the α_i are constants admits quantifier elimination then K is an algebraically closed field; (ii) if an ordered field K in the language $\{+, -, ., 0, 1, <, \alpha_1, \dots, \alpha_k\}$ where the α_i are constants admits quantifier elimination then K is a real-closed field; (iii) if an infinite ordered abelian group G in the language $\{+, -, 0, \alpha_1, \dots, \alpha_k\}$ where the α_i are constants admits quantifier elimination then G is an ordered $\mathbb{Q}$-vector space of dimension ≥ 1 (see [23] for (i); (ii) and (iii) are direct consequences of [28, Theorem 2.3 and 2.1]). Thus for classical structures we know where to look for and since the quantifier elimination algorithms have been studied in detail, one may hope to prove something about the question P =? NP. Nevertheless, for the above structures this main question is still open (and it is conjectured that the answers are negative). There are at least two main differences between the classical work on algorithmic quantifier elimination and the question P_M =? NP_M. The first one is that for the question P_M =? NP_M we can use algorithms in the sense of M for eliminating quantifiers and thus use elements of M. The second one is that for the question P_M =? NP_M the eliminating formula can be a circuit which can be more compact than a quantifier-free formula.

Now we want to define the polynomial hierarchy. First of all, note that a problem X of M is NP_M iff there exist a sequence of existential formulae $(\phi_n(x_1,\ldots,x_n,y_1,\ldots,y_k))_{n\geq 0}$ and $\alpha \in M^k$ such that $(\phi_n(x,\alpha))_{n\geq 0}$ solves X and such that there exists a standard algorithm which constructs the formulae $\phi_n(x,y)$ in polynomial time (this comes from the fact that there exists a polynomial algorithm (in the standard sense) which, given a circuit $C(x_1,\ldots,x_n)$, constructs an existential formula $\phi(\bar{x})$ which is equivalent to C). Let $h \geq 1$ be an integer. Then we can define $\Sigma_{h,M}$ (respectively, $\Pi_{h,M}$) as the class of problem X of M which are solved by a sequence $(\phi_n(x,\alpha))_{n\geq 0}$ of Σ_h (respectively, Π_h) formulae of $\mathcal{L}$ with parameters $\alpha \in M^k$ such that $\phi_n(x,y)$ can be constructed by a standard polynomial algorithm. Of course, we set $\Delta_{h,M} = \Sigma_{h,M} \cap \Pi_{h,M}$ and PH_M is the union of all the $\Sigma_{h,M}$. We define the alternating polynomial time PAT_M in the same way by imposing that the formulae ϕ_n are in prenex form but without bounds on the alternation of quantifiers. The usual inclusions hold and these definitions are in accordance with the definitions using machine over M. One can also define the nonuniform counterpart of these classes: $\Sigma_{h,M}$/polybool, $\Pi_{h,M}$/polybool, $\mathbb{PH}_M$ and $\mathbb{PAT}_M$, by just imposing a polynomial size condition on the ϕ_n in the place of the standard algorithm.
One can be surprised by the importance we give to nonuniform complexity classes. There are a number of arguments in [14] in favor of nonuniformity. First we recall that if the structure M contains the reals with its addition and its usual order, then, in general, there is no difference between the uniform and the nonuniform setting since we can encode the advice function in the digits of a real number and take back these advices using $+$ and $<$. For example, for such a structure $\mathrm{P}_M = \mathbb{P}_M$ (and thus $\mathrm{NP}_M = \mathbb{NP}_M$), $\mathrm{EXP}_M = \mathbb{EXP}_M$ and $\mathrm{A}_M = \mathbb{A}_M$ (and the same thing holds for all the complexity classes defined above). Secondly, one can prove a Karp-Lipton Theorem for arbitrary structures (see Section 2.4). Finally, in this paper we need to work with nonuniform complexity classes. For example, for the ordered field of real algebraic numbers P/const $\neq$ P for somewhat obvious reasons (see Proposition 3.15 and Proposition 4.16).

2.3 A Model of Parallel Computation

As in the previous subsection we assume that all our circuits have only one output gate and that this gate is a test (thus, a circuit compute a function into $\{0,1\}$). We recall that the depth of a circuit is the length of a maximal directed path. Sequential time corresponds to the size of circuits. A natural way to define parallel time is to use the depth of circuits (see [2, Chapter X] for the standard case). However, to obtain a "concrete" model of computation (as opposed to the nonuniform one) one has to introduce some uniformity condition on the sequences of circuits.

Definition 2.1 *Let X be a problem of M and d a function from $\mathbb{N}$ into $\mathbb{N}^*$.*
We say that a problem X is $\mathrm{DEPTH}_M(d(n))$ if there exists a sequence of circuits $(C_n(x_1,\ldots,x_n,y_1,\ldots,y_k))_{n\geq 0}$ (k fixed) and a k-tuple α of M such that $(C_n(x,\alpha))$ solves X and such that the depth of C_n is $\leq O(d(n))$.

We say that X is $\mathrm{UDEPTH}_M(d(n))$ *(respectively,* $\mathbb{U}\mathrm{DEPTH}_M(d(n))$*) if, moreover, there exists a standard algorithm in* $\mathrm{SPACE}(d(n))$ *(respectively, in* $\mathrm{SPACE}(d(n))$ *with advices of size $O(d(n))$) which on input 1^n outputs C_n.*
By definition, X is $\mathbb{PAR}_M$ *if X is* $\mathrm{DEPTH}_M(n^c)$ *for a constant c. In the same way, we define* PAR_M *and* $\mathbb{P}\mathrm{AR}_M$ *with* UDEPTH_M *and* $\mathbb{U}\mathrm{DEPTH}_M$ *in place of* $\mathrm{DEPTH}_M(n^c)$*, and we define* $\mathbb{PEXP}_M$*,* PEXP_M *and* $\mathbb{P}\mathrm{EXP}_M$ *with $exp(n^c)$ in place of n^c.*

The definition above is not the same as the definition given in [8], [9] and [10]. However, it is not very difficult to show that the PAR defined here is equal to the PAR defined in the above cited papers.
With this definition, in order to show that a problem is in PAR one must first exhibit a family of polynomial depth circuits that solves the problem, and then show that this family can be constructed in polynomial space. We will often use a different characterization: a problem is in PAR if it can be solved in polynomial time by a parallel machine using an exponential ($2^{n^{O(1)}}$) number of processors. It can be shown as in the standard case that these two definitions are equivalent. See [5] for a formal development on parallel machines over the reals, and [2] for the standard case. The second definition is convenient because of its more algorithmic flavor. Thus, in order to show that a problem is in PAR, we will just describe informally a parallel algorithm that solves it in polynomial time; and to show that it is in $\mathbb{P}$AR, we will describe a parallel algorithm that solves it in polynomial time with the help of a polynomial amount of boolean advice.
Note that a circuit of depth d has size at most $\exp(cd(n))$ where c is a constant which depends only on $\mathcal{L}$. Thus the usual inclusion between parallel time d and sequential time $exp(d)$ holds. If M is a real-closed field which contains the reals $\mathbb{R}$, then, one can prove that $\mathbb{U}\mathrm{DEPTH}_M(d(n)) = \mathrm{UDEPTH}_M(d(n))$. Remark that $\mathbb{P}\mathrm{AR}_\mathbb{R}$ is strictly contained in $\mathbb{PAR}_\mathbb{R}$ (and the same thing is true for every real-closed fields). Indeed, we always have that $\mathcal{BP}(\mathbb{PAR}_M)$ is the set of all problems in $\{0,1\}^\infty$ and the proof of the main result of [10] implies that $\mathcal{BP}(\mathbb{P}\mathrm{AR}_\mathbb{R})$ is PSPACE/poly (if $\mathcal{C}$ is a complexity class over M, $\mathcal{BP}(\mathcal{C}_M)$ is the set of problems in $\{0,1\}^\infty$ which are $\mathcal{C}_M$). One might think that the class $\mathbb{PAR}_M$ does not have any interest, but note, for example, that $\mathbb{PAR}_\mathbb{R} \subseteq \mathrm{EXP}_\mathbb{R}$ and that the separation of $\mathrm{PAR}_\mathbb{R}$ and $\mathrm{EXP}_\mathbb{R}$ given in [8] and [9] is shown with $\mathbb{PAR}_\mathbb{R}$ in the place of $\mathrm{PAR}_\mathbb{R}$ (which gives a stronger result). We recall from [9] the relationship, for a real-closed field, between all the classes defined from now: P $\subseteq$ NP $\subseteq$ PH $\subseteq$ PAR $\subset$ EXP $\subseteq$ PEXP, PAR $\subset$ PAT $\subseteq$ PEXP. The relationship between EXP and PAT is not known ($\subseteq$ means the inclusion and that we do not known if the inclusion is strict). We have the same thing for the nonuniform setting (with $\mathbb{P}$AR in the place of PAR and $\mathbb{P}$EXP in the place PEXP) but we can strictly insert $\mathbb{PAR}$: ...$\mathbb{P}$AR $\subset$ $\mathbb{PAR}$ $\subset$ $\mathbb{EXP}$.... The inclusion PH $\subseteq$ PAR and PAT $\subseteq$ PEXP come from the "fast" algorithm of elimination of quantifier for real-closed fields (see section 4.1 for details).

The situation for the reals without multiplication (which leads to consider ordered $\mathbb{Q}$-vector spaces) is quite similar. The above inclusion and strict inclusion hold as well and no more is known.

2.4 A Karp-Lipton Theorem for Arbitrary Structures

We recall that the polynomial hierarchy is said to collapse at level h where $h \geq 1$ is an integer if any one of these three equivalent statements holds: $\Sigma_{h,M} = \Pi_{h,M}$, $\Sigma_{h+1,M} = \Sigma_{h,M}$, or $\Pi_{h+1,M} = \Pi_{h,M}$. Recall that for the standard case, if $\mathbb{P} = \mathbb{NP}$ then the uniform (standard) polynomial hierarchy collapse at its second level (see [18]). If M is an arbitrary structure we define $\mathrm{P}_M/\mathrm{poly}$ as for the standard case where poly is the set of functions f from $\mathbb{N}$ into M^∞ such that the length of $f(n)$ is polynomial (for the standard case see [1, Chapter IV]). Obviously, $\mathbb{P}_M \subseteq \mathrm{P}_M/\mathrm{poly}$ and this inclusion is in general strict (if M is infinite).

Theorem 2.2 *Let M be an arbitrary structure. If* $\mathrm{NP}_M \subseteq \mathrm{P}_M/\mathrm{poly}$ *then the (uniform) polynomial hierarchy over M collapses at the third level.*

Proof. Assume that $\mathrm{NP}_M \subseteq \mathrm{P}_M/\mathrm{poly}$ and let $X \in \mathrm{NP}_M$. By definition, there exists a polynomial p and $Y \in \mathrm{P}_M$ such that

$$\forall x \in M^n \; [x \in X \Leftrightarrow \exists y \in M^{p(n)} \langle x, y\rangle \in Y].$$

Since $\mathrm{NP}_M \subseteq \mathrm{P}_M/\mathrm{poly}$, there exists another problem $Z \in \mathrm{P}_M$, a polynomial q and a sequence $a_n \in M^{q(n)}$ such that

$$\forall x \in M^n \; [x \in X \Leftrightarrow \langle x, a_n\rangle \in Z].$$

Note that the set of $a \in M^{q(n)}$ that are "good advice" can be defined by the formula

$$\forall x \in M^n \; [\langle x, a\rangle \in Z \Leftrightarrow \exists y \in M^{p(n)} \langle x, y\rangle \in Y].$$

In prenex form this gives:

$$\forall x \in M^n \; \forall z \in M^{p(n)} \; \exists y \in M^{p(n)} \; \langle x, y, z, a\rangle \in W \tag{2}$$

where the polynomial-time set W is defined by

$$(\langle x, a\rangle \in Z \wedge \langle x, y\rangle \in Y) \vee (\langle x, a\rangle \notin Z \wedge \langle x, z\rangle \notin Y).$$

We are now ready to prove that $\Sigma_{3,M} = \Pi_{3,M}$. Thus, let $L \in \Sigma_{3,M}$. By definition, for $x \in M^n$, $x \in L$ iff

$$\exists u_1 \; \forall u_2 \; \langle x, u_1, u_2\rangle \in X,$$

where $X \in \mathrm{NP}_M$ (here each quantified variable is in $M^{p(n)}$ for some polynomial p; from now on this is omitted for notational simplicity). We can apply the remarks above to X. Thus there exists $Z \in \mathrm{P}_M$ such that for any $x \in M^\infty$, $x \in L$ iff for any a which is a good advice for X,

$$\exists u_1 \; \forall u_2 \; \langle x, u_1, u_2, a\rangle \in Z.$$

Using the characterization of good advice given by (2), this is equivalent to

$$\forall a \; [\forall x', u_1', u_2' \forall z \exists y \langle x', u_1', u_2', y, z, a\rangle \in W \Rightarrow \exists u_1 \forall u_2 \langle x, u_1, u_2, a\rangle \in Z]$$

where $W \in \mathrm{P}_M$. This is equivalent to

$$\forall a \; [\exists u_1 \forall u_2 \langle x, u_1, u_2, a\rangle \in Z \vee \exists U \exists z \forall y \langle U, y, z, a\rangle \notin W]$$

where U stands for x', u_1', u_2'. Finally, this is equivalent to

$$\forall a \; \exists u_1, U, z \; \forall u_2, y \; [\langle x, u_1, u_2, a\rangle \in Z \vee \langle X, y, z, a\rangle \notin W].$$

Hence $L \in \Pi_{3,M}$. $\square$

3 The Abstract Theory

In this section M will be a first order structure in a finite language $\mathcal{L}$ and N will be in general an (elementary) extension of M. $\mathcal{C}$ will be a "good" complexity class. We do not want to give a formal definition and here a good complexity class will be one of the global complexity class defined in the preliminaries such as P, $\mathbb{P}$, $\mathbb{P}$AR NP,..., A, $\mathbb{A}$.

3.1 Restrictions and Extensions

The restriction X of a subset $Y \subseteq N^n$ to a smaller structure $M \leq N$ is defined in the natural way: $X = Y \cap M^n$. The restriction of a problem $Y \subseteq N^\infty$ is $X = \bigcup_{n \in \mathbb{N}} (Y \cap M^n)$. If X is a restriction of Y we say that Y is an extension of X. In general a given set or problem has too many different extensions for this notion to be useful. We will only consider extensions of definable sets and problems, and will usually require that Y be defined by the same *quantifier-free* formula(e) over N as X over M. This is justified by the following obvious observation.

Lemma 3.1 *Let $X \subseteq M^n$ be defined by a first-order formula ϕ over M. Let $Y \subseteq N^n$ be defined by the same formula in an extension N of M. If ϕ is quantifier-free, $X = Y \cap M^n$.* $\square$

This is no longer true for quantified formulae. For instance, the formula $\forall x \; x^2 \neq 2$ defines $X = \mathbb{Q}$ over $\mathbb{Q}$, but defines the empty set over $\mathbb{C}$. Even with quantifier-free formulae, the extension may not be unique. For instance, the set $X = \mathbb{Q}$ can be defined by the formula $x = x$ over $\mathbb{Q}$. The corresponding extension to

$N = \mathbb{C}$ is $B = \mathbb{C}$. The same X can also be defined by the formula $x^2 \neq 2$. The corresponding extension now is $\mathbb{C} \setminus \{-\sqrt{2}, \sqrt{2}\}$. These difficulties disappear if $M \leq N$ is an elementary extension: one can now use quantified formulae, and the extension of a definable problem is uniquely defined.

Lemma 3.2 *Let $X \subseteq M^n$ be defined by a formula ϕ. If N is an elementary extension of M, the subset $X' \subseteq N^n$ defined by ϕ interpreted in N is an extension of X. Moreover, X' is the only extension of X to N that can be defined by a formula with parameters in M.*

Proof. It follows immediately from the elementary extension hypothesis that X is the restriction of X' to M.
Let $X'' \subseteq N^n$ be defined by a formula ψ with parameters in M. If X'' is an extension of X, it follows from elementary equivalence that X is defined by ψ. Thus the following formula holds:

$$\forall x \in M^n \ \phi(x) \Leftrightarrow \psi(x).$$

Again by elementary equivalence, this formula must also hold in N, hence $X' = X''$. $\square$

Note that the above lemma holds ("by definition") for problems. Thus, if X is a definable set or a definable problem of M and if N is an elementary extension the extension of X to M is well-defined. Note that if X is a problem in $\mathcal{C}_M$, then it is definable. Thus we have the following obvious lemma.

Lemma 3.3 *Let $M \leq N$ be an elementary extension and let X be a problem of M in $\mathcal{C}_M$, then the extension of X to N is $\mathcal{C}_N$ with the same algorithm that solves X over M.* $\square$

Let A be a subset of N. We denote by $\mathcal{C}_N(A)$ the class of problems which are in $\mathcal{C}_N$ with a machine (or a sequences of circuits) which uses parameters from A. If $M \leq N$ is an elementary extension and if Y is a problem of N definable with parameters from M, then it is easily verified that the restriction of Y to M is definable by the same family of formulae that define Y. Thus we have:

Lemma 3.4 *Let $M \leq N$ be an elementary extension and let Y be a problem of $\mathcal{C}_N(M)$, then the restriction of Y to M is $\mathcal{C}_M$ with the same algorithm that solves Y over N.* $\square$

Now we state a general version of an upward transfer for question of the form $\mathcal{C} =? \mathcal{C}'$ due to Michaux [26].

Lemma 3.5 *Let $M \leq N$ be an elementary extension, $\mathcal{C}'$ be good complexity class and $\mathcal{D}$ a good deterministic complexity class such that $\mathcal{D} \subseteq \mathcal{C} \subseteq \mathcal{C}'$ for N and M. Assume that there is a problem S in $\mathcal{C}'_N(M)$ which is $\mathcal{C}'_N$-complete under $\mathcal{D}_N$-reduction such that the reduction of a problem in $\mathcal{C}'_N(M)$ to S can be performed with parameters in M (i.e., a $\mathcal{D}_N(M)$-reduction). Then, the restriction of S to M is $\mathcal{C}'_M$-complete under $\mathcal{D}_M$-reduction and if $\mathcal{C}_M = \mathcal{C}'_M$ then $\mathcal{C}_N = \mathcal{C}'_M$.*

Proof. Since S is in $\mathcal{C}'_N(M)$ Lemma 3.4 implies that the restriction of S is in $\mathcal{C}'_M$. Let X be a problem of $\mathcal{C}'_M$, then the extension Y of X to N is in $\mathcal{C}'_N(M)$ by Lemma 3.3. Thus there exists a $\mathcal{D}_N(M)$-reduction of Y to S. Then, this reduction gives "by Lemma 3.4" a $\mathcal{D}_M$-reduction of X to the restriction of S to M. We have shown that the restriction of S to M is $\mathcal{C}'_M$-complete under $\mathcal{D}_M$-reduction. Now, assume that $\mathcal{C}_M = \mathcal{C}'_M$, then the restriction of S to M is $\mathcal{C}_M$ and thus S is $\mathcal{C}_N$ by Lemma 3.3. By $\mathcal{C}'_M$-completeness of S, $\mathcal{C}_N = \mathcal{C}'_M$. □

Let us recall that the formulae satisfiability problem SAT_M is NP_M-complete in any structure M. Moreover, SAT_M is clearly in $\mathrm{NP}_M(\emptyset)$ and the proof of the NP_M-hardness of SAT_M shows that if $X \in \mathrm{P}_M$ then there is a $\mathrm{P}_M(\emptyset)$-reduction of X to SAT_M (the same is true if we replace P by $\mathbb{P}$). Note also that if $M \leq M$ is an elementary extension, then the restriction of SAT_N is SAT_M and the extension of SAT_M is SAT_N.

Corollary 3.6 *If N is an elementary extension of M, $\mathrm{P}_M = \mathrm{NP}_M$ implies $\mathrm{P}_N = \mathrm{NP}_N$.* □

Note that the following complexity classes (and their nonuniform counterpart) have a complete problem (under P-reduction) with the same properties as SAT: $\Sigma_{h,M}$, $\Pi_{h,M}$, PAR_M, EXP_M, PAT_M.

3.2 $\mathcal{C}$-saturation

The following proposition gives examples of $\mathcal{C}$-saturated structures. It is essentially due to Michaux [26] as some of the ideas of this subsection, however, the presentation is slightly different and there are additional results.

Proposition 3.7 *Every $\aleph_1$-saturated structure is $\mathcal{C}$-saturated.*

Proof. Let $X \in \mathcal{C}^0_M/k$, and let $Y \in \mathcal{C}^0_M$ be the corresponding problem given by (1). For every $j \in \mathbb{N}$, let $\phi_j(y)$ be the formula

$$\forall x \in M^j \ \langle x, y\rangle \in Y \Leftrightarrow \langle x, \alpha_j\rangle \in Y$$

where the free variable y lives in M^k. By definition of $\mathcal{C}^0_M/k$, any finite subset $\{\phi_1(y), \ldots, \phi_n(y)\}$ of the family $\{\phi_n(y);\ n \in \mathbb{N}\}$ is satisfied by α_n. Since M is $\aleph_1$-saturated, this implies that there exists $\alpha \in M^k$ satisfying the whole family. Hence for any $x \in M^\infty$, $x \in X$ if and only if $\langle x, \alpha\rangle \in Y$. This shows that $X \in \mathcal{C}^k_M$. □

If X is in $\mathcal{C}_M/\mathrm{const}$, then X is definable (with parameters in M), thus if N is an (elementary) extension of M, the extension of X to N is well-defined. We can be more precise.

Lemma 3.8 *Let $M \leq N$ be an elementary extension, $k \in \mathbb{N}$ and let X be a definable problem of M. Then, X is in $\mathcal{C}^0_M/k$ if and only if the extension of X to N is in $\mathcal{C}^0_N/k$.*

Proof. Assume that $X \in \mathcal{C}^0_M/k$, and let $Y \in \mathcal{C}^0_M$ be the corresponding problem given by (1). Let X' and Y' be the extensions of X and Y to N. Since N is an elementary extension, it follows from (1) that

$$\forall x \in N^{\leq n}\ [x \in X' \Leftrightarrow \langle x, \alpha_n \rangle \in Y'].$$

Hence $X' \in \mathrm{P}^0_N/k$.
Conversely, assume that the extension X' of X to N is $\mathcal{C}^0_N/k$ and that X is definable by a sequence $(\phi_n)_{n\geq 0}$ of first-order formulae with parameters in M. Since N is an elementary extension of M, the sequence $(\phi_n)_{n\geq 0}$ defines X'. Moreover, there exists $Y' \in \mathcal{C}^0_N$ such that for all $n \geq 0$, the following formula holds:

$$\exists \alpha \in N^k\ \forall x \in N^{\leq n}\ [\phi_n(x) \Leftrightarrow \langle x, \alpha \rangle \in Y'].$$

Since $Y' \in \mathcal{C}^0_N$, Y' is $\emptyset$-definable and the restriction Y of Y' to M is $\mathcal{C}^0_M$ and $\emptyset$-definable with the same formulae. Thus, by elementary equivalence, the formula

$$\exists \alpha \in M^k\ \forall x \in M^{\leq n}\ [\phi_n(x) \Leftrightarrow \langle x, \alpha \rangle \in Y]$$

must hold for all $n \geq 0$. Hence $X \in \mathcal{C}^0_M/k$. $\square$

We can characterize $\mathcal{C}_M/\mathrm{const}$ in terms of extensions.

Proposition 3.9 *X is in $\mathcal{C}_M/\mathrm{const}$ if and only if X is definable and there exists an elementary extension N of M such that the extension of X to N is $\mathcal{C}_N$.*

Proof. Assume that $X \in \mathcal{C}_M/\mathrm{const}$. We know that M has an $\aleph_1$-saturated elementary extension N. By Lemma 3.8 the extension X' of X to N is $\mathcal{C}_N/\mathrm{const}$ and by Proposition 3.7 X' is $\mathcal{C}_N$.
Conversely, assume that X is a definable problem of M such that there exists an elementary extension N of M such that the extension X' of X to M is in $\mathcal{C}^k_N$, then X' is in $\mathcal{C}^0_N/k$ and by Lemma 3.8 X is in $\mathcal{C}^0_M/k$. $\square$

We can also characterize $\mathcal{C}$-saturation in term of "elimination of parameters". But here we need to work with a theory T (say the theory of M).

Proposition 3.10 *Let T be a first-order complete theory (in a finite language). The following properties are equivalent:*
(a) for all $M \models T$, $\mathcal{C}_M/\mathrm{const} = \mathcal{C}_M$;
(b) for all $N \models T$ and all elementary restrictions M of N, if Y is $\mathcal{C}_N$ and definable with parameters in M then Y is $\mathcal{C}_N(M)$.
(c) for an $\aleph_1$-saturated model N of T and for all elementary restrictions M of N, if Y is $\mathcal{C}_N$ and definable with parameters in M then Y is $\mathcal{C}_N(M)$.

Proof. The implication (b) $\Rightarrow$ (c) is obvious. Assume (a) and let us prove (b). Let $M \leq N$ be an elementary extension of models of T and let Y be in $\mathcal{C}_N$ and definable with parameters in M. Then, the restriction X of Y to M is also definable and by Proposition 3.9, X is $\mathcal{C}_M/\mathrm{const}$ and thus $\mathcal{C}_M$ by hypothesis. Since the extension of X to N is Y, by Lemma 3.3, we see that $Y \in \mathcal{C}_N(M)$.
Assume (c) and let us prove (a). Let N be an $\aleph_1$-saturated model of T and let X be a problem in $\mathcal{C}_M/\mathrm{const}$. Then, X is definable using only countably many parameters in M and by the Tarski-Löwenheim-Skolem theorem M has a countable elementary restriction M_0 which contains all these parameters. Then the restriction X_0 of X to M_0 is in $\mathcal{C}_{M_0}/\mathrm{const}$ and the extension of X_0 to M is X. By $\aleph_1$-universality of N, M_0 can be elementarily embedded in N. Then, by Lemma 3.8 and Proposition 3.7, the extension Y of X_0 to N is $\mathcal{C}_N$. By hypothesis, Y is in $\mathcal{C}_N(M_0)$. Thus X_0 is $\mathcal{C}_{M_0}$ and it follows that X is $\mathcal{C}_M$. $\square$

Note that for the equivalence of (a) and (b) we do not need the completeness of T. Michaux has introduced the class $\mathrm{P}_M/\mathrm{const}$ motivated by the following proposition (which holds at the nonuniform level).

Proposition 3.11 *If* $\mathrm{P}_M = \mathrm{P}_M/\mathrm{const}$ *and N is an elementary extension of M,* $\mathrm{P}_N = \mathrm{NP}_N$ *implies* $\mathrm{P}_M = \mathrm{NP}_M$.

Proof. $\mathrm{SAT}_N \in \mathrm{P}_N$ if $\mathrm{P}_N = \mathrm{NP}_N$. As pointed out before Corollaries 3.6, SAT_M is the restriction of SAT_N to M. Hence $\mathrm{SAT}_M \in \mathrm{P}_M/\mathrm{const}$ by Proposition 3.9 (SAT_N is $\emptyset$-definable). This implies $\mathrm{SAT}_M \in \mathrm{P}_M$ if $\mathrm{P}_M = \mathrm{P}_M/\mathrm{const}$, and thus $\mathrm{P}_M = \mathrm{NP}_M$ by definition of NP-completeness. $\square$

Notice that in the above proposition we do not need the full force of the hypothesis. Assume for simplicity that the theory of M admits elimination of quantifiers. We only need that $\mathrm{P}_M/\mathrm{const} \cap \mathbb{A}^0_M \subseteq \mathrm{P}_M$ or even that $\mathrm{P}_M/\mathrm{const} \cap \mathrm{A}^0_M \subseteq \mathrm{P}_M$ if the theory of M is decidable (i.e., if we have a standard algorithm deciding whether each parameter-free sentence in the first-order theory of M is true or false). Note that the proof of Proposition 3.7 implies that if M is ω-saturated, (respectively, recursively saturated) then $\mathrm{P}_M/\mathrm{const} \cap \mathbb{A}_M = \mathrm{P}_M$ (respectively, $\mathrm{P}_M/\mathrm{const} \cap \mathrm{A}_M = \mathrm{P}_M$). One can also characterize the above equalities in terms of extension and in terms of elimination of parameters.

The proof of the above proposition shows that if $M \leq N$ is an elementary extension and if $\mathbb{P}_N = \mathrm{N}\mathbb{P}_N$, then $\mathrm{SAT}_M \in \mathbb{P}_M/\mathrm{const}$ and thus $\mathrm{N}\mathbb{P}_M \subseteq \mathbb{P}_M/\mathrm{const}$. Since, obviously, $\mathbb{P}_M/\mathrm{const} \subseteq \mathrm{P}_M/\mathrm{poly}$, Theorem 2.2 gives:

Proposition 3.12 *Let N be an elementary extension of M. $\mathrm{P}_N = \mathrm{NP}_N$ (or $\mathbb{P}_N = \mathrm{N}\mathbb{P}_N$) implies that the uniform polynomial hierarchy for M collapses at the third level.* $\square$

One can generalize Proposition 3.11 as follows (we do not need complete problems).

Proposition 3.13 *Let $\mathcal{C}'$ be a good complexity class such that for all elementary extension N of M, $\mathcal{C}_N \subseteq \mathcal{C}'_N$. If $\mathcal{C}_M/\mathrm{const} = \mathcal{C}_M$ and if N is an elementary extension of M, $\mathcal{C}_N = \mathcal{C}'_N$ implies $\mathcal{C}_M = \mathcal{C}'_M$.*

Proof. Let X be a problem of $\mathcal{C}'_M$. Since $\mathcal{C}'_M$ is good, X has an extension X' to N which is $\mathcal{C}'_N$ and thus $\mathcal{C}_N$ by hypothesis. By Proposition 3.9, $X \in \mathcal{C}_M/\mathrm{const}$ and thus by hypothesis $X \in \mathcal{C}_M$. $\square$

Another motivation is the existence of a Ladner-type theorem in P-saturated structures.

Fact 3.14 *Let M be a structure such that $\mathrm{NP}_M \subsetneq \mathrm{P}_M/\mathrm{const}$. Assume that the theory of M is decidable. Then there exist problems in $\mathrm{NP}_M \backslash (\mathrm{P}_M/\mathrm{const})$ which are not NP_M-complete.*

In particular, there are non-NP_M-complete problems in $\mathrm{NP}_M \backslash \mathrm{P}_M$ if M is P-saturated, has a recursive decision problem, and $\mathrm{P}_M \neq \mathrm{NP}_M$.
For a proof the reader can consult [3]. The first Ladner-type theorem in the BSS model was established in [24] for $M = \mathbb{C}$. In that paper, the authors first showed the result for $\bar{\mathbb{Q}}$ using the countability of $\bar{\mathbb{Q}}$. Their argument can be generalized for some other countable structures. For example, it is possible to prove a Ladner-type theorem for the real algebraic numbers. However, the case of the ordered field of the reals is open. Both [3] and [24] follow closely Ladner's original proof [22] for the standard case $M = \{0, 1\}$.
Note that one can obtain a nonuniform version of Theorem 3.14 (replace P by $\mathbb{P}$ and NP by $\mathrm{N}\mathbb{P}$), moreover in this case there is no need for the decidability of the theory of M.

3.3 Some Counterexamples

If R is a countable real-closed field or a countable ordered $\mathbb{Q}$-vector space, then there are problems in $\mathrm{P}^0_R/1$ which are not A_R. This can be explained as follows. Let B be a subset of M. A (quantifier-free) k-type of M over B is a consistent set of (quantifier-free) formulae with parameters in B in k fixed free variables, maximal for these properties. Equivalently, a (quantifier-free) k-type of M over B is the set of (quantifier-free) formulae with parameters in B satisfied by a k-tuple a of an elementary extension N of M. We denote by $tp(a/B)$ (and $tp^{qf}(a/B)$) these sets of formulae. Note that such a set of formulae is finitely satisfiable in M.

Proposition 3.15 *Assume that M is a countable structure with uncountably many quantifier-free k-types over $\emptyset$. Then, there are boolean problems in P^0_M/k which are not A_M.*

Proof. Let $\sigma(x_1, \ldots, x_k)$ be a quantifier-free k-type of M over $\emptyset$. Then, after an adequate encoding of quantifier-free formulae, σ can be viewed as a boolean problem of M. Let n be an integer. There is a finite number of quantifier-free formulae with variables $x_1, \ldots, x_k$ of size $\leq n$. Thus, since σ is finitely satisfiable in M, there exists a_n in M^k such that for all quantifier-free formulae $\psi(x_1, \ldots, x_k)$ of size $\leq n$, $\psi \in \sigma$ iff $M \models \psi(a_n)$. Since, we can decide whether $M \models \psi(a_n)$? in time polynomial in the size of ψ, we see that σ is P^0_M/k. Now, we can conclude by a simple cardinality argument. If M is countable there is at most a countable number of problems in A_M. Thus, if we have uncountably many quantifier-free k-types over $\emptyset$, most of them are not A_M. $\square$

Let R be a real-closed field. Then, R has uncountably many quantifier-free 1-types over $\emptyset$. Indeed, consider a real-closed extension R_1 of R containing $\mathbb{R}$ (such extension is elementary by elimination of quantifiers for real-closed fields). If a and b are in $\mathbb{R}$, then $a = b$ iff $tp^{qf}(a/\emptyset) = tp^{qf}(b/\emptyset)$. The same argument works for ordered $\mathbb{Q}$-vector spaces.

Let B be a *finite* subset of M and let σ be a quantifier-free k-type of M over B. Then, as in the proof above we can view σ as a problem in P^l_M/k where l is the cardinality of B. One can also associate to σ the set of 'decisional' circuits in k variables with parameters in B equivalent to a quantifier-free formula of σ (i.e., a circuit k-type of M over B). This problem is in P^l_M/k and is a priori more difficult to solve with a fast algorithm over M. It seems to us that the above family of problems gives good tests for the questions $\mathrm{P}_M/\mathrm{const} =? \mathrm{P}_M$, $\mathbb{P}_M/\mathrm{const} =? \mathbb{P}_M$,..., $\mathrm{A}_M/\mathrm{const} =? \mathrm{A}_M$ and $\mathbb{A}_M/\mathrm{const} =? \mathbb{A}_M$.

Let T be a complete theory which admits elimination of quantifiers. A (quantifier-free) k-type of T over $\emptyset$ is a (quantifier-free) k-type of a model M of T over $\emptyset$ (since T is complete such a set is finitely satisfiable in every model of T). By elimination of quantifiers, a type is determined by its quantifier-free part. Thus, if $\mathrm{A}_M/\mathrm{const} = \mathrm{A}_M$ for a countable model of T, T has countably many types over $\emptyset$. A theory with this property is called small by a model theorist. A theory is small if and only if T has a countable ω-saturated model M_1 (which is unique up to an isomorphism). Moreover, a small theory has an elementary prime model M_0: M_0 is a model of T which can be elementarily embedded in every model of T (M_0 is unique up to isomorphism). Note that the above family of problems are obviously in P_{M_1} and that all these problems (with $B = \emptyset$) are, say, $\mathbb{P}_M$ for every models of T iff all these problems are $\mathbb{P}_{M_0}$.

Now we construct an example where $\mathbb{A}/\mathrm{const} = \mathbb{A}$ but where $\mathrm{P}/\mathrm{const}$ is not included in $\mathbb{P}$. For this, we consider a countable version of the "arborescent" dictionary of [14]. The underlying set M is the disjoint union of the booleans $\{0,1\}$ and the set of functions u from $\{0,1\}^\infty$ into $\{0,1\}$ satisfying the following property: there exists n such that u is constant on the elements of $\{0,1\}^\infty$ of size $\geq n$. The language is constituted of two constants for the booleans and of three unary functions r (roots), d (right) and g (left) which are the identity on the booleans, such that $r(u) = u(\emptyset)$ (hence $r(u)$ is a boolean) and such that $d(u)$ and $g(u)$ are functions from $\{0,1\}^\infty$ into $\{0,1\}$ defined by $d(u)(x) = u(0x)$ and $g(u)(x) = u(1x)$. It is easy to see that the theory of M admits elimination of quantifiers. Moreover, it is not very difficult to show that if N is an elementary extension of M and if Y is a problem of N in $\mathbb{A}_N$, then the restriction of Y to M is $\mathbb{A}_M$ (i.e., M is $\mathbb{A}$-stable, see the next subsection) and thus by Lemma 3.9, $\mathbb{A}_M/\mathrm{const} = \mathbb{A}_M$ (note that one can apply Proposition 3.15 to see that $\mathrm{A}_M/\mathrm{const} \neq \mathrm{A}_M$). We claim that every boolean problem is $\mathrm{P}_M/\mathrm{const}$. Indeed, let X be a boolean problem. For an integer n we consider the element u_n of M defined by: $u_n(x) = 0$ if x is of size $> n$ or if $x \notin X$, and $u_n(x) = 1$ otherwise. Then, it is easy to construct in polynomial time a sequence of circuits (using the selector!) $(C_n(x,y))$ such that $(C_n(x,u_n))$ shows that X is in $\mathrm{P}_M/\mathrm{const}$. On the other hand, since a given u in M contains only a finite amount of information, it is not difficult to prove that a boolean problem in $\mathbb{P}_M$ is in $\mathrm{P}/poly$.

Now we give an example of a structure M such that $\mathbb{A}_M/\mathrm{const} \neq \mathbb{A}_M$ (and which admits elimination of quantifiers). The underlying set M is the disjoint union of $\mathbb{N}$ and of the set of ultimately constant sequences u on two fixed symbols α and β. The language is constituted of two constants for the 0 and the 1 of $\mathbb{N}$, of a unary predicate P which defines $\mathbb{N}$, of a unary function s which is the successor function on $\mathbb{N}$ and the identity elsewhere, and of a ternary predicate R such that $M \models R(n,u,v)$ iff $n \in \mathbb{N}$, u and v are not in $\mathbb{N}$ and for any integer m with $0 \leq m \leq n$ $u(m) = v(m)$. Note that for $n \in \mathbb{N}$, $R(n,x_1,x_2)$ defines an equivalence relation on $M\backslash\mathbb{N}$. It is not very difficult to prove that the theory of M admits elimination of quantifiers. Then, we consider a *non ultimately constant* sequence u on α and β (thus $u \notin M$). For a positive integer we consider the sequence u_n of M defined by $u_n(m) = u(m)$ if $m \leq n$ and by $u_n(m) = \alpha$ otherwise. Then, we consider the problem Y defined by $\langle a_1,\ldots,a_n\rangle \in Y$ iff $R(s^n(0), a_1, a_n)$. It is clear that $Y \in \mathrm{P}_M$ and that the problem defined by $\langle a_1,\ldots,a_n\rangle \in X$ iff $\langle a_1,\ldots,a_n,u_n\rangle \in Y$ is in $\mathrm{P}^0_M/1$. We claim that X is not $\mathbb{A}_M$. The proof of this is left to the reader.

The following result sheds some light on the above example. It also stresses the importance of definable equivalence relations.

Proposition 3.16 *Assume that the theory of M admits elimination of quantifiers. $\mathbb{A}_M/\mathrm{const} = \mathbb{A}_M$ if and only if for every integer $k \geq 1$, every sequence $(E_n(x,y))_{n\geq 0}$ of $\emptyset$-definable equivalence relations of M^k such that E_{n+1} refines E_n, and for every sequences $(S_n)_{n\geq 0}$ such that S_n is a class of E_n and such that $S_{n+1} \subseteq S_n$, there exists a tuple β of M such that all the sets S_n are β-definable.*

Proof. Assume that $\mathbb{A}_M/\mathrm{const} = \mathbb{A}_M$. Let β_n be an element of S_n. Then, $(E_n(x,\beta_n))_{n\geq 0}$ defines a k-dimensional problem in $\mathbb{A}^0_M/k$ such that $X \cap M^n = S_n$. Thus, this problem is in $\mathbb{A}_M$ and this gives the conclusion.
Conversely, let X be a problem in $\mathbb{A}^0_M/k$. There exist a sequence of quantifier-free formulae $(\phi_n(x_1,\ldots,x_n,y_1,\ldots,y_k))_{n\geq 0}$ and a sequence $(\beta_n)_{n\geq 0}$ of k-tuples of M such that $\phi_n(x,\beta_m)$ defines $X\cap M^n$ if $m \geq n$. For $n \geq 0$, we consider the equivalence relation $E_n(y,z)$ of M^k defined by the parameter-free formulae

$$\forall x \in M^n \quad \bigwedge_{i=0}^{n}(\ \phi_i(x,y) \Leftrightarrow \phi_i(x,z)\ ).$$

Let S_n be the equivalence class of β_n for E_n. Then, by definition of $\mathbb{A}^0_M/k$, we can apply our hypothesis. There is a tuple β of M and a sequence of parameter-free formulae $\theta_n(y,u)$ such that $\theta_n(y,\beta)$ define S_n. Then, we consider the formula

$$\exists y \in M^k \quad \theta_n(y,\beta)\ \wedge \phi_n(x,y).$$

By elimination of quantifier, the above formula is equivalent to a quantifier-free formula $\psi_n(x,\beta)$. Clearly, the sequence of formula $(\psi_n(x,\beta))_{n\geq 0}$ shows that X is $\mathbb{A}_M$. $\square$

Of course, one can state a version of the above Proposition for A_M. In light of this, one can probably construct a structure M such that $\mathrm{A}_M/\mathrm{const} = \mathrm{A}_M$ and $\mathbb{A}_M/\mathrm{const} \neq \mathbb{A}_M$!

3.4 A Word on $\mathcal{C}$-stability

Let T be a theory (in a finite language), M a model of T and $\mathcal{C}$ a good complexity class. We denote by $\mathcal{C}_M/\mathrm{ext}(T)$ the class of problems X of M which are the restriction of a problem $Y \in \mathcal{C}_N$ of an extension N of M such that $N \models T$. Obviously, $\mathcal{C}_M \subseteq \mathcal{C}_M/\mathrm{ext}(T)$. We say that M is $\mathcal{C}_T$-stable if $\mathcal{C}_M = \mathcal{C}_M/\mathrm{ext}(T)$ and we say that T is $\mathcal{C}$-stable if every model of T is $\mathcal{C}_T$-stable. We denote by $\mathcal{C}_M/\mathrm{ext}$ the class of problems X of M which are the restriction of a problem Y of an *elementary extension* N of M (here the theory T does not play any role). We say that M is $\mathcal{C}$-stable if $\mathcal{C}_M = \mathcal{C}_M/\mathrm{ext}$. Let T' be the theory of M. It is easy to see that $\mathcal{C}_M \subseteq \mathcal{C}_M/\mathrm{ext} \subseteq \mathcal{C}_M/\mathrm{ext}(T') \subseteq \mathcal{C}_M/\mathrm{ext}(T)$. A priori all these inclusions are in general strict. However, for example, if T' admits elimination of quantifiers or if $\mathcal{C}$ is deterministic, then $\mathcal{C}_M/\mathrm{ext} = \mathcal{C}_M/\mathrm{ext}(T')$.
An immediate consequence of Proposition 3.9 is that *if M is $\mathcal{C}$-stable, then M is $\mathcal{C}$-saturated.* Let $M \leq N$ be an elementary extension and Let Y be a problem of N in $\mathcal{C}_N$ with a restriction X to M which is definable. In general the extension of X to N is not Y and Y is not in general definable with parameters in M. In other words, the restriction X can be a drastically "different" problem than Y (the proof of Theorem 4.26 give some examples). However, things can sometimes work nicely:

Proposition 3.17 *Let $M \leq N$ be an elementary extension and $Y \in \mathcal{C}_N$. If Y is definable with parameters in M and if M is $\mathcal{C}$-stable, Y is $\mathcal{C}_N(M)$.*

This follows from the $\mathcal{C}$-saturation of M and from Proposition 3.10, but there is a more direct proof.

Proof. By definition of $\mathcal{C}$-saturation, the restriction X of Y to M is $\mathcal{C}_M$. By Lemma 3.3, the extension of X to N is $\mathcal{C}_N(M)$. But this extension is Y since Y is definable with parameters in M. $\square$

There are connections between $\mathcal{C}$-stability and stability in model theory (a very important part of model theory studied by Shelah and a number of mathematicians). These connections will be considered in detail elsewhere. Let us say a word on this. Let T be a first order theory. For simplicity we assume that T is complete and admits elimination of quantifiers. Then, if T is $\mathbb{A}$-stable (respectively, A-stable), then T is superstable (respectively, ω-stable). We do not want to recall the definition of a superstable theory and of an ω-stable theory. It is easy for algorithmician to understand what a stable theory is (stability implies superstability and superstability implies ω-stability): T is stable iff for every elementary extension $M \leq N$ of models of T, if Y is a definable problem of N then the restriction of Y to M is definable.
A typical example of ω-stable theory is the theory of algebraically closed fields of fixed characteristic. On the other hand, if we can (first-order) define an infinite linear order on a model of T, then the theory is not stable. In particular, the theory of real-closed fields and the theory of ordered $\mathbb{Q}$-vector spaces are not $\mathbb{A}$-stable and in fact not P-stable neither $\mathbb{P}$-stable (this is obvious: see Proposition 4.22). However, it is not completely obvious to show that $\mathbb{R}$ is not P-stable (see Theorem 4.24) and we will see that $\mathbb{R}$ viewed as an ordered $\mathbb{Q}$-vector space is P-stable (see Section 5.3). In fact, these properties correspond to a general result of Marker and Steinhorn on o-minimal theories (first proved by van den Dries [35] in the case of real-closed fields) which can be stated as follows for an algorithmician: Let M be an o-minimal structure and $M \leq N$ an elementary extension which is Dedekind complete: if Y is a definable problem of N, then the restriction of Y to M is definable.
With our terminology, a remarkable result of Blum, Cucker, Shub, and Smale [4] says that if K is a field contained in the algebraic closure of $\mathbb{Q}$, then K is P_{F_0}-stable where F_0 is the theory of fields of characteristic 0. In fact, the proof of this result shows that F_0 is P-stable (the witness theorem of [4] holds for any field of characteristic zero since it can be expressed by a universal sentence in the language of fields; then the proof of Proposition 9 of [4] works as well for any extension of fields of characteristic 0). Using this result, Portier [32] has shown that the theory of differential fields of characteristic 0 is P-stable. Moreover, the proofs and results of [21] imply that the theory of fields is $\mathbb{P}$-stable and give an alternative proof of the P-stability of F_0. Note that it is unknown whether the algebraic closure of a finite field is P-stable. All the above results are not obvious. If one want to have an example of a P-stable theory with a simple proof (to construct a classroom exercise) one may consider the theory of nontrivial divisible abelian groups.

4 Real-Closed Fields

4.1 Background

For the notions of real-closed field, semi-algebraic set, definable set ...etc, we refer the reader to [7] and also to [13] for a more model-theoretic point of view.
In this paper R denotes a real-closed field. We need the following quantifier elimination result which can be found in Renegar [33] or Heintz, Roy and Solernó [15].

Fact 4.1 *Let $\phi(x)$ be a formula in the language of ordered rings, with a total of n variables and $l \leq n$ free variables (thus $x \in R^l$). Assume that ϕ is in prenex form with w blocks of quantifiers. Assume that the m atomic predicates in Φ are of the form $P\Delta 0$ where Δ is one of the "standard relations"*

$$>, \geq, =, \neq, \leq, <$$

and P is a polynomial of degree at most D, with integer coefficients of bit length at most L.
$\Phi(x)$ is equivalent to a quantifier-free formula of the form:

$$\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} (Q_{ij}(x)\Delta_{ij}0),$$

where Δ_{ij} is one of the 6 standard relations; I,J_i and the degrees of the polynomials Q_{ij} are bounded by $(mD)^{(O(n))^w}$. The coefficients of the Q_{ij} are integers of bit length at most $(L+l)(mD)^{(O(n))^w}$.
Moreover, the quantifier-free formula can be construct by a standard algorithm which works in parallel time $log(L)[n^w log(mD)]^{O(1)}$.

Note that the above result can be applied with formulae with parameters in R. Just replace the parameters by new variables, apply the elimination and replace the new variables by the parameters.
We recall an algorithmic version of Milnor-Petrovskii-Oleinik-Thom's theorem on sign conditions (a result which is used in the proof of the Fact above). Let $P_1, \ldots, P_m$ be polynomials of R in n variables. A consistent sign vector for $P_1, \ldots, P_m$ is a sequence $(\Delta_1, \ldots, \Delta_m)$ of $\{<, =, >\}$ such that there exists a a in R^n such that $P_i(a)\Delta_i 0$ for $i = 1, \ldots, m$. A priori, there are 3^m consistent sign vectors, however we have the following result (see [33, Proposition 4.1]).

Fact 4.2 *Let $P_1, \ldots, P_m$ be polynomials in n variables with coefficients in R of degrees at most D. There are at most $(mD)^{O(n)}$ consistent sign vectors for $P_1, \ldots, P_m$. These consistent sign vectors can be constructed from the coefficients of the P_i with $(mD)^{O(n)}$ operations in parallel time $[nlog(mD)]^{O(1)}$. If the coefficients of the P_i are integers of bit length at most L this construction can be accomplished in parallel time $(log(L))[nlog(mD)]^{O(1)}$.*

We consider R with the order topology and R^k with the product topology. Let X be a definable subset of R^k (by quantifier elimination this is the same thing as a semi-algebraic set and one can replace definable by semi-algebraic everywhere in what follows). We recall that X is said to be definably connected if X has no nonempty proper open-closed (in X) definable subset. X can be decomposed in a unique way in a finite number of definable definably connected subsets $Y_1, \ldots, Y_s$ such that $Y_j \cap Y_i = \emptyset$ for $i \neq j$ and such that the Y_i are open-closed in X. The Y_i are the definably connected component of X.
We need a result of Pillay on definable equivalence relation (see [27], Proposition 2.1 and its proof; do not make a confusion between cell and definably connected component).

Fact 4.3 *Let R be a real-closed field or any o-minimal structure. Let $\sim$ be a definable equivalence relation on R^k. Then, $\sim$ has a finite number of equivalence classes with a nonempty interior. Let $U_1, \ldots, U_s$ be the interior of these classes and let V be the set of $\beta \in R^k$ which are in an open subset of R^k contained in a class of $\sim$. V is definable, open in R^k and V is the union of the U_i. Moreover, let $V_1, \ldots, V_t$ be the decomposition of V in definable definably connected components. Then, the decomposition of V in the V_i is a refinement of the decomposition of V in the U_i.*

4.2 Elimination of Algebraic Parameters

In this section R can be any real-closed field. The results of this subsection are stated and proved in the uniform setting. However, the statements and the proofs extend in an obvious way to the nonuniform setting.

Lemma 4.4 *Assume that a problem $X \subseteq R^\infty$ can be recognized in sequential time $s(n)$ and in parallel time $d(n)$ by a machine over R with parameters in an algebraic extension $K[\alpha]$ of a subfield $K \leq R$. Then, X can be recognized in sequential time $c.s(n)$ and in parallel time $c.d(n)$, where c is a constant, by a machine using parameters from K only.*

Proof. Let M be the minimal polynomial of α over K, and d its degree. The idea is to simulate the original machine $\mathcal{M}$ (or the original sequence of circuits) by a machine $\mathcal{M}'$ (a new sequence of circuits) which computes modulo M. More precisely, any quantity computed by $\mathcal{M}$ can be represented as a polynomial in α (with coefficients in R) of degree at most $d-1$ (we assume without loss of generality that $\mathcal{M}$ does not perform divisions) and such a polynomial can be represented as a d-tuple. After a multiplication of two variables $P(\alpha)$ and $Q(\alpha)$, a Euclidean division by M can bring back the degree of the product PQ below d.
The crucial point is how to perform tests, which we assume without loss of generality to be of the form "$P(\alpha) \geq 0$?". Hence we need to determine when a vector $(a_0, \ldots, a_{d-1})$ is in the set $S = \{a \in R^d;\ \sum_{k=0}^{d-1} a_k \alpha^k \geq 0\}$. We claim that S is a semi-algebraic set, and can be defined by polynomial (in)equalities involving only

parameters from K. This will complete the proof since the test "$a \in S$?" can then be performed in constant (independent of the input size) time. Hence the new machine is slower than the original one by a constant factor only.
The proof of the claim is as follows. Assume that α is the l-th largest root of M. S is defined by the formula F(a):

$$\exists \alpha_1 \alpha_2 \cdots \alpha_l \ \ (\ \alpha_1 < \alpha_2 < \cdots < \alpha_l \wedge \bigwedge_{i=1}^{l} M(\alpha_i) = 0 \wedge \sum_{k=0}^{d-1} a_k \alpha_l^k \geq 0 \ ).$$

Since the parameters in F are from K only, there exists an equivalent quantifier-free formula with parameters from K as well. $\square$

Theorem 4.5 (Elimination of Algebraic Parameters) *Assume that a problem $X \subseteq R^{\infty}$ can be recognized in sequential time $s(n)$ and in parallel time $d(n)$ by a machine over R with parameters $(\alpha_1, \ldots, \alpha_k)$. X can be solved in sequential time $c.s(n)$ and in parallel time $c.d(n)$, where c is a constant, by a machine using $l \leq k$ algebraically independent parameters, where l is the transcendence degree of the field $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$.*

Proof. Assume for instance that $(\alpha_1, \ldots, \alpha_l)$ is a transcendence base of L. Taking $K = \mathbb{Q}[\alpha_1, \ldots, \alpha_{k-1}]$ in Lemma 4.4, we see that X can be recognized with parameters in K only. This process can be reiterated $k-1-l$ times. We conclude that A can be recognized by a machine with parameters in $\mathbb{Q}[\alpha_1, \ldots, \alpha_l]$. Elements in this field can be built in a finite number of steps from the algebraically independent parameters $\alpha_1, \ldots, \alpha_l$. The times conditions follow from the times conditions of Lemma 4.4. $\square$

The following lemma will play an important role in section 4.5.

Lemma 4.6 *Let $X \subseteq R^{\infty}$ be a problem in* $\mathrm{A}_R/\mathrm{const}$ *with a corresponding problem $Y \in \mathrm{A}_R$ solved in sequential time $s(n)$ and in parallel time $d(n)$. Then, $X \in \mathrm{A}_R^l/k$ with a corresponding problem $Z \in \mathrm{A}_R^l$ solved in sequential time $c_1.s(n+c_2)$ and in parallel time $c_1.d(n+c_2)$, where c_1 and c_2 are constants, and such that for all $n \geq 1$ the set S_n of parameters $\beta \in R^k$ satisfying*

$$\forall x \in R^{\leq n} \ [x \in X \Leftrightarrow \langle x, \beta \rangle \in Z]$$

has a nonempty interior.

Proof. By hypothesis there exists a sequence of quantifier-free formulae $(\phi_n(x, y, z))$ with $l(x) = n$, $l(y) = k_1$ and $l(z) = l_1$ and $\alpha \in R^{k_1}$ such that for all n, $\phi_n(x, y, \alpha)$ defines $Y \cap R^{n+k_1}$. Moreover, there exists a sequence (β_n) of R^{k_1} such that for all m and all $n \geq m$, $\phi_m(x, \beta_n, \alpha)$ defines $X \cap R^m$. Let R_1 be an $\aleph_1$-saturated elementary extension of R. The formula $\phi_n(x, \beta_n, \alpha)$ interpreted in R_1 defines $X_1 \cap R_1^n$, where X_1 is the extension of X to X_1. Moreover, by the proof of Lemma 3.8, X_1 is in A_{R_1}/const with corresponding problem Y_1 the extension of Y to R_1. Y_1 is solved in

R_1 by the machine which solves Y in R. By the proof of Proposition 3.7, there exists $\beta \in R_1^{k_1}$ such that X_1 is solved in R_1 with the machine that solves Y_1 and with the parameters $\langle \beta, \alpha \rangle$. Now we apply Theorem 4.5 over R: X_1 is solved in sequential time $c.s(n+k_1)$ and parallel time $c.d(n+k_1)$, where c is a constant, with parameters $\langle \beta', \alpha' \rangle$ such that $\alpha' \in R^k$, $\beta' \in R_1^l$ and the β_i' are algebraically independent over R. Now, by the proof of Lemma 3.8, X is in A_R^l/k with a corresponding problem $Z \in \mathrm{A}_R^l$ solved in sequential time $c.s(n+k_1+k)$ and parallel time $c.d(n+k_1+k)$. We denote by Z_1 the extension of Z to R_1.
For all n, β' is in the set S_n' of "suitable parameters" up to size n:

$$S_n' = \{y \in R_1^k;\ \forall x \in R_1^{\leq n}\ x \in X_1 \Leftrightarrow \langle x, y, \beta \rangle \in Z_1\}. \tag{3}$$

S_n' is definable with parameters in R only, using the formulae $\phi_m(x, \beta_n, \alpha)$. Moreover, the same formula define the S_n of the lemma's statement. We claim that S_n' has a nonempty interior. This can be expressed by a formula with parameters in R

$$\exists u \in R_1^k\, \exists v \in R_1^k\, \forall z \in R_1^k\ [(\bigwedge_{i=1}^{k} u_i < z_i < v_i) \Rightarrow (z \in S_n')]$$

where the condition $z \in S_n'$ can be replaced by a first-order formula using (3). Applying the transfer principle for real-closed fields to this formula, we conclude that the set S_n in the lemma's statement also has a non-empty interior.
The proof of the claim is as follows. By quantifier elimination, S_n' is a union of basic semi-algebraic sets $B_{n,i}$ defined by conditions of the form

$$p_1(y) > 0, \ldots, p_{r_{n,i}}(y) > 0, q_1(y) = 0, \ldots, q_{s_{n,i}}(y) = 0$$

where the p's and q's are polynomial with coefficients in R (because S_n' is definable with parameters in R only). Since $\beta' \in S_n'$ and the β_i' are algebraically independent over R, β' belongs to a $B_{n,i}$ with $s_{n,i} = 0$. By continuity the sign of $p_1, \ldots, p_{r_{n,i}}$ is constant in a neighborhood of β', hence a box is included in S_n'. $\square$

The results of this subsection can be also obtained for nondeterministic complexity classes and in fact are more easy. Indeed, assume for example that X is in NP_R with a nondeterministic machine $\mathcal{M}$ which uses a unique algebraic parameter α. Then, we have a formula $\theta(y)$ (that we may assume to be quantifier-free) without parameters which defines α. Then, we consider the machine which on an input $a \in R^\infty$ guesses a β and runs $\mathcal{M}$ with $\langle a, \beta \rangle$ if β satisfies $\theta(y)$. Such a machine shows that X is in NP_R without parameters.
One can also obtain generalization of all the above results for an o-minimal structure which admits (effective for the uniform level) elimination of quantifiers in a finite language (for such a structure there is a natural topology and a good notion of algebraicity and independence). However, in this general case we cannot obtain the time conditions since it is difficult to generalize the notion of minimal polynomial. However, in order to prove Lemma 4.4 one can use the method of the paragraph above with the elimination of quantifiers.

4.3 The Reals

This section gather results that are specific to the field $\mathbb{R}$ of real numbers (in the sense that they do not apply to all other real-closed fields). The following simple lemma will be useful. It is a straightforward consequence of the nested intervals property and of König's lemma on infinite trees.

Lemma 4.7 *Let $(E_n)_{n\geq 0}$ be a family of subsets of $[-1,1]$ satisfying the following properties for all $n \in \mathbb{N}$:*

(i) $E_n \neq \emptyset$.

(ii) $E_{n+1} \subseteq E_n$.

(iii) E_n *has a finite number of connected components.*

(iv) $\bigcap_{n\geq 0} E_n = \emptyset$.

Then there exists $N \in \mathbb{N}$, a sequence $(I_n)_{n\geq N}$ with I_n a connected component of E_n, $\alpha \in [-1,1]$, and a sequence $(b_n)_{n\geq 0}$ of points of $[-1,1]$ such that one of these two properties holds for all $n \geq N$:

1. $I_n =]\alpha, b_n[$ *or* $I_n =]\alpha, b_n]$.
2. $I_n =]b_n, \alpha[$ *or* $I_n = [b_n, \alpha[$.

Proof. By König's Lemma, it follows from (i), (ii) and (iii) that there exists a sequence $(I_n)_{n\geq 0}$ of intervals where $I_{n+1} \subseteq I_n$ and I_n is a connected component of E_n. Let α_n and β_n be the left and right endpoints of I_n. We claim that one of the sequences (α_n), (β_n) is ultimately constant. Otherwise one could extract a strictly increasing subsequence (α_{n_k}) and a strictly decreasing subsequence (β_{n_k}). This would contradict (iv).
If (α_n) is ultimately constant, I_n must be open in α_n by (iv) and thus property 1 holds. In the other case property 2 holds. $\Box$

The following result is the main result of this subsection.

Theorem 4.8 $\mathrm{P}^0_{\mathbb{R}}/1 = \mathrm{P}^1_{\mathbb{R}}$.

Proof. Let $X \in \mathrm{P}^0_{\mathbb{R}}/1$, and let $Y \in \mathrm{P}^0_{\mathbb{R}}$ be the corresponding problem and (α_n) be the corresponding sequence of $\mathbb{R}$. Let $\mathcal{M}$ be a parameter-free machine recognizing Y in polynomial time. For each n we have an equivalence relation $\sim_n$ on $\mathbb{R}$: $y \sim_n y'$ if and only if the following parameter-free formula is satisfied:

$$\forall x \in \mathbb{R}^{\leq n}\ \langle x, y\rangle \in Y \Leftrightarrow \langle x, y'\rangle \in Y. \tag{4}$$

Let S_n be the set of parameters $y \in \mathbb{R}$ such that $y \sim_n \alpha_n$. This set is definable since it is an equivalence class for the relation $\sim_n$ on $\mathbb{R}$ defined by (4). Hence the

sets $E_n = S_n \cap [-1, 1]$ satisfy hypothesis (iii) of Lemma 4.7. Hypothesis (ii) is also clearly satisfied. One can assume without loss of generality that $E_n \neq \emptyset$ for all $n \geq 0$. Indeed, if $E_n = \emptyset$ for $n \geq n_0$, instead of α_n we can use for $n \geq n_0$ the new parameter $\alpha'_n = 1/\alpha_n \in [-1, 1]$ (in this case, for all n, we first compute $\alpha_n = 1/\alpha'_n$ and then run $\mathcal{M}$). Therefore we assume in the remainder of this proof that (i) also holds.
If (iv) does not hold, let $\alpha \in \bigcap_{n \geq 0} E_n$: it follows from (1) that by "plugging" α into $\mathcal{M}$, we obtain a machine which recognizes X in polynomial time. Hence $X \in \mathrm{P}^1_{\mathbb{R}}$.
In the rest of the proof we consider the case where (iv) also holds. One can therefore apply Lemma 4.7. From now on we assume that property 1 holds (the other case is similar). Pick any $n \geq N$ and a rational point $\beta \in]\alpha, b_n[$. The following formula defines α:

$$\neg(y \sim_n \beta) \wedge (\forall z \; y < z < \beta \Rightarrow \beta \sim_n z).$$

Since this formula contains only rational parameters, α is an algebraic number. Let Q be its minimal polynomial. We now want to show that for each $n \geq N$, α_n can be replaced by a new parameter which needs not be "too close" to α. In order to do this, let us consider the set $J_n = \{\epsilon > 0;\ ]\alpha, \alpha + \epsilon] \subseteq E_n\}$. Note that $J_n =]0, b_n - \alpha[$ or $J_n =]0, b_n - \alpha]$. We would like to define J_n by a "small" formula with (small) integer parameters only.
If α is the i-th largest root of P, this algebraic number can be defined by a formula stating that $P(\alpha) = 0$ and that there are exactly $i - 1$ roots of P smaller than α. For any $\epsilon > 0$, $\epsilon \in J_n$ if:

$$\forall z \quad (\alpha < z < \alpha + \epsilon \Rightarrow z \sim_n \alpha + \epsilon). \tag{5}$$

Since Y is recognized in polynomial time by the parameter-free machine $\mathcal{M}$, the condition $\langle x, y\rangle \in Y$ can be expressed for $x \in \mathbb{R}^{\leq n}$ by a quantifier-free formula $\phi_n(\epsilon)$ with $exp(n^{O(1)})$ atomic predicates (we go through all possible computation paths of $\mathcal{M}$). The degree and bit length of the polynomials occurring in $\phi_n(\epsilon)$ are also at most $exp(n^{O(1)})$. Hence (5) can be translated into a formula $\Phi_n(\epsilon)$ with a bounded number of quantifier alternations. This formula satisfies the same size, degree, and bit-length bounds as $\phi_n(\epsilon)$. By Fact 4.1, $\Phi_n(\epsilon)$ is equivalent to a quantifier-free formula $\Psi_n(\epsilon)$ in which all polynomials have integer coefficients of bit length $\leq exp(n^{O(1)})$. By the well-known bound on polynomial roots, the smallest positive root r of any such polynomial must satisfy $\log\log\frac{1}{r} < n^{O(1)}$. We conclude that J_n contains an interval of the form $]0, r_n[$ where $\log\log\frac{1}{r_n} < n^{O(1)}$. A parameter-free machine can thus construct (by "repeated squaring") an element $\epsilon_n \in J_n$ in time $n^{O(1)}$. Then one can "plug" $\alpha + \epsilon_n$ in $\mathcal{M}$ in place of α_n. The resulting machine $\mathcal{M}'$ recognizes X in polynomial time with a single parameter: the algebraic number α (note that this parameter can be eliminated by Theorem 4.5). $\Box$

The proof of Theorem 4.8 (or Theorem 4.8 with a padding argument) also shows that if $X \in \mathrm{A}^0_{\mathbb{R}}/1$ with a corresponding problem $Y \in \mathrm{A}^0_{\mathbb{R}}$ solved in time $s(n)$, then $X \in \mathrm{A}^1_{\mathbb{R}}$

in time $q(s(n+1))$ where q is a polynomial. Moreover, the proof of Theorem 4.8 can be adapted to the polynomial hierarchy, for example we have $\mathrm{NP}^0_{\mathbb{R}}/1 = \mathrm{NP}^1_{\mathbb{R}}$. We do not know whether $\mathrm{P}^1_{\mathbb{R}}/1 \subseteq \mathrm{P}_{\mathbb{R}}$, but we have the following result.

Proposition 4.9 *If $X \in \mathrm{P}^l_{\mathbb{R}}/1$, then X is in Σ_2 over $\mathbb{R}$.*

Proof. Let $X \in \mathrm{P}^l_{\mathbb{R}}/1$ and let $Y \in \mathrm{P}^l_{\mathbb{R}}$ be the corresponding problem with corresponding sequence (α_n) of parameters in $\mathbb{R}$. As in the proof of Theorem 4.8, we consider the sets S_n of "suitable values" for α_n. More precisely, $\beta \in S_n$ if and only if

$$\forall x \in \mathbb{R}^{\leq n} \; [x \in X \Leftrightarrow \langle x, \beta \rangle \in Y].$$

As in the proof of Theorem 4.8, we assume without loss of generality that $E_n = S_n \cap [-1,1] \neq \emptyset$ for all $n \in \mathbb{N}$. If $\bigcap_{n \geq 0} E_n \neq \emptyset$ then $X \in \mathrm{P}^{l+1}_{\mathbb{R}}$. Therefore in the rest of the proof we consider the case where $\bigcap_{n \geq 0} E_n \neq \emptyset$.
Assume for instance that we are in case 1 of Lemma 4.7. For any $x \in \mathbb{R}^{\leq n}$ with $n \geq N$, $x \in X$ if and only if

$$\exists \epsilon \; \forall \epsilon' \; \langle x, \epsilon, \epsilon' \rangle \in X'$$

where $X' \in \mathrm{P}^{l+1}_{\mathbb{R}}$ is defined by

$$\epsilon > 0 \wedge [0 < \epsilon' < \epsilon \Rightarrow \langle x, \alpha + \epsilon') \rangle \in Y].$$

It follows that X is Σ_2 over $\mathbb{R}$. $\Box$

The above result shows that a negative answer to the question $\mathrm{P}^1_{\mathbb{R}}/1 \subseteq ?\ \mathrm{P}_{\mathbb{R}}$ would have dramatic consequences. On the other hand, it seems to us that there is not a lot of hope to prove that $\mathrm{P}^1_{\mathbb{R}}/1 \subseteq \mathrm{P}_{\mathbb{R}}$. Let us explain why. A circuit $C(x_1, \ldots, x_n)$ over $\mathbb{R}$ is said to be arithmetical if it has one output gate and no test gates (such a circuit computes a polynomial function). Let $\mathbb{R} \leq R$ be a nontrivial ordered extension of $\mathbb{R}$ and let Ω be a positive element of R infinitely large over $\mathbb{R}$. For a nonalgebraic element a of $\mathbb{R}$ we consider the set W_a of parameter-free arithmetical circuits $C(x,y)$ with two inputs such that $C(\Omega, a) > 0$. The set W_a can be viewed as a boolean problem of $\mathbb{R}$ and it is easy to see that $W_a \in \mathrm{P}^1_{\mathbb{R}}/1$. Now we ask: is W_a in $\mathrm{P}_{\mathbb{R}}$ for all (nonalgebraic) elements a of $\mathbb{R}$?
To conclude this subsection we show that $\mathrm{A}_{\mathbb{R}}/\mathrm{const} = \mathrm{A}_{\mathbb{R}}$. This result will be precised (times conditions) and proved, in the nonuniform setting, for every real-closed field.

Theorem 4.10 *Any problem in $\mathrm{A}_{\mathbb{R}}/\mathrm{const}$ is algorithmic over $\mathbb{R}$ in bounded time.*

Proof. Let $X \in \mathrm{A}_{\mathbb{R}}/\mathrm{const}$. By Lemma 4.6, we may assume that $X \in \mathrm{A}^l_{\mathbb{R}}/k$ with a corresponding problem $Y \in \mathrm{A}^l_{\mathbb{R}}$ such that the sets S_n defined as in Lemma 4.6 have a nonempty interior. Thus, for all n, S_n contains a rational point $(c_{n1}, \ldots, c_{nk})$. We obtain a $\mathbb{N} \times k$ matrix with columns $c_1, \ldots, c_k$. In order to recognize X with a real machine $\mathcal{M}$, we just have to encode each column vector in a element of $\mathbb{R}$: we encode c_i in the digits of a single real number c'_i. On an input in $\mathbb{R}^n$, $\mathcal{M}$ can read the digits of c'_i and retrieve the appropriate parameter c_{ni}. Therefore $\mathcal{M}$ can recognize X in bounded time (by definition of the S_n). $\square$

The proof of the above result shows that if R is a real-closed field contained in $\mathbb{R}$ then $\mathbb{A}_R/\text{const} = \mathbb{A}_R$. Using a different method, it is also possible to obtain a more precise result concerning the number of parameters:

Theorem 4.11 *$\mathbb{A}_R^0/k = \mathbb{A}_R^k$ for any real-closed field R contained in $\mathbb{R}$ and any integer k.*

The proof relies on a lemma of independent interest.

Lemma 4.12 *Let $R \subseteq \mathbb{R}$ be a real-closed field. Let $(C_n)_{n\geq 0}$ be a sequence of nested ($C_{n+1} \subseteq C_n$) nonempty definable subsets of R^k.*

(i) There exists a tuple a of elements of R and a family of formulas $G_n(a, .)$ with parameter a such that G_n defines a unique point $c_n \in R^k$, and $c_n \in C_n$.

(ii) Let $F_n(a_n, .)$ be a defining formula for C_n. There exists n_0 such that (i) holds with $a = a_p$ for any $p \geq n_0$.

Proof. By induction on k. For $k = 1$, each C_n is a finite union of points and intervals. If the C_n's are all infinite they must contain rational points, which are definable without parameters. Otherwise, let n_0 be such that C_{n_0} is finite. For $p \geq n_0$ and $n \geq p$, any point in C_n is in C_p, and any point of C_p is definable over a_p (it is either the largest element of C_p, or the second largest, or the 3rd, etc).
Assume now that the result holds in dimension $k-1$. Let P_n be the projection of C_n on R^{k-1}, and $I_n \subseteq P_n$ the set of points with infinitely many preimages in R^k. The P_n's are nested, nonempty, and definable with the same parameters as C_n. I_n is also definable over a_n: a set of preimages is infinite iff it contains a nonempty open interval. One can thus apply the induction hypothesis to the I_n's if these sets are all nonempty (they are nested as required). Then each defined point $c_n \in I_n$ can be completed by a rational point q_n such that $\langle c_n, q_n\rangle \in C_n$. Assume now that $I_n = \emptyset$ for $n \geq n_0$. In this case we apply the induction hypothesis to (P_n): there exists a family of formulas $G_n(a, .)$ defining a unique point $c_n \in P_n$. Moreover, there exists n_1 such that one can take $a = a_p$ for any $p \geq n_1$. Now let $n_2 = \max(n_0, n_1)$: For $p \geq n_2$ and $n \geq p$, $G_n(a_p, .)$ defines a unique point $c_n \in P_n$. A preimage of c_n in C_n is either the largest element of C_p above c_n, or the second largest, or the 3rd, etc. Hence one can define a point $d_n \in C_n$ above c_n by a formula with parameter a_p (note that there can be several occurrences of a_p in this formula: those that help define c_n, and those that help define a point above c_n). $\square$

The proof of (i) by induction on k was suggested by Bruno Poizat.

Proof of Theorem 4.11. Let $X \in \mathbb{A}^0_R/k$ and $Y \in \mathbb{A}^0_R$ the corresponding problem. The sets C_n of parameters $\alpha_n \in R^k$ such that (1) holds satisfy the hypotheses of Lemma 4.12, and each of them is definable with k parameters (recall from the proof of Theorem 4.8 that C_n is an equivalence class of an equivalence relation on R^k definable without parameters). Hence for any $x \in R^n$,

$$x \in X \Leftrightarrow \exists c \in R^k \; G_n(a,c) \wedge \langle x,c \rangle \in Y$$

where a and G_n are given by Lemma 4.12. The result follows by quantifier elimination. $\Box$

For $\mathbb{R}$ and uniform algorithms, one can also obtain the best possible bound on the number of parameters.

Theorem 4.13 *For any $k \geq 0$, $\mathrm{A}^0_{\mathbb{R}}/k = \mathrm{A}^k_{\mathbb{R}}$.*

Proof. Let $X \in \mathrm{A}^0_{\mathbb{R}}/k$. By Theorem 4.11, $X \in \mathrm{A}^k_{\mathbb{R}}$. A sequence of formulas $F_n(a,.)$ with $a \in R^k$ defining $X \cap \mathbb{R}^n$ can be encoded in the digits of a single real constant. Hence we obtain $X \in \mathrm{A}^{k+1}_{\mathbb{R}}$. We can obtain $X \in \mathrm{A}^k_{\mathbb{R}}$ if one of the parameters $a_1, \ldots, a_k$ turns out to be rational (in this case we effectively need $k-1$ parameters only). Let C_n be the set of parameters $\alpha_n \in \mathbb{R}^k$ such that (1) holds. Recall from the proof of Theorem 4.11 that a can be any element of C_n if n is large enough. Then there are two cases. If the C_n's are all infinite, by Lemma 4.14 below there exists a point with a rational component in C_n, and we are done. If C_n is finite for n large enough, then $\bigcap_{n \geq 0} C_n \neq \emptyset$ and by picking a point in this intersection we obtain directly $A \in \mathrm{A}^k_{\mathbb{R}}$. $\Box$

Lemma 4.14 *Let $E \subseteq \mathbb{R}^k$ be a definable set. If this set is infinite, it contains a point with a rational component.*

Proof. By induction on k. For $k=1$ the result is clear since E is a finite union of points and intervals. Assume now that the result holds in dimension $k-1$, and let E' be the projection of $E \subseteq \mathbb{R}^k$ on $\mathbb{R}^{k-1}$. If E' is infinite it must contain a point with a rational component by induction hypothesis, and we are done. Otherwise since E is infinite, E' must contain a point x_0 with infinitely many preimages in E. In this case, we can apply the $k=1$ result to the set of preimages of x_0. $\Box$

4.4 The Class DEPTH for Real-Closed Fields

A quantifier-free formula of the form

$$\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} (Q_{ij} \Delta_{ij} 0),$$

is said to be in (disjunctive-conjunctive) normal form (the Δ_{ij} are one of the 6 standard relations). We say that the above formula is of size $\leq s$ if the degrees of the polynomials Q_{ij}, I,J_i and the bit length of the coefficients of the Q_{ij} are bounded by s. We need the following characterization of the class DEPTH for real-closed fields. The proof depends on Fact 4.2 on the number of consistent sign conditions (this is not the first application of this result in complexity theory over the reals).

Theorem 4.15 *Let d be a function from $\mathbb{N}$ into $\mathbb{N}^*$ such that for all n, $d(n) \geq n$. Let X be a problem in* $\mathrm{DEPTH}_R(d(n))$. *There exists a sequence of quantifier-free formulae $(\phi_n(x_1, \ldots, x_n, y_1, \ldots, y_k))_{n\geq 0}$ in normal form and $\alpha \in R^k$ such that $(\phi_n(x, \alpha))_{n\geq 0}$ solves X and such that the ϕ_n are of size $\leq exp(q(d(n)))$ where q is a polynomial. Moreover, if X is in* $\mathrm{UDEPTH}_R(d(n))$ *(respectively, in* $\mathbb{U}\mathrm{DEPTH}_R(d(n))$*) then the sequences (ϕ_n) is* $\mathrm{SPACE}(q(d(n)))$ *uniform (respectively,* $\mathrm{SPACE}(q(d(n)))$ *uniform with boolean advice of size $q(d(n))$).*
Moreover, the converses hold (within a polynomial).

Proof. The "converse" of the Theorem is easy and the proof is left to the reader. For the first part, it suffices to prove that there is a polynomial q such that if $C(x_1, \ldots, x_n)$ is a parameter-free circuit in the sense of R of depth d, then there exists a quantifier-free formula $\phi(x)$ in normal form of size $\leq q(d)$ equivalent to $C(x)$ and that moreover formula $\phi(x)$ can be constructed from $C(x)$ by a standard algorithm which works in parallel time polynomial in d.
First, we concentrate our attention on the existence of a ϕ with good bounds. Note first that we may assume that the tests of C are of the form $P(\bar{x}) > 0$ (where P is a polynomial which depends on the answers to the previous tests). Note also that a parameter-free circuit of depth e without tests and with one output gate computes a polynomial of degree $\leq exp(e)$ and with coefficients of bit length $\leq exp(e)$ (we say that the polynomial is of size $\leq exp(e)$). Let G be the set of test gates of C. The height of a gate $g \in G$ is the maximal number of gates in G in a path from an input gate to g (including g). Let s be the maximum of the height of a gate in G. Then, obviously $1 \leq s \leq d$. We denote by G_i the set of gates of height i; G_s is constituted by the output gate and the G_i are of cardinal $m_i \leq exp(d)$. Set $G_1 = \{g_{1,1}, \ldots, g_{m_1,1}\}$: at gate $g_{i,1}$, C makes a test of the form $P_{i,1}(x) > 0$ where $P_{i,1}(x)$ is a fixed polynomial of size $\leq exp(d)$. If $s = 1$, then $m_1 = 1$ and we can take for ϕ the formula $P_{1,1}(x) > 0$. Thus, we assume that $s \geq 2$. Let $G_2 = \{g_{1,2}, \ldots, g_{m_2,2}\}$. At gate $g_{i,2}$, C makes a test of the form $P_{i,2}(x) > 0$ where $P_{i,2}(x)$ is a polynomial of size $\leq exp(d)$. But the form of $P_{i,2}$ depends on the answers of the tests performed at the gates of height 1. More precisely, for each vector of consistent sign conditions $\Delta = (\Delta_1, \ldots, \Delta_{m_1})$ for $P_{1,1}, \ldots, P_{m_1,1}$, there exists a fixed polynomial $P_{i,2}^{\Delta}$ such that the test performed by C at gate $g_{i,2}$ is $P_{i,2}^{\Delta} > 0$ for the inputs which give to the $P_{i,1}$ the sign determined by Δ. We denote by CSC_1 the set of vectors of consistent sign conditions for $P_{1,1}, \ldots, P_{m_1,1}$; by Fact 4.2, CSC_1 is of cardinality $\leq (exp(d)exp(d))^{cn} = exp(2cnd)$ (where c is a universal constant). Then,

if $s = 2$ we consider the formula

$$\bigwedge_{\Delta \in CSC_1} [(\wedge_{i=1}^{m_1} P_{i,1}(x)\Delta_i 0) \Rightarrow (P_{1,2}^{\Delta}(x) > 0)]$$

which is equivalent to $C(x)$ and which contains at most $exp(3cnd)$ polynomials. If $s \geq 3$ we proceed as above with the gates of height 3 and if $s = 3$, $C(x)$ is equivalent to a formula of the form

$$\bigwedge_{\Delta_1 \in SC_1} [(\wedge_{i=1}^{m_1} P_{i,1}(x)\Delta_{i,1} 0) \Rightarrow (\bigwedge_{\Delta_2 \in CSC^{\Delta_1}} [(\wedge_{i=1}^{m_2} P_{i,2}^{\Delta_1}(x)\Delta_{i,2} 0) \Rightarrow (P_{1,3}^{\Delta_1,\Delta_2}(x) > 0)])]$$

where CSC^{Δ_1} is a set of consistent sign conditions which depends on Δ_1 of cardinality $\leq exp(2cnd)$, and we see that there are at most $exp(4cnd)$ distinct polynomials in this formula. We continue this process and at the end (which is attained at most after d steps) we obtain a quantifier-free formula $\psi(x)$ equivalent to $C(x)$ of the form

$$\bigwedge[(\wedge\ ) \Rightarrow (\bigwedge[(\wedge\ ) \Rightarrow (\bigwedge[(\wedge\ ) \Rightarrow \ldots \Rightarrow (P_{1,s}^{\Delta_1,\ldots,\Delta_s}(x) > 0)]\ldots)]$$

which contains at most $exp(2cnd^3)$ distinct polynomials of size $\leq exp(d)$. Let $Q_1, \ldots, Q_r$ be these polynomials. If Δ is a vector of length r of $\{<, =, >\}$ then we denote by θ_Δ the formula $\wedge_{i=1}^{r} Q_i \Delta_i 0$. Then, by Fact 4.2, there are at most $(exp(2cnd^3)exp(d))^n = exp(2cn^2d^3 + nd)$ Δ's such that θ_Δ defines a nonempty subset of R^n. Moreover, ψ is equivalent to a disjunction of some of the formulae θ_Δ. Such a disjunction provides a formula $\phi(x)$ with the required bounds. More precisely, for any Δ we have that either $R \models \forall x(\theta_\Delta(x) \Rightarrow \psi(x))$ or $R \models \forall x \neg(\theta_\Delta(x) \wedge \psi(x))$ and this can be tested in a boolean fashion (by replacing the basic subformulae $P(x)\Delta' 0$ of $\psi(x)$ by 1 if $P(x)\Delta' 0$ is consistent with $\wedge_{i=1}^{r} Q_i \Delta_i 0$ and by 0 otherwise, and then evaluating this boolean instance of ψ).
Now we have to prove the uniformity of the above procedure. First, we note that by Fact 4.2 we can compute the possible vectors of consistent sign conditions of a family $P_1, \ldots, P_m$ of polynomials in n variables of degree $\leq D$ and with coefficient of bit length L in parallel time $log(L)(nlog(mD))^c$ where c is a universal constant. Thus, in the above context such a computation takes time at most d^{3c} in parallel. Note also that the construction of ϕ from ψ can be done in parallel time polynomial in d using the (parallelizable) procedure described in the paragraph above and the fast algorithm for the computation of consistent sign conditions. The construction of ψ is "parallelizable" in the sense that it can be decomposed in at most d steps. At one step we have to compute some sign conditions and this can be done rapidly and we have to extract some polynomials from C. Essentially, we need an algorithm which given a circuit C' of depth $\leq d$ without tests and with one output gate computes the polynomial of size $\leq exp(d)$ that it defines in parallel time polynomial in d. Since it is easy to describe such an algorithm the proof of the theorem is completed. $\Box$

4.5 The Class A/const for Real-Closed Fields

As mentioned previously, if R is a countable real-closed field there are problems in $\mathrm{P}^0_R/1$ which are not A_R (see Proposition 3.15). The following proposition gives additional information.

Proposition 4.16 $\mathbb{P}_R \subseteq \mathrm{P}_R/1$.

Proof (sketch). Let $X \in \mathbb{P}_R$ be solved by a sequence of circuits $(C_n(x,\beta))$. We can encode in the digits (in radix 2) of a rational $\alpha_n \in]0,1[$ the circuits $C_0(y), C_1(x_1,y), \ldots, \mathcal{C}_n(x,y)$. Then, we consider the following $\mathrm{P}_R/1$ algorithm: on an input $a \in R^n$ extract (using $+$, $-$ and $<$) the n^{th} circuit encoded in α_n and (using a universal machine) applies it to $\langle a, \beta\rangle$. $\square$

Note that the same argument shows that, for example, $\mathbb{P}\mathrm{AR}_R \subseteq \mathrm{PAR}_R/1$ and $\mathbb{A}_R \subseteq \mathrm{A}_R/1$.
If we want to study A_R/const for an arbitrary real-closed field we need to work at the nonuniform level. Do not forget that if R contains the reals, then most of the nonuniform classes are in fact uniform : $\mathbb{P}_R = \mathrm{P}_R$, $\mathbb{PH}_R = \mathrm{PH}_R$, $\mathbb{P}\mathrm{AR}_R = \mathrm{PAR}_R$, $\mathrm{PAT}_R = \mathbb{PAT}_R$, $\mathbb{EXP}_R = \mathrm{EXP}_R$ and $\mathrm{PEXP}_R = \mathbb{P}\mathrm{EXP}_R$ (however, $\mathbb{P}\mathrm{AR}_R \subset \mathbb{PAR}$ and $\mathbb{P}\mathrm{EXP}_R \subset \mathbb{PEXP}_R$ for every real-closed field). Thus, all the results that follow have a uniform version in the special case where R contains the reals (we shall not mention them explicitly).
Here, the main open question is $\mathbb{P}_{\mathbb{R}_{alg}}/\mathrm{const} =? \, \mathbb{P}_{\mathbb{R}_{alg}}$ where $\mathbb{R}_{alg}$ is the ordered field of real algebraic numbers. It seems that this question is difficult. On the one hand, we shall prove that $\mathbb{P}_R/\mathrm{const} \subseteq \mathbb{P}\mathrm{AR}_R$ (and it is not known whether $\mathbb{P}_R \neq \mathbb{P}\mathrm{AR}_R$). On the other hand, if $a \in \mathbb{R}\backslash\mathbb{R}_{alg}$ we can consider the set W_a of parameter-free arithmetical circuits $C(x)$ in one free-variable such that $C(a) > 0$ (compare with the problems that follow the proof of Proposition 4.9). It is easy to see that the problems W_a are in $\mathrm{P}^0_{\mathbb{R}_{alg}}/1$, but it seems very difficult to show that all these problems are $\mathbb{P}_{\mathbb{R}_{alg}}$ (one may conjecture that there are some a's such that W_a is not $\mathbb{P}_{\mathbb{R}_{alg}}$).
We need to introduce a new "complexity class". Let $l \geq 0$ and $k \geq 1$. We say that a problem X of R is in $\mathbb{A}^l_R/^*k$ if there exists a problem Y (the corresponding problem) in $\mathbb{A}^l_R$ and a sequence $(\beta_n)_{\geq 0}$ of R^k such that

(i) for all $n \geq 0$, for all $a \in R^n$, $a \in X$ iff $\langle a, \beta_n\rangle \in Y$ and

(ii) for all $n \geq 0$ the set

$$S^*_n = \{u \in R^k \mid \forall x \in R^n \ (\ \langle x, \beta_n\rangle \in Y \text{ iff } \langle x, u\rangle \in Y\ )\,\}$$

has a nonempty interior.

Moreover, we set $\mathbb{A}^l_R/^*0 = \mathbb{A}^l_R$ and $\mathbb{A}_R/^*\mathrm{const} = \bigcup_{l,k} \mathbb{A}^l_R/^*k$. If $\mathcal{C}$ is a complexity class such as $\mathbb{P}$, $\mathbb{P}\mathrm{AR}$,..., we can define $\mathcal{C}^l_R/^*k$ by imposing $Y \in \mathcal{C}$.

Proposition 4.17 $\mathbb{A}_R/\text{const} \subseteq \mathbb{A}_R/{}^*\text{const}$ *"without" any loss of time and uniformity (time is multiplied by a constant).*

Proof. The proposition is an immediate consequence of Lemma 4.6 since the sets S_n of Lemma 4.6 are contained in the sets S_n^*. $\square$

We will see that $\mathbb{A}_R/{}^*\text{const} \subseteq \mathbb{A}_R$ (this is obvious if R is archimedean), thus $\mathbb{A}_R/\text{const} = \mathbb{A}_R/{}^*\text{const}$. However, we do not know if $\mathbb{P}_R/\text{const} = \mathbb{P}_R/{}^*\text{const}$ neither if $\mathrm{P}^0_{\mathbb{R}}/{}^*1 \subseteq \mathrm{P}_{\mathbb{R}}$. We can answer these questions for parallel time.

Theorem 4.18 $\mathbb{PAR}_R/\text{const} = \mathbb{PAR}_R/{}^*\text{const} = \mathbb{PAR}_R$ *and* $\mathbb{P}\text{AR}_R/\text{const} = \mathbb{P}\text{AR}_R/{}^*\text{const} = \mathbb{P}\text{AR}_R$.

Proof. By the above proposition we just have to prove that $\mathbb{PAR}_R/{}^*\text{const} \subseteq \mathbb{PAR}_R$ and $\mathbb{P}\text{AR}_R/{}^*\text{const} \subseteq \mathbb{P}\text{AR}_R$. First we concentrate ourselves on the first inclusion. Let X be a problem in $\mathbb{PAR}_R/{}^*\text{const}$, then X is in $\mathbb{PAR}^l_R/{}^*k$ for some integers k, l and we may assume that $k \geq 1$. The hypothesis and Theorem 4.15 imply that (we may assume that) there exists a sequence of quantifier-free formulae

$$(\phi_n(x_1, \ldots, x_n, y_1, \ldots, y_k, z_1, \ldots, z_l))_{n \geq 1}$$

of size $exp(n^{O(1)})$, an $\alpha \in R^l$ and a sequence $(\beta_n)_{\geq 0}$ of R^k such that

(i) for all $n \geq 0$, for all $x \in R^n$, $x \in X$ iff $R \models \phi_n(x, \beta_n, \alpha)$ and

(ii) for all $n \geq 0$ the set

$$S_n^* = \{y \in R^k \mid \forall x \in R^n \ (\ \phi_n(x, \beta_n, \alpha) \text{ iff } \phi_n(x, y, \alpha)\ )\ \}$$

has a nonempty interior.

Let $\sim_n$ be the equivalence relation on R^k defined by :

$$y \sim_n y' \quad \text{iff} \quad \forall a \in R^n \ (\ \phi_n(a, y, \alpha) \Leftrightarrow \phi_n(a, y', \alpha)\ ).$$

The relation $\sim_n$ is α-definable and S_n^* is a class of $\sim_n$ with nonempty interior. By Fact 4.3, $\sim_n$ has a finite number of classes with nonempty interior. Let $U_{1,n}, \ldots, U_{s_n,n}$ be the interior of these classes. We may assume that the interior of S_n^* is $U_{1,n}$. We consider the set V_n of the $y \in R^k$ such that

$$\exists u \in R^k\, \exists v \in R^k\, [\wedge_{i=1}^k u_i < y_i < v_i \wedge \forall y' \in R^k\, ((\wedge_{i=1}^k u_i < y'_i < v_i) \Rightarrow (y \sim_n y'))].$$

V_n is the set of $y \in R^k$ such that there exists an open set U of R^k such that $y \in U$ and U is contained in a class of $\sim_n$. Moreover, V_n is α-definable and V_n is the union of the $U_{i,n}$.
The idea is to "construct" a point in $\pi U_{1,n}$, the projection of $U_{1,n}$ onto the last coordinate. More precisely, we are going to construct a quantifier-free formula $\theta_n(y_k, \alpha)$

which is satisfied by a unique point β'_n of R which is in $\pi U_{1,n}$. Moreover, Fact 4.1 allows us to show that the size of $\theta_n(y_k,\alpha)$ is $\leq exp(n^{O(1)})$. Assume that such a sequence of formulae has been constructed. Then, X is solved by the sequence of formulae $(\exists y_k\ \theta_n(y_k,\alpha)\wedge\psi_n(x,\beta'_{1,n},\ldots,\beta'_{k-1,n},y_k,\alpha))_{n\geq 0}$ where the $(k-1)$-tuples $(\beta'_{1,n},\ldots,\beta'_{k-1,n})$ are such that $(\beta'_{1,n},\ldots,\beta'_{k-1,n},\beta'_n)$ is in $U_{1,n}$. Then, we apply Fact 4.1 to the above sequence of formulae and we obtain a sequence of quantifier-free formulae $(\psi_n(x,y_1,\ldots,y_{k-1},z))_{n\geq 0}$ in normal form and of size $\leq exp(n^{O(1)})$. Note that for all n the set

$$\{y\in R^{k-1}\,|\,\forall x\in R^n\ (\ \psi_n(x,\beta'_{1,n},\ldots,\beta'_{k-1,n},\alpha)\text{ iff }\psi_n(x,y,\alpha)\ )\}$$

has nonempty interior. Then, by Theorem 4.15, the problem defined by $(\psi_n(x,y_1,\ldots,y_{k-1},\alpha))_{n\geq 0}$ is in $\mathbb{PAR}^l_R$ and this problem shows that X is in $\mathbb{PAR}^l_R/^*(k-1)$. Repeating the above argument, we obtain that X is in $\mathbb{PAR}^l_R$ (k is fixed !). Note that we need to work with the class $\mathbb{PAR}_R/^*$const. Indeed, if X is in $\mathbb{PAR}^l_R/k$ the above argument does not imply that X is in $\mathbb{PAR}^l_R/(k-1)$ (even if the S_n defined in Lemma 4.6 have nonempty interior and the equivalence relations $\sim_n$ are adequately defined) because in general the above $\beta'_{1,n},\ldots,\beta'_{k-1,n}$ works only for inputs of size n.
Let us construct a formula θ_n with the announced properties. We consider the set B_n of elements $e\in R$ such that e is a boundary point of the projection onto the last coordinate of one of the $U_{i,n}$. Note that B_n is the set of elements $e\in R$ such that there exists $y\in V_n$ such that e is a boundary point of the projection onto the last coordinate of the set of elements of V_n $\sim_n$-equivalent to y. Thus B_n is a definable subset of R and since we have a finite number of $U_{i,n}$, B_n is finite. Now we consider the set T_n of the $y_k\in R$ such that

$$\exists e_1,e_2\in B_n\ (y_k=0\ \vee\ y_k=e_1+1\ \vee\ y_k=e_1-1\ \vee\ 2y_k=e_1+e_2).$$

Since B_n is definable and finite, T_n is definable and finite. Moreover, T_n contains at least one point of $\pi U_{1,n}$. Now following the construction of the formula which defines T_n we see that this formula has size $exp(n^{O(1)})$ and that its only parameters are the α. Moreover, this formula has a bounded number of quantifier alternations. Thus, by Fact 4.1, this formula is equivalent to a quantifier-free formula of the form

$$\bigvee_{i=1}^{I}\bigwedge_{j=1}^{J_i}(Q_{ij}(y_k,\alpha)\Delta_{ij}0),$$

and of size $\leq exp(n^{O(1)})$. Since this formula defines a finite set, there exists i and j such that a point β'_k of $\pi U_{1,n}$ is a zero of $Q_{ij}(y_k,\alpha)$. We denote by P_n such a polynomial. Let D be the degree of P_n. We denote by δ_n the vector $(\Delta_i)_{i=1}^{D-1}$ of $\{<,=,>\}$ such that for $i=1,\ldots,D-1$ we have $P_n^{(i)}(\beta'_k,\alpha)\Delta_i 0$. Then, we take for θ_n the formula $(P_n(y_k,\alpha)=0)\wedge\wedge_{i=1}^{D-1}(P_n^{(i)}(y_k,\alpha)\Delta_i 0)$. By construction, a point of $\pi U_{1,n}$ satisfies this formula and by Thom's lemma it is the only one.

Moreover, θ_n is clearly of size $\leq exp(n^{O(1)})$. This completes the proof of the inclusion $\mathbb{PAR}_R/^*\text{const} \subseteq \mathbb{PAR}_R$.
For the inclusion $\mathbb{P}\text{AR}_R/^*\text{const} \subseteq \mathbb{P}\text{AR}_R$ we need to show that ψ_n can be constructed from ϕ_n in parallel polynomial time with the help of a boolean advice of polynomial size. Fact 4.1 overcomes almost all difficulties. However, for the construction of θ_n we need to know which polynomial Q_{ij} to choose for P_n and then we need to "compute" the vector of sign conditions δ_n. At this point we need a boolean advice (especially for δ_n; one can overcome this difficulty for the P_n). By Fact 4.1, the list of the Q_{ij} can be constructed in parallel polynomial time. There are at most an exponential number of Q_{ij} and a good P_n is, say, the s^{th}. Thus we have a boolean advice of polynomial size which tell us where there is a good P_n. For δ_n we proceed in the same way. By Fact 4.2, we can compute the vectors of consistent sign conditions of $(P_n^{(1)}, \ldots, P_n^{(D-1)})$ in parallel polynomial time and there are at most an exponential number of such vectors. Again a boolean advice of polynomial size can tell to us which one we must take for δ_n. $\square$

Of course, Theorem 4.18 implies that $\mathbb{P}_R \subseteq \mathbb{P}\text{AR}_R$. Also, by a simple padding argument (or using the proof of Theorem 4.18) we obtain that $\mathbb{A}_R/\text{const} = \mathbb{A}_R/^*\text{const} = \mathbb{A}_R$ and that $\mathbb{EXP}_R/\text{const} \subseteq \mathbb{P}\text{EXP}_R/\text{const} = \mathbb{P}\text{EXP}_R/^*\text{const} = \mathbb{P}\text{EXP}_R$ and $\mathbb{PEXP}_R/\text{const} = \mathbb{PEXP}_R/^*\text{const} = \mathbb{PEXP}_R$. Since Lemma 4.6 is true for nondeterministic complexity classes and since $\mathbb{PH}_R \subseteq \mathbb{P}\text{AR}_R$ and $\mathbb{PAT}_R \subseteq \mathbb{P}\text{EXP}_R$ we obtain $\mathbb{PH}_R/\text{const} \subseteq \mathbb{PH}_R/^*\text{const} \subseteq \mathbb{P}\text{AR}_R$ and $\mathbb{PAT}_R/\text{const} \subseteq \mathbb{PAT}_R/^*\text{const} \subseteq \mathbb{P}\text{EXP}_R$. Note that we can apply Theorem 4.18 with Theorem 4.5 and Proposition 3.10 to obtain results of "elimination of parameters". For example, we have that if a problem is $\mathbb{P}\text{AR}_R$ and $\emptyset$-definable, then it is $\mathbb{P}\text{AR}_R$ without parameters.
We can also obtain a result of a general nature.

Proposition 4.19 *Let M be an o-minimal structure which admits elimination of quantifiers. Then,* $\mathbb{A}_M/\text{const} = \mathbb{A}_M/^*\text{const} = \mathbb{A}_M$.

Proof. Since Lemma 4.6 is true for M (but without time conditions) we have $\mathbb{A}_M/\text{const} \subseteq \mathbb{A}_M/^*\text{const}$ (see the end of section 4.2). To prove that $\mathbb{A}_M/^*\text{const} \subseteq \mathbb{A}_M$ we begin as in the proof of Theorem 4.18. But at the end of the second paragraph we decompose V_n in its definable definably connected components: $V_{1,n}, \ldots, V_{t_n,n}$. By the second part of Lemma 4.3 we may assume that $V_{1,n} \subseteq U_{1,n}$. Since V_n is α-definable, $V_{1,n}$ is definable by a formula $\theta_n(y, \alpha)$ with parameters α only (see [17]). Thus, for all n and all $a \in R^n$, $a \in X$ iff $\exists y\ \theta_n(y, \alpha) \wedge C_n(a, y, \alpha)$. Thus, by elimination of quantifiers $X \in \mathbb{A}_M$. $\square$

We conclude this section with some applications of Theorem 4.18. The point is that some questions concerning the reals $\mathbb{R}$ or an arbitrary real-closed field can be difficult to answer (due to the presence of parameters) but the same question for $\mathbb{R}_{alg}$ may be easy (by Theorem 4.5 there is no problem with parameters). Then, one can sometime use Theorem 4.18 to transfer results form $\mathbb{R}_{alg}$ to every real-closed field.

Corollary 4.20 *Let R be a real-closed field and let $u = (u_n)_{n\geq 1}$ be a sequence of $\mathbb{R}_{alg}$. We denote by X_u the problem of R defined by: $(a_1, \ldots, a_n) \in X_u$ iff $a_1 = u_n$. If X_u is $\mathbb{PAR}_R$, then there exists a polynomial q such that for all n, $|u_n| \leq exp(exp(q(n)))$.*

Proof. First we assume that $R = \mathbb{R}_{alg}$. By Theorem 4.5, X_u is in $\mathbb{PAR}_R$ with a sequence of circuits which do not use parameters from R. It is easy to see that X_u is solved by a sequence of formulas $(\phi_n(\bar{x}))$ where the ϕ_n are of the form

$$\bigvee_{i=1}^{I_n} \bigwedge_{j=1}^{J_{in}} (Q_{ijn}(\bar{x})\Delta_{ij}0),$$

where the Q_{ijn} are polynomials of $\mathbb{Z}[\bar{x}]$ of degree and bit length of the coefficients bounded by $exp(q_1(n))$ where q_1 is a polynomial (here we do not need Theorem 4.15 because we only need bounds on the $Q_{i,j}$). By definition of X_u, u_n is the unique element of R which satisfies $\phi_n(x_1, 0, \ldots, 0)$. Thus, u_n is a zero of a polynomial $h(x_1)$ of $\mathbb{Z}[x_1]$ of degree bounded by $exp(q_1(n))$ and with the absolute value of the coefficients bounded by $exp(exp(q_1(n)))$. Then, the well-known bound on the absolute value of the roots of such a polynomial implies that for all n, $|u_n| \leq exp(exp(q(n)))$ for some polynomial q.
Now we suppose that R is an arbitrary real-closed field. X is $\emptyset$-definable and the extension of X viewed as a problem of $\mathbb{R}_{alg}$ to R is X. Thus, by Proposition 3.9, X is $\mathbb{PAR}_{\mathbb{R}_{alg}}$/const. By Theorem 4.18, X is $\mathbb{PAR}_{\mathbb{R}_{alg}}$. This completes the proof. □

Note that this result can fail if u is not a sequence of algebraic numbers. Here is a counterexample. Let $\alpha \in]0, 1[$ be a transcendent number with radix-2 expansion $\alpha = 0.a_1a_2 \cdots a_n \cdots$. Let $u_n = 1/(\alpha - 0.a_1a_2 \cdots a_n)$. The problem X_u is in $\mathrm{P}_{\mathbb{R}}$ since the digits $a_1, \ldots, a_n$ can be extracted from α in time $O(n)$. However, one can choose α so that no bound of the form $|u_n| \leq \exp(\exp(q(n)))$ (or any other bound set *a priori*) holds for every n: just take a sequence of digits with very long sequences of consecutive zeroes.
Set $u_n = exp(exp(exp(n)))$. Clearly, X_u is in EXP_R for every real-closed field. By the corollary above X_u can not be $\mathbb{PAR}_R$ and we obtain the separation of $\mathbb{PAR}_R$ and EXP_R with a simpler problem than the problems used in [8] and [9].
We can also obtain the main result of [10]. We recall that if $\mathcal{C}$ is a complexity class $\mathcal{BP}(\mathcal{C}_M)$ is the class of problems $X \subseteq \{0,1\}^\infty$ which are in $\mathcal{C}_M$.

Corollary 4.21 *If R is a real-closed field, then $\mathcal{BP}(\mathbb{P}\mathrm{AR}_R) = \mathrm{PSPACE/poly}$.*

Proof. The inclusion PSPACE/poly $\subseteq \mathcal{BP}(\mathbb{P}\mathrm{AR}_R)$ is "obvious". The reverse inclusion is easy for $\mathbb{R}_{alg}$ (use Theorem 4.5). If $X \subseteq \{0,1\}^\infty$, then X is $\emptyset$-definable and the extension of $X \subseteq \mathbb{R}_{alg}^\infty$ to R is X. Thus, if X is $\mathcal{BP}(\mathbb{P}\mathrm{AR}_R)$, then X is $\mathcal{BP}(\mathbb{P}\mathrm{AR}_{\mathbb{R}_{alg}}/\mathrm{const})$ and thus $\mathcal{BP}(\mathbb{P}\mathrm{AR}_{\mathbb{R}_{alg}})$ by Theorem 4.18. □

We denote by WEXP_R ($\mathbb{WEXP}_R$) the class of problem solved by a machine over R in weak (nonuniform) exponential time (see [20] and [12] for a definition; one can define $\mathbb{WEXP}_R$ as $\mathrm{WEXP}_R/\mathcal{F}$ where $\mathcal{F}$ is the set of functions from $\mathbb{N}$ into $\{0,1\}^\infty$ such that $f(n)$ is of exponential size in n). Note that again $\mathrm{WEXP}_R = \mathbb{WEXP}_R$ if R contains the reals. One can use Theorem 4.18 to obtain transfer results relating parallel polynomial time classes to higher complexity classes. For instance, the question $\mathbb{PAR}_R =?\mathbb{WEXP}_R$ has the same answer in all real-closed fields. Unfortunately, this result is of little interest since, unlike the inclusion $\mathrm{P}_R \subseteq \mathrm{NP}_R$, the inclusion $\mathbb{PAR}_R \subset \mathbb{WEXP}_R$ is known to be strict in every real-closed field (this follows from a connected component argument). Other inclusions of this type are also known to be strict. For instance, it is noted in [10] that Corollary 4.21 implies that $\mathbb{P}\mathrm{AR}_R$ is strictly include in $\mathbb{WEXP}_R$ because $\mathcal{B}P(\mathbb{WEXP}_R)$ is the set of all boolean problems.
We conclude this subsection by a remark somewhat out of context. In the case of the reals, the separation of $\mathbb{P}\mathrm{AR}$ and $\mathbb{WEXP}$ gives the separation of PAR and WEXP, but if $R = \mathbb{R}_{alg}$ we have $\mathcal{B}P(\mathrm{PAR}_R) = \mathrm{PSPACE}$ and $\mathcal{B}P(\mathrm{WEXP}) = \mathrm{EXP}$. Thus, the separation of $\mathrm{PAR}_{\mathbb{R}_{alg}}$ and $\mathrm{WEXP}_{\mathbb{R}_{alg}}$ using a boolean problem depends on the well-known open question: PSPACE $\neq$? EXP.

4.6 Non P-stability of the Reals

Let R be real-closed field. If $R \not\simeq \mathbb{R}$ it is rather obvious that R is not P-stable.

Proposition 4.22 *Let R be a real-closed field not isomorphic to $\mathbb{R}$. There exists a real-closed field R' containing R and a problem in $\mathrm{P}^1_{R'}$ with a restriction to R which is not definable and thus not $\mathbb{A}_R$.*

Proof. First, we suppose that R is archimedean. Then, we may assume that $R \leq \mathbb{R}$ and let $a \in \mathbb{R}\backslash R$. Let Y_a be the problem of $\mathbb{R}^\infty$ defined by: $(x_1, ..., x_n) \in Y_a$ if and only if $x_1 < a$. Clearly, $Y_a \in \mathrm{P}^1_{\mathbb{R}}$. Moreover, the set of $x \in R$ so that $x < a$ is not definable in R and thus the restriction of Y_a to R is not $\mathbb{A}_R$.
Now we assume that R is not archimedean. Let A be the set of $x \in R$ such that $x < n$ for an integer n. Then, there exists a real-closed field $R' \geq R$ with an element a so that $x \in A$ if and only if $x < a$ (such an element exists in any $card(A)^+$-saturated elementary extension of R). Then, we can proceed as above. □

We can use the Dedekind completeness of $\mathbb{R}$ to prove a weak kind of P^1-stability for $\mathbb{R}$ (compare with Proposition 4.9).

Proposition 4.23 *Let K be an ordered extension of $\mathbb{R}$. If $X \in \mathrm{P}_K$ with a machine $\mathcal{M}$ which uses as parameters $\alpha_1, ..., \alpha_k$ with $\alpha_1, ..., \alpha_{k-1} \in \mathbb{R}$, then the restriction of X to $\mathbb{R}$ is in $\mathrm{PH}_{\mathbb{R}}$.*

Proof (sketch). If $\alpha_k \in \mathbb{R}$ there is nothing to prove. If $|\alpha_k|$ is not infinitely large over $\mathbb{R}$, then, by Dedekind completeness of $\mathbb{R}$, $\alpha_k = \beta_k + \epsilon$ with $\beta_k \in \mathbb{R}$ and ϵ infinitely

small over $\mathbb{R}$. So, we may assume that $\alpha_k > a$ for all $a \in \mathbb{R}$ (replace α_k by $-\alpha_k$ or $\pm 1/(\alpha_k - \beta_k)$ and add β_k to $\alpha_1, ..., \alpha_{k-1}$ and compute α_k before running $\mathcal{M}$).
Here, the *Witness Problem* $\mathrm{WITNESS}^1_>$ is the set of straight-line programs $P_1, \ldots, P_v$ where the P_i are polynomials over $\mathbb{R}$ with one indeterminate (i.e., a circuit without test, with one output gate, one input gate and with parameters in $\mathbb{R}$) such that the sign of the leading coefficient of P_v (the polynomial computed by the circuit) is > 0. $\mathrm{WITNESS}^1_>$ is in the second level of $\mathrm{PH}_\mathbb{R}$:

$$P_1, \ldots, P_v \in \mathrm{WITNESS}^1_> \text{ if and only if } \exists x\, \forall y\, (\, y > x \;\Rightarrow\; P_v(y) > 0\,).$$

Now, by hypothesis on α_k, if $P \in \mathbb{R}[y]$,

$$P(\alpha_k) > 0 \text{ if and only if } \exists x \forall y\, (\, y > x \;\Rightarrow\; P(y) > 0\,).$$

For inputs in $\mathbb{R}$, α_k can then be viewed as an indeterminate y and one can use $\mathrm{WITNESS}^1_>$ to perform tests (that we may assume without loss of generality to be of the form "$P > 0$?") in a simulation of the circuit family recognizing X. It is then easy to see that $A \in \mathrm{PH}_\mathbb{R}$. $\square$

Then it is natural to ask whether the problem $\mathrm{WITNESS}^1_>$ of the proof of Proposition 4.23 is in $\mathrm{P}_\mathbb{R}$? Of course, a positive answer would imply that the problem X of Proposition 4.23 is in $\mathrm{P}_\mathbb{R}$ and that $\mathrm{P}^l_\mathbb{R}/1 \subseteq \mathrm{P}_\mathbb{R}$.
Let R be real-closed extension of $\mathbb{R}$. If $Y \in \mathrm{P}_R$, then it follows from a result of van den Dries [35] that the restriction of Y to $\mathbb{R}$ is definable. However, the proposition above cannot be generalized to more that one parameter not in $\mathbb{R}$: in general we need an infinite number of parameters to define the restriction of Y to $\mathbb{R}$. The proof uses a construction communicated to us by van den Dries [36].

Theorem 4.24 *Let $\mathbb{R}_{pui}$ be the real-closed field of Puiseux series over $\mathbb{R}$. There exists a problem $Y \in \mathrm{P}^2_{\mathbb{R}_{pui}}$ whose restriction X to $\mathbb{R}$ is not $\mathrm{A}_\mathbb{R}$.*

Proof. Let R be a real-closed. The field R_{pui} of Puiseux series over R is the field of formal power series:

$$\sum_{i=k}^{+\infty} a_i \epsilon^{i/q} \quad \text{with } k \in \mathbb{Z},\, q \in \mathbb{N}\backslash\{0\} \text{ and } a_i \in R$$

with the formal addition and multiplication (a series of the above form is positive if and only if $a_k > 0$). R_{pui} is real-closed and $R \leq R_{pui}$ in the obvious way.
Given a sequence a of positive real numbers we denote by γ_a the element $\sum_{i \geq 1} a_i \epsilon^i$. Let $Y_a \subseteq \mathbb{R}^\infty_{pui}$ be the following problem: for $x \in \mathbb{R}^n_{pui}$, $x \in Y_a$ if and only if $\sum_{k=1}^n x_k \epsilon^k < \gamma_a$. Obviously, $Y_a \in \mathrm{P}^2_{\mathbb{R}_{pui}}$. Let X_a be the restriction of Y_a to $\mathbb{R}$. For $x \in \mathbb{R}^n$, $x \in X_a$ if and only if:

$$\begin{array}{lll} (x_1 < a_1) & \vee & (x_1 = a_1 \wedge x_2 < a_2) \\ & \vee & (x_1 = a_1 \wedge x_2 = a_2 \wedge x_3 < a_3) \\ & \cdots & \\ & \vee & (x_1 = a_1 \wedge \cdots \wedge x_{n-2} = a_{n-2} \wedge x_{n-1} < a_{n-1}) \\ & \vee & (x_1 = a_1 \wedge \cdots \wedge x_{n-1} = a_{n-1} \wedge x_n \leq a_n). \end{array}$$

In particular, an input of the form $(a_1, \ldots, a_{n-1}, x_n)$ is in X_a if and only if $x_n \leq a_n$. Assume that X_a can be solved in bounded time by a machine over $\mathbb{R}$ with l real parameters $\alpha_1, \ldots, \alpha_l$. The above remark implies that a_n is algebraic over $\mathbb{Q}(\alpha_1, \ldots, \alpha_l, a_1, \ldots, a_{n-1})$. It then follows from a straightforward induction on n that the a_i's are all algebraic over $\mathbb{Q}(\alpha_1, \ldots, \alpha_l)$. We obtain a contradiction when the a_n's are algebraically independent. $\Box$

This theorem shows that there are problems $Y \in \mathrm{P}_R$ in an extension $\mathbb{R} \leq R$ whose restriction X to $\mathbb{R}$ is not $\mathrm{P}_\mathbb{R}$, and, even worse, is not $\mathrm{A}_\mathbb{R}$. One could try to recover the property $X \in \mathrm{P}_\mathbb{R}$ by adding additional hypotheses. Unfortunately, even if X is $\mathrm{A}_\mathbb{R}$ it may still be the case that $X \notin \mathrm{P}_\mathbb{R}$. The proof is similar to that of Theorem 4.24. Instead of algebraically independent a_n's, we use a sequence of algebraic numbers with very fast growing degrees over $\mathbb{Q}$. This will ensure that the problem X_a of the proof of the above theorem is $\mathrm{A}_\mathbb{R}$ (since an algebraic element is $\emptyset$-definable). We also need a lemma of independent interest. Roughly speaking, the morale is that algebraically independent parameters do not help create algebraic numbers of high degree.

Lemma 4.25 *Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_l)$ be an extension of $\mathbb{Q}$ where $\alpha_1, \ldots, \alpha_l$ are algebraically independent. Let $\beta \in \overline{\mathbb{Q}}$ be of degree k over $\mathbb{Q}$. The degree of β over K is also equal to k.* $\Box$

Proof. Let d be the degree of β over K. Obviously, $d \leq k$. For the converse, let $M(\alpha, .) = \sum_{j=0}^{l} P_l(\alpha) y^j$ be the minimal polynomial of β over K, where $M \in \mathbb{Z}[x_1, \ldots, x_l, Y]$. The polynomial $M(., \beta) \in \mathbb{Z}[\beta][x_1, \ldots, x_d]$ vanishes for $x_1 = \alpha_1, \ldots, X_l = \alpha_l$. Since $\alpha_1, \ldots, \alpha_l$ are algebraically independent over $\mathbb{Q}[\beta]$, this implies that $M(., \beta) \equiv 0$. Let $a_1, \ldots, a_l$ be rational constants such that $P_l(a_1, \ldots, a_l) \neq 0$. It follows that $M(a_1, \ldots, a_l, \beta) = 0$ and $M(a_1, \ldots, a_l, .) \not\equiv 0$. Thus $d \geq k$ (otherwise $M(\alpha, .)$ would not be of minimal degree). $\Box$

Theorem 4.26 *There exists a problem in $\mathrm{P}^2_{\mathbb{R}_{pui}}$ with a restriction X to $\mathbb{R}$ which is $\mathrm{A}_\mathbb{R}$, but $X \notin \mathrm{P}_\mathbb{R}$.*

Proof. Consider the problems X_a introduced in the proof of Theorem 4.24. Assume that X_a can be solved in time bn^c by a machine with l parameters $\alpha_1, \ldots, \alpha_l$. We have seen in the proof of that theorem that the a_i's must be algebraic over $\mathbb{Q}(\alpha_1, \ldots, \alpha_l)$. One can estimate their degrees by, e.g., Theorem 4.1. Namely, there exists a (monotone) bound $f(b, c, n, l)$ depending only on b, c, n, and l such that a_n is of degree at most $f(b, c, n, p)$ over $\mathbb{Q}(\alpha_1, \ldots, \alpha_p)$. We can assume without loss of generality that $\alpha_1, \ldots, \alpha_{l-1}$ are algebraically independent, and that α_l is algebraic over $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_{p-1})$. Let k be the degree of α_p over K. The degree of a_n over K is then bounded by $g(b, c, n, l, k) = kf(b, c, n, l)$. By Lemma 4.25, $g(b, c, n, l, k)$ is also a bound for the degree of a_n over $\mathbb{Q}$. A contradiction results from a simple diagonalization argument: just take a_n of degree at least $g(n, n, n, n, n) + 1$. The corresponding language X_a is not in $\mathrm{P}_{\mathbb{R}}$. We have already seen that X_a is algorithmic over $\mathbb{R}$ in bounded time since the a_n's are algebraic. $\square$

Note that the above theorem holds as well for every real-closed field and that a real-closed field is Dedekind complete in its field of Puiseux series.

5 Ordered $\mathbb{Q}$-vector Spaces

5.1 Background

In this section we consider machine over $\mathbb{R}$ and related structures which perform only addition, opposite and branching with $=$ and $<$. In the model theoretic setting the language is the language of ordered abelian groups with a distinguished element $\bar{1}$: $\mathcal{L} = \{+, -, 0, \bar{1}, <, =\}$. The theory of divisible ordered abelian groups with a distinguished element $\bar{1} > 0$ is complete, admits elimination of quantifiers and is o-minimal (in particular, any extension $E \leq F$ of models of this theory is elementary). The models of this theory are exactly the ordered $\mathbb{Q}$-vector spaces with an element $\bar{1} > 0$. The reals $\mathbb{R}$ without multiplication are of course a model of this theory (interpreting $\bar{1}$ by 1 or any positive element). To avoid confusion, when we look at $\mathbb{R}$ in $\mathcal{L}$ we denote it by $\mathbb{R}_{ovs}$. Computation over $\mathbb{R}_{ovs}$ has been studied in a number of papers (see for example [19] and [11]) and the question $\mathrm{P}_{\mathbb{R}_{ovs}} = ?\ \mathrm{NP}_{\mathbb{R}_{ovs}}$ seems to be difficult. In this section, E will be an ordered vector space and we always assume that our ordered vector spaces have a distinguished element $\bar{1} > 0$ (and thus has dimension ≥ 1). We can make a correspondence with the setting of the previous section: ordered $\mathbb{Q}$-vector spaces correspond to real-closed fields, the ordered $\mathbb{Q}$-vector space of dimension one that we denote by $\mathbb{Q}_{ovs}$ corresponds to $\mathbb{R}_{alg}$ (as the ordered $\mathbb{Q}$-vector space which embeds in all ordered $\mathbb{Q}$-vector spaces) and of course $\mathbb{R}_{ovs}$ corresponds to $\mathbb{R}$ (as the only ordered $\mathbb{Q}$-vector space with a complete order). We consider E with the order topology and E^k with the product topology. As for real-closed fields we can express some topological facts with first-order formulae. Also, we can define the classes $\mathbb{A}/^*$const, $\mathbb{P}/^*$const,..., as for real-closed fields.
In Section 5.2, we need a good elimination theorem. If ϕ is a formula of $\mathcal{L}$ with parameters α, then the terms which appear in ϕ are of the form

$$a_1.x_1 + \ldots + a_n.x_n + b_1.\alpha_1 + \ldots b_k.\alpha_k$$

where the a_i and the b_i are in $\mathbb{Z}$. The bit length of such a term is the max of the bit length of the a_i and the b_i. We denote by $\#(\phi)$ the max of the bit length of the terms which appear in ϕ. The following result is a consequence of a result of Sontag (see [34, Lemma 3.3]).

Fact 5.1 *There exists a polynomial p such that following holds. Assume that $\phi(\bar{x}, \alpha)$ is a formula of the form*

$$Q_1\bar{y}_1 \ldots Q_\omega\bar{y}_\omega\ \phi'(\bar{y}_1, \ldots, \bar{y}_\omega, \bar{x}, \alpha)$$

where the Q_i are quantifiers, ϕ' is quantifier-free, the $\bar{y}_i$ are tuples of length $\leq n$ and the α are parameters of E. Then, there exists a quantifier-free formula $\psi(\bar{x}, \alpha)$ equivalent to $\phi(\bar{x}, \alpha)$ such that $\#(\psi) \leq p(n)^w \#(\phi')$.

Now, we recall some facts that we shall need (in section 5.3) to prove the P-stability of $\mathbb{R}_{ovs}$. Let G be an abelian ordered group. A subset X of G is convex if for every $g, h \in X$, if $g < c < h$ then $c \in X$. The convex hull of a subset of G is the smallest convex subset of G which contains X. If X is a subgroup of G, then the convex hull H of X is also a subgroup of G. Moreover, if G is divisible then H is also divisible (thus the convex hull of a subspace of an ordered $\mathbb{Q}$-vector space is a subspace). We denote by $|g|$ the absolute value of g. Let g and h be two elements of G. We write $g << h$ if $ng < |h|$ for all $n \in \mathbb{Z}$. We say that g and h are comparable if neither $g << h$ nor $g << h$. If X and Y are subsets of G, we write $X << Y$ if for all $g \in X \backslash \{0\}$ and all $h \in Y \backslash \{0\}$, $g << h$. G is archimedean if all the nonzero elements of G are comparable. These groups are well-known:

Fact 5.2 *An abelian ordered group is archimedean iff it is isomorphic to a subgroup of the ordered additive group of the reals. Moreover, a Dedekind complete ordered abelian group is isomorphic to $\mathbb{R}_{ovs}$.*

We recall the "classification" of finite dimensional ordered $\mathbb{Q}$-vector spaces.

Fact 5.3 *Let E be an ordered $\mathbb{Q}$-vector space of finite dimension. There exist subspaces $E_1, \ldots, E_m$ of E such that*
(1) $E \simeq E_1 \times \ldots E_m$ (as a vector space);
(2) the E_i are archimedean;
(3) $E_1 << E_2 << \ldots << E_m$. In other words, E is a direct product of archimedean vector spaces E_j and the order on E is given by the right lexicographic order on $E_1 \times \ldots \times E_n$.

5.2 $\mathbb{P}$-saturation

Note first that Proposition 3.15 implies that if E is countable, there are boolean problems in $\mathrm{P}_E^0/1$ which are not in A_E. Moreover, the proof of Proposition 4.16 does not use multiplication and holds for ordered $\mathbb{Q}$-vector spaces (i.e., $\mathbb{P}_E \subseteq \mathrm{P}_E/1$). Thus we need to work at the nonuniform level. Note that, again, if E contains $\mathbb{R}_{ovs}$, then most of the nonuniform classes for E are uniform without lost of time (in particular, $\mathbb{P}_{\mathbb{R}_{ovs}} = \mathrm{P}_{\mathbb{R}_{ovs}}$).
The results of Section 4.2 can be adapted. We need the following well-known lemma.

Lemma 5.4 *Let E be an ordered $\mathbb{Q}$-vector space. Let X be a problem in $\mathrm{SIZE}_E^k(t)$, and $(\alpha_1, \ldots, \alpha_k)$ the corresponding vector of parameters. Then, X is in $\mathrm{SIZE}_E^l(t)$ using $l \leq k$ linearly independent parameters over the subspace spanned by $\bar{1}$, where $l+1$ is the dimension of the subspace spanned by $(1, \alpha_1, \ldots, \alpha_k)$. (The same result holds with* TIME *in the place of* SIZE*).* $\Box$

With this lemma and the proof of Lemma 4.6 we obtain the analogue of Proposition 4.17.

Proposition 5.5 *Let E be an ordered $\mathbb{Q}$-vector space.* $\mathbb{A}_E/\mathrm{const} \subseteq \mathbb{A}_E/^*\mathrm{const}$ *"without" any loss of time and uniformity.* □

In ordered $\mathbb{Q}$-vector spaces, everything is for the best in the best of all possible worlds.

Theorem 5.6 $\mathbb{P}_E/^*\mathrm{const} = \mathbb{P}_E/\mathrm{const} = \mathbb{P}_E$.

Proof. The beginning of the proof is the same as the proof of Theorem 4.18, but here, the formulae ϕ_n are circuits $C_n(x_1, \ldots, x_n, y_1, \ldots, y_k, z_1, \ldots, z_l)$ of polynomial size in n: $(C_n(x, y, \alpha))_{n\geq 0}$ define a problem Y of E, there exists a sequence (β_n) of E^k such that for all n, $X \cap E^n$ is solved by $C_n(x, \beta_n, \alpha)$ and for all n the set S_n^* of the $\beta \in E^k$ such that $X \cap E^n$ is solved by $C_n(x, \beta, \alpha)$ has nonempty interior. We define $\sim_n$ and V_n in the same way as in the proof of Theorem 4.18. Using Fact 4.3, we know that V_n is the union of $U_{1,n}, \ldots, U_{s_n,n}$ where the $U_{i,n}$ are the interior of the classes of $\sim_n$ with nonempty interior. We may assume that $U_{1,n}$ is the interior of S_n^*. Then, we define the sets B_n and T_n in the same way as in the proof of Theorem 4.18. Note that there exists a formula $\psi_n(x, y, z)$ equivalent to $C_n(x, y, z)$ of polynomial size (in n) of the form $\exists w\ \psi_n'(x, y, z, w)$ where $\psi_n'(x, y, z, w)$ is quantifier-free. It follows that the T_n are defined by formulae of polynomial size with a bounded number of alternation of quantifiers (with parameters α only). Thus, by Fact 5.1, T_n is defined by a quantifier-free $\theta_n(y_k, \alpha)$ such that $\#(\theta_n)$ is polynomial in n. By construction, we have a point β_n' in $\pi U_{1,n}$ which satisfies $\theta_n(y_k, \alpha)$. Since T_n is finite there exists a term $t(y_k, \alpha)$ of $\theta_n(y_k, \alpha)$ such that $t(\beta_n', \alpha) = 0$. Thus $b_n.\beta_n' = a_{0,n}.1 + a_{1,n}.\alpha_1 + \ldots + a_{l,n}.\alpha_l$ where b_n and the $a_{i,n}$ are integers of bit length polynomial in n. Clearly, we have a circuit $D_n(z)$ (without tests and selections and with one output) of polynomial size such that $D_n(\alpha)$ computes $b_n.\beta_n'$. Using D_n it is then easy to construct a circuit $C_n'(x, y_1, \ldots, y_{k-1}, z)$ such that C_n' is of polynomial size and such that $C_n'(x, y_1, \ldots, y_{k-1}, \alpha)$ is equivalent to $C_n(x, y_1, \ldots, y_{k-1}, \beta_n', \alpha)$. Then, we see that X is in $\mathbb{P}_E^l/^*(k-1)$. We can repeat k times the above procedure and we see that X is in $\mathbb{P}_E^l$. □

By Fact 3.14 and since $\mathbb{P}_{\mathbb{R}_{ovs}} = \mathrm{P}_{\mathbb{R}_{ovs}}$ we obtain:

Corollary 5.7 *(i)* $\mathrm{P}_{\mathbb{R}_{ovs}}/\mathrm{const} = \mathrm{P}_{\mathbb{R}_{ovs}}$.
(ii) If $\mathrm{P}_{\mathbb{R}_{ovs}} \neq \mathrm{NP}_{\mathbb{R}_{ovs}}$, *then there exist problems in* $\mathrm{NP}_{\mathbb{R}_{ovs}} \backslash \mathrm{P}_{\mathbb{R}_{ovs}}$ *which are not* $\mathrm{NP}_{\mathbb{R}_{ovs}}$*-complete.*

Also, Proposition 3.11 gives:

Corollary 5.8 *If E and F are two ordered $\mathbb{Q}$-vector spaces, then* $\mathbb{P}_E = \mathrm{N}\mathbb{P}_E$ *if and only if* $\mathbb{P}_F = \mathrm{N}\mathbb{P}_F$. *If E and F contain $\mathbb{R}_{ovs}$, we can replace $\mathbb{P}$ by P in the above statement.*

As a corollary (to the proof) of Theorem 5.6 we have the following result (the details are left to the reader).

Corollary 5.9 *Let E be an ordered $\mathbb{Q}$-vector space and $\mathcal{C}$ be one of the following complexity classes $\Sigma_h/\text{polybool}$, $\Pi_h/\text{polybool}$, $\mathbb{PH}$, $\mathbb{P}\text{AR}$, $\mathbb{PAR}$, $\mathbb{EXP}$, $\mathbb{PAT}$, $\mathbb{P}\text{EXP}$, $\mathbb{PEXP}$. Then, $\mathcal{C}_E/\text{const} = \mathcal{C}_E$.*

The results above have as consequences some of the known [11] results about boolean part: $\mathcal{B}P(\mathbb{P}_E) = \text{P/poly}$ and $\mathcal{B}P(\mathbb{P}\text{AR}_E) = \text{PSPACE/poly}$. Of course $\mathcal{B}P(\mathbb{EXP}_E)$ and $\mathcal{B}P(\mathbb{PAR}_E)$ are the class of all the problems of $\{0,1\}$. This gives the separation of $\mathbb{P}\text{AR}_E$ and $\mathbb{PAR}_E$. Note that the analogue of Corollary 4.20 (with $\exp(\exp(q(n))$ in place of $\exp(q(n)))$ is easy in the context of this section. This gives the separation of $\mathbb{PAR}_E$ and $\mathbb{EXP}_E$. One can also obtain results similar to Corollary 5.8, for example we have: the questions $\Sigma_h/\text{polybool} =?\ \Pi_h/\text{polybool}$ and $\mathbb{PH} =?\ \mathbb{P}\text{AR}$ are the same in every ordered $\mathbb{Q}$-vector space.
Note that (in contrast to the case of real-closed fields) the boolean part of $\mathbb{P}_E$, $\text{N}\mathbb{P}_E$, $\Sigma_{h,E}/\text{polybool}$, $\Pi_{h,E}/\text{polybool}$, $\mathbb{PH}_E$ and $\mathbb{P}\text{AR}_E$ are known and are equal to (respectively) P/poly, NP/poly, $\Sigma_h/poly$, Π_h/poly, PH/poly and PSPACE/poly (see [11]; the main point is that for E boolean nondeterminism is the same thing as nondeterminism). Thus, for example, if $\mathbb{P}_E = \text{N}\mathbb{P}_E$ then P/poly = NP/poly (and by [18] the standard (uniform) polynomial hierarchy collapse at its second level). A way to obtain a converse to this would be to show that SAT (the standard one) is $\text{N}\mathbb{P}_E$-complete (see [30, Chapter 7] where examples are given of infinite structures where such a converse holds). However, it seems unlikely that this can be true. Assuming P/poly $\neq$ NP/poly, $\mathbb{P}_E \neq \text{N}\mathbb{P}_E$ and there exists quite artificial non-$\text{N}\mathbb{P}_E$-complete problems in $\text{N}\mathbb{P}_E \backslash \mathbb{P}_E$ (by Corollary 5.7) and SAT is not $\mathbb{P}_E$. Thus, we ask the following: is SAT non-$\text{N}\mathbb{P}_E$-complete ?

5.3 P-stability of $\mathbb{R}_{ovs}$

In this subsection we shall show some P-stability results for ordered $\mathbb{Q}$-vector spaces. We need the following lemma which allows to get controllable parameters.

Lemma 5.10 *Let $E \leq F$ be an extension of ordered $\mathbb{Q}$-vector spaces. We assume that E is Dedekind complete in F. Let $\alpha_1, \ldots, \alpha_k$ be elements of F. Then, there exist integers $m, m', s_0, \ldots, s_m, t_1, \ldots, t_{m'}$, elements $\beta_1, \ldots, \beta_{s_0}$ of E, for every $j \in \{1, \ldots, m\}$ a finite dimensional subspace H_j of F spanned by $(\epsilon_{i,j})_{i=1}^{s_j}$ and for every $j \in \{1, \ldots, m'\}$ a finite dimensional subspace G_j of F spanned by $(\gamma_{i,j})_{i=1}^{t_j}$ such that*
(1) each α_i is a linear combination of the β_i, $\epsilon_{i,j}$ and $\gamma_{i,j}$;
(2) the subspaces E, H_j and G_j of F are in direct sum;
(3) $H_1 << H_2 << \ldots << H_m << E << G_1 << \ldots << G_{m'}$.
Thus the subspace spanned by E, the H_j and the G_j is isomorphic to $H_1 \times \ldots H_m \times E \times G_1 \ldots \times G_{m'}$ with the right lexicographic order.

Proof. We denote by F_0 the convex hull of E in F. Then, there exists a subspace G of F such that $F \simeq F_0 \times G$. Then it easy to see that $F_0 << G$. We may assume that $\alpha_1, \ldots, \alpha_l \in F_0$ and that $\alpha_{l+1}, \ldots, \alpha_k \in G$. Then, we apply Fact 5.3 to the subspace spanned by $\alpha_{l+1}, \ldots, \alpha_k$ and we get the G_i and the γ (we take for the H_j subspaces of F_0). Obviously, we may assume that $\alpha_1, \ldots, \alpha_l \in F_0 \backslash E$. Let $i \in \{1, \ldots, l\}$, then, since α_i is in the convex hull of E and since E is Dedekind complete in F, $st(\alpha_i) \in E$. If $st(\alpha_i) = 0$ we do not modify α_i. If $st(\alpha_i) \neq 0$, then $\alpha_i = st(\alpha_i) + \epsilon$ where $\epsilon \in F_0 \backslash E$ and $st(\epsilon) = 0$ and we replace α_i by ϵ. The above argument shows that we may assume that that for all $i \in \{1, \ldots, l\}$, $st(\alpha_i) = 0$. Let H be the subspace spanned by $\alpha_1, \ldots, \alpha_l$. Then, $H << E$ and $H \cap E = (0)$. We can apply Fact 5.3 to H and we obtain the H_j and ϵ. $\square$

Theorem 5.11 *Let $E \leq F$ be a Dedekind complete extension of ordered $\mathbb{Q}$-vector spaces. If X is a problem of F which is $\mathbb{P}_F$, then the restriction of X to E is $\mathbb{P}_E$. In particular, $\mathbb{R}_{ovs}$ is* P*-stable.*

Proof. It suffices to show that if α is a k-tuple of F, then there exists a polynomial q and a k'-tuple α' of E such that for every circuit $C(x_1, \ldots, x_n, y_1, \ldots, y_k)$ of $\mathcal{L}_{ovs}$ (do not forget the selector), there exists a circuit $D(x, y_1, \ldots, y_{k'})$ of $\mathcal{L}_{ovs}$ of size $\leq q(size(C))$ such that for all $v \in E$, $E \models D(v, \alpha')$ iff $F \models C(v, \alpha)$. Note that we may assume that all the tests in C are of the form $L(x, \alpha) < 0$.
By Lemma 5.10 we may assume that α is equal to $\langle \beta, \epsilon, \gamma \rangle$ with the properties (and the notations of) Lemma 5.10 (we assume without loss of generality that $\beta_1 = 1$). Then, we have a tower of Dedekind extensions

$$E \leq H_m \times E \leq \ldots \times_{i=1}^{m} H_i \times E \leq \ldots \times_{i=1}^{m} H_i \times E \times \times_{i=1}^{m'} G_i.$$

Clearly we may assume that $F = \times_{i=1}^{m} H_i \times E \times \times_{i=1}^{m'} G_i$. Moreover, an induction shows that it suffices to consider extensions of the form $E \leq H_m \times E$ and $E \leq E \times G_1$. Let us consider an extension of the form $E \leq H_m \times E$ (the other case is similar). Thus, we assume that $F = H \times E$, $H << E$, H is archimedean and that $\alpha = \langle \beta, \epsilon \rangle$. Now we construct a new circuits D'. The idea is to replace each computation (addition or subtraction) gate of C by two gates so as to separate infinitely small elements from standard parts. If on an input v in E^n a gate of C computes the value $L(v, \beta, \epsilon) = L_1(v, \beta) + L_2(\epsilon)$, then the value of the first corresponding gate in D' (the "standard gate") should be $L_1(v, \beta)$, and the value of the second gate (the "infinitesimal gate") should be $L_2(\epsilon)$. Here L, L_1 and L_2 are linear functions with integer coefficients. The construction of D' by induction is clear. In order to perform an addition, we apply the rule:

$$[L_1(v, \beta) + L_2(\epsilon)] + [L'_1(v, \beta) + L'_2(\epsilon)] = [L_1(v, \beta) + L'_1(v, \beta)] + [L_2(\epsilon) + +L'_2(\epsilon)].$$

A similar rule applies to subtractions. In order to perform a test $L(v, \beta, \epsilon) < 0$, we apply the following rules:

(i) if $L_1(v,\beta) \neq 0$, $L(v,\beta,\epsilon) < 0$ iff $L_1(v,\beta) < 0$;

(ii) if $L_1(v,\beta) = 0$, $L(v,\beta,\epsilon) < 0$ iff $L_2(\epsilon) < 0$.

The nullity test for the first argument of a selection gate can be performed as follows: $L_1(v,\beta) + L_2(\epsilon) = 0$ iff $L_1(v,\beta) = 0$ and $L_2(\epsilon) = 0$. Thus we replace each test gate and each selection gate of C by a little subcircuit made of test and selection gates. The circuit $C(x,\alpha)$ is equivalent to the circuit $D'(x,\beta,\epsilon)$ for inputs in E. Moreover, the size of D' is bounded by $c \cdot \mathrm{size}(C)$ where c is a universal constant.

To complete the proof, we want to replace $\epsilon \in H^s$ by a "small" vector of $\mathbb{Q}^s$ (which depends on C). ϵ can be replaced by any $\eta \in \mathbb{Q}^s$ such that for any input in E^n and any value $L_2(\epsilon)$ computed at an infinitesimal gate of D', $L_2(\epsilon)$ and $L_2(\eta)$ have the same sign. This yields a finite system of linear inequalities, even though there are infinitely many inputs (that's because the coefficients of L_2 are integers of bounded size; indeed their size is polynomial in the size of C). This finite system has a solution in H^s (namely, ϵ), so it must have a solution in $\mathbb{Q}^s$ since H is elementarily equivalent to $\mathbb{Q}$. This implies the existence of a solution $\eta = (p_1/q_1, \ldots, p_s/q_s)$ where the p_i's and q_i's are integers of polynomial size (this fact was used in [19] to show that the boolean part of $\mathrm{P}_{\mathbb{R}_{ovs}}$ is P/poly). Finally, the binary digits of the p_i's and q_i's can be "plugged" in a circuit $D(v,\beta)$ that will simulate $D'(v,\beta,\eta)$ for $v \in E^n$. The size of D is polynomially related to the size of C. $\square$

Note that in this proof we have not used the fact that H is archimedean. One could therefore take directly $H = \times_{i=1}^{m} H_i$ to avoid the induction on m. However, the proof by induction has its merits when E contains $\mathbb{R}_{ovs}$. In this case, since H is archimedean, there exists an embedding of H in $\mathbb{R}_{ovs}$. Let ϵ' the image of the tuple ϵ by this embedding. Then, it is easy to see that the circuit $D'(x,\beta,\epsilon')$ is equivalent to $D'(x,\beta,\epsilon)$ for input in E. Thus, in this case, we do not need to use the existence of small rational points in polyhedra.

Note also that the depth of D in the proof above is also polynomial in the depth of C (with a polynomial which depends only on α). Thus $\mathbb{R}_{ovs}$ is also PAR-stable. Finally, note that Theorem 5.11 implies Corollary 5.7. This gives a very different proof of this result (the proof of Theorem 5.11 for $\mathbb{R}_{ovs}$ does not use Fact 5.1 neither the existence of small rational points in polyhedra).

For an obvious reason, if E is not isomorphic to $\mathbb{R}_{ovs}$, then E is neither P-stable nor $\mathbb{P}$-stable (the proof of Proposition 4.22 works as well for ordered $\mathbb{Q}$-vector spaces). However, it seems to us that every ordered $\mathbb{Q}$-vector space satisfies a weak form of $\mathbb{P}$-stability: if $E \leq F$ is an extension of ordered $\mathbb{Q}$-vector spaces, if $X \in \mathbb{P}_F$ and the restriction of X to E is in $\mathbb{A}_E$, then the restriction of X to E is $\mathbb{P}_E$. Note that, again, we need to work at the nonuniform level: there exist boolean problems which are $\mathrm{A}_{\mathbb{Q}_{ovs}}$ and $\mathrm{P}_{\mathbb{R}_{ovs}}$ but not $\mathrm{P}_{\mathbb{Q}_{ovs}}$.

Acknowledgments

Felipe Cucker pointed out the strict inclusion $\mathbb{PAR}_R \subset \mathbb{WEXP}_R$.

References

[1] J. Balcazar, J. Diaz and J. Gabarro, *Structural complexity I* (Springer-Verlag, Berlin, 1988).

[2] J. Balcazar, J. Diaz and J. Gabarro, *Structural complexity II* (Springer-Verlag, Berlin, 1990).

[3] S. Ben-David, K. Meer, and C. Michaux, A note on non-complete problems in $NP_{\mathbb{R}}$, preprint (1996).

[4] L. Blum, F. Cucker, M. Shub, and S. Smale, Algebraic settings for the problem "P$\neq$NP?", In: *The mathematics of numerical analysis (Park City, UT, 1995)*, Lectures in Applied Mathematic, Vol. 32 (Amer. Math. Soc., Providence, RI, 1996) 125–144.

[5] L. Blum, F. Cucker, M. Shub and S. Smale, *Complexity and Real Computation* (Springer, to appear).

[6] L. Blum, M. Shub, and 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.

[7] J. Bochnak, M. Coste amd M.-F. Roy, *Géométrie algébrique réelle* (Springer-Verlag, Berlin, 1987).

[8] F. Cucker, $P_{\mathbb{R}} \neq NC_{\mathbb{R}}$, *J. Complexity* **8** (1992) 230-238.

[9] F. Cucker, On the complexity of quantifier elimination: the structural approach, *Comput. J.* **36** (1993) 400-408.

[10] F. Cucker and D. Grigoriev, On the power of real Turing machines over binary inputs, *SIAM J. Comput.* **26** (1997) 243-254.

[11] F. Cucker and P. Koiran, Computing over the reals with addition and order: higher complexity classes, *J. Complexity* **11** (1995) 358-376.

[12] F. Cucker, M. Shub, and S. Smale, Separation of complexity classes in Koiran's weak model, *Theoret. Comput. Sci.* **133** (1994) 3-14.

[13] M. Dickmann, Applications of model theory to real algebraic geometry. A survey, In: *Methods in Mathematical Logic*, Lecture Notes in Mathematic, Vol. 1130 (Springer-Verlag, Berlin, 1985) 76-150.

[14] J. Goode, Accessible telephone directories, *J. Symbolic Logic* **59** (1994) 92-105.

[15] J. Heintz, M.-F. Roy, and P. Solernó, Sur la complexité du principe de Tarski-Seidenberg, *Bull. Soc. Math. France* **118** (1990) 101-126.

[16] W. Hodges, Model Theory (Cambridge University Press, Cambridge, 1993).

[17] J. Knight, A. Pillay and C. Steinhorn, Definable sets in ordered structures II, *Trans. Amer. Math. Soc.* **295** (1986) 593-605.

[18] R. Karp and R. Lipton, Turing machines that take advice, *Enseign. Math.* **28** (1982) 191-209.

[19] P. Koiran, Computing over the reals with addition and order, *Theoret. Comput. Sci.* **133** (1994) 35-47.

[20] P. Koiran, A weak version of the Blum, Shub & Smale model, *J. Comput. System Sci.* **54** (1997) 177-189.

[21] P. Koiran, Elimination of constants from machines over algebraically closed fields, Technical Report 96-24, DIMACS (http://dimacs.rutgers.edu/), 1996. To appear in *J. Complexity.*

[22] R. Ladner, On the structure of polynomial time reducibility, *J. Assoc. Comput. Mach.* **22** (1975) 155-171.

[23] A. Macintyre, On ω_1-categorical theories of fields, *Fund. Math.* **71** (1971) 1-25.

[24] G. Malajovich and K. Meer, On the structure of $\mathrm{NP}_{\mathbb{C}}$, *SIAM J. Comput.*, to appear.

[25] D. Marker and C. Steinhorn, Definable types in o-minimal structures, *J. Symbolic Logic* **59** (1994) 185-198.

[26] C. Michaux, P$\neq$NP over the nonstandard reals implies P$\neq$NP over $\mathbb{R}$, *Theoret. Comput. Sci.* **133** (1994) 95-104.

(Presses Universitaires de France, Paris, 1989).

[27] A. Pillay, Some remarks on definable equivalence relations in o-minimal structures, *J. Symbolic Logic* **51** (1986) 709-714.

[28] A. Pillay and C. Steinhorn, Definable sets in ordered structures I, *Trans. Amer. Math. Soc.* **295** (1986) 565-593.

[29] B. Poizat, *Cours de Théorie des modèles* (Nur al-mantiq wal-ma'rifa, Villeurbanne, 1985).

[30] B. Poizat, *Les Petits Cailloux* (Aléas, Lyon, 1995).

[31] B. Poizat, Gonflette dans les modèles ω-saturés, Exposé au groupe de travail LIP-IGD "Complexité Algébrique", Lyon, 1996.

[32] N. Portier, Stabilité polynomiale des corps différentiels, preprint (1997).

[33] J. Renegar, On the computational complexity and geometry of the first-order theory of the reals. parts I, II, III, *J. Symbolic Comput.* **13** (1992) 255–352.

[34] E. Sontag, Real addition and the polynomial hierarchy, *Inform. Process. Lett.* **20** (1985) 115-120.

[35] L. van den Dries, Tarski's problem and pfaffian functions, In: J. Paris, A. Wilkie and G. Wilmers, eds., *Logic Colloquium'84* (North-Holland, Amsterdam, 1985) 59-90.

[36] L. van den Dries, Personal comunication, April 1996.