An Introduction to the Computation Model of Blum, Shub and Smale

Corine CEOLA
Institute of Mathematic, University of Liège (B37)
Grande Traverse, 12
Sart Tilman B-4000 LIEGE (Belgium)
Ph +32 (0)4 366 94 87
Fax +32 (0)4 366 95 47
e-mail Corine.CEOLA@ulg.ac.be

Abstract
In this paper, we present an introduction to the theory of computability and complexity over a ring proposed by L. Blum, M. Shub and S. Smale in [Blum-Shub-Smale-1989].

Keywords: computability, recursion theory, decidability, acceptability, complexity.

1 Introduction

In [Blum-Shub-Smale-1989], Lenore Blum, Mike Shub and Steve Smale have developed a general theory of computation (the *BSS-model*) in which the smallest codable information elements belong to a ring A (or a field) and whose basic operations are this ring's operations and some tests. It allows them to study usual algorithms coming under (numerical) analysis, geometry, optimization and topology, which deal with continuous domains, as $\mathbb{R}$ and $\mathbb{C}$, and so, for which the classical theory of computability and complexity (developed for example by Gödel, Church and Turing) is inappropriate because restricted to discrete problems.

In the BSS-model, an algorithm is described as a machine M changing an input $y \in A^k$ ($k \in \mathbb{N}_0 \cup \{\infty\}$) into the output $\varphi_M(y)$ thanks to a finite sequence of polynomial transformations (rational if A is a field) submitted to tests "$= 0$?" or "≥ 0?" if A is ordered. Note that the special case $k = \infty$ allows to describe general algorithms (in particular uniform with the arbitrary size of their inputs) and to build an universal machine able to simulate any other machine.

Two essential preoccupations of any computation model are, on the one hand, to describe computable maps in the sense of the model (*computability*) and on the other hand, to estimate means neccessary to realize the evaluation of these maps (*complexity*).

The description of computable maps in the BSS-model - i.e. maps φ_M - is formally the same than in classical theory; in particular, it is independent of the ordered ring A. These maps are the recursive ones over the ring A obtained from some basic maps and rules. For example, when $A = \mathbb{Z}$, they are exactly the maps computed by Turing's machines. Domains Ω_M and codomains $\varphi_M(\Omega_M)$ of computable maps are also studied to lead to results connecting these sets (respectively called *halting sets* and *output sets*) and semialgebraic sets [Blum-Shub-Smale-1989, Blum-Smale-1993, Ceola-1995, Meer-Michaux-1997, Mercier-1989, Michaux-1990, Saint Jones-1995].

As for the theory of complexity of the BSS-model, it depends appreciably on the ring A. Here are some illustrations.

The definition of the complexity function involves a notion of height which is defined explicitly by Blum, Shub and Smale only over some rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, what sometimes complicates the transposition of Turing's methods.

Classicaly, the complexity classes (such as the class P of decidable problems in polynomial time, the class NP of verifiable problems in polynomial time, ...) are often defined in terms of decision problems. Maybe some reasons to do so is that it is technically easier and practically better suited than studying directly complexity of functions. Moreover, it is justified by the fact [Lewis-Papadimitriou-1981] that the computability of a map f in the sense of Turing is equivalent to the decidability of its graph $\mathcal{G}_f$. In the BSS-model, if it is always true that the computability of f implies the decidability of $\mathcal{G}_f$, the converse is false: it is true over an algebraically closed field (for example, $\mathbb{C}$) [Ceola-Lecomte-1997] but over $\mathbb{R}$, we can show [Ceola-1995] maps which are not computable but whose graphs are decidable.

In Turing's theory, it is easy to prove that any problem in class NP is decidable. But in the BSS-model, this essential fact is not true in general. At first, over $A = \mathbb{R}$, the decidability of problems in class NP comes, via a non trivial way, from the existence of a problem in class NPC whose decidability results from the exponential algorithm of quantifier elimination of Tarski-Seidenberg [Kreisel-Krivine-1967, Renegar-1989, Seidenberg-1954]. Afterwards, a general result [Goode-1994] characterizes rings over which problems in class NP are decidable, as being rings which admit quantifier elimination.

At last, the validity of the conjecture $P \neq NP$ seems to depend on the ring A. Anyway, it is false in some variations of the BSS-model [Meer-1992, Meer-1993a], in which the basic operations are modified.

Most of notations and results cited or used in this paper come from the original paper [Blum-Shub-Smale-1989]. Proofs are not included in this general presentation but can be found in references.

2 Basic Definitions

Let's describe briefly the concept of *finite dimensional machine* (in normal form) over a commutative ring A. It consists of an *input space* $D = A^k$ ($k \in \mathbb{N}_0$[1]), a *state space* $E = A^l$ ($l \in \mathbb{N}_0$), an *output space* $R = A^m$ ($m \in \mathbb{N}_0$) and a directed graph whose nodes are labelled $1, \ldots, N$. These nodes belong to one of the four following types:

(i) *input node*: only node 1 is of this type; it has no incoming edge, only one outgoing edge to its *next node* $\beta(1)$ and is characterized by the linear injective map $i : D \to E : y \mapsto (y, 0^{l-k})$;

(ii) *output node*: only node N is of this type; it has no outgoing edge and is characterized by the linear map $s : E \to R$ which with x associates $(x_1, \ldots, x_m)$ if $l \geq m$ and $(x_1, \ldots, x_l, 0^{m-l})$ otherwise;

(iii) *computation node*: such a node n has a single outgoing edge to its *next node* $\beta(n)$ and is characterized by a polynomial map $g_n : E \to E$; if A is a field, the map g_n can be rational;

(iv) *branch node*: such a node n has two outgoing edges to its *next nodes* $\beta^-(n)$ and $\beta^+(n)$; if x is a *state* (that is an element of E), the node $\beta^-(n)$ is bound up with the condition $x_1 = 0$ ($x_1 < 0$ if A is ordered) and the node $\beta^+(n)$ up with the condition $x_1 \neq 0$ ($x_1 \geq 0$ if A is ordered).

[1]The set $\mathbb{N}_0$ consists of all stricly positive integers and $\mathbb{N}$ is the union of $\mathbb{N}_0$ and $\{0\}$.

An *infinite dimensional machine* (in normal form) over A consists of an *input space* $D = A^k$ ($k \in \mathbb{N}_0 \cup \{\infty\}$)[1], a *state space* $E = \mathbb{N}_0 \times \mathbb{N}_0 \times A^\infty$, an *output space* $R = A^m$ ($m \in \mathbb{N}_0 \cup \{\infty\}$) and a directed graph. Elements of E are indexed from -1; components of index -1 and 0 are the counters of the state and so, of the machine. Nodes belong to one of the five following types[2]:

(i) *input node*: the linear injective map $i : D \to E$ is defined by

$$\begin{cases} i_{-1}(y) &= 1 \\ i_0(y) &= 1 \\ i_2(y) &= l(y) \\ i_{2r-1}(y) &= y_r \quad \text{if } 1 \le r \le l(y) \\ i_{2r}(y) &= 0 \quad \text{if } 2 \le r \le l(y) - 1 \\ i_r(y) &= 0 \quad \text{if } r \ge 2l(y) \end{cases}$$

where $l(y)$ is the length of y, i.e. the greatest integer λ such that $y_\lambda \neq 0$ (the length of a vector whose all components are zero is zero); then

$$\forall y \in D : i(y) = (1, 1, y_1, l(y), y_2, 0, y_3, \ldots, 0, y_{l(y)}, 0^\infty)$$

where 0^∞ is an infinite sequence of zero's;

(ii) *output node*: the linear map $s : E \to R$ is defined by

$$\forall r \ge 1 : s_r(x) = x_{2r-1};$$

(iii) *computation node*: the polynomial (or rational) map $g_n : E \to E$ is defined by

$$g_n(x) = (g_n^{(1)}(x_{-1}), g_n^{(1)}(x_0), g_n^{(2)}(x))$$

where

$$\begin{cases} g_n^{(1)} : \mathbb{N}_0 \to \mathbb{N}_0 : r \mapsto r + 1 \text{ or } 1 \\ g_n^{(2)} : E \to A^\infty; \end{cases}$$

(iv) *branch node*;

(v) *copy node*: such a node n has a single outgoing edge to its *next node* $\beta(n)$ and is characterized by a map $g_n : E \to E$ such that

$$\forall r \ge -1 : \begin{cases} g_{n,r}(x) &= x_r \quad \text{if } r \neq x_0 \\ g_{n,x_0}(x) &= x_{x_{-1}}. \end{cases}$$

Remark. The concept of infinite dimensional machine has been introduced to solve problems of same kind, by an uniform method which is independent of the arbitrary size of the inputs (for example, a polynomial evaluator, independent of the degree of the

[1]The set A^∞ consists of all "almost everywhere null" sequences over A.

[2]Only differences with the finite case are mentionned.

polynomial map). This concept will be also useful to define an universal machine, which can simulate any other machine.

Example. Figure 1 shows a finite dimensional machine over $\mathbb{R}$. The input and ouput spaces are $\mathbb{R}$ and the state space is $\mathbb{R}^2$. The map of the input (respectively output) node is $i : \mathbb{R} \to \mathbb{R}^2 : y \mapsto (y, 0)$ (respectively $s : \mathbb{R}^2 \to \mathbb{R} : (x_1, x_2) \mapsto x_1$).

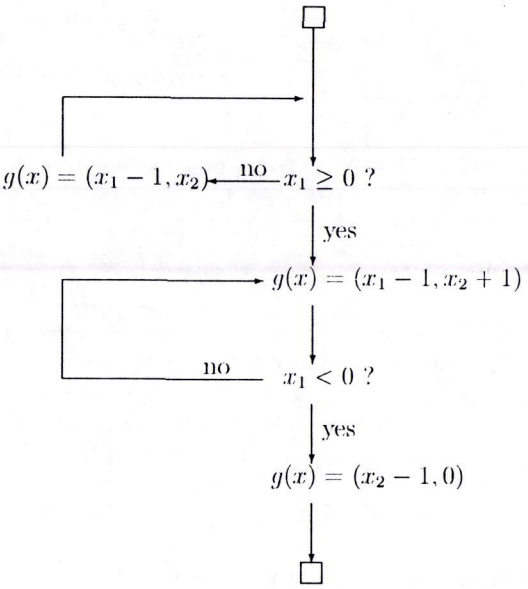

Figure 1. A finite dimensional machine

Let's describe how a machine M works on an *input* y (that is an element of D). The working is characterized by a sequence of node-state couples. At the beginning, we are at node 1 in state $x = i(y)$. We then go, without changing state, to node $n = \beta(1)$, next node of the input node; if n is a computation or copy node, we go to node $\beta(n)$ while producing new state $g_n(x)$; if n is a branch node, the state is still x and we go to node $\beta^-(n)$ or $\beta^+(n)$, according to whether $x_1 = 0$ ($x_1 < 0$ if A is ordered) or whether $x_1 \neq 0$ ($x_1 \geq 0$ if A is ordered). Thus this computation proceeds until the output node N is reached (if ever); we then compute $s(x)$ if x is the state at this node N. We then say that *the computation stops* and *produces* $\varphi_M(y) = s(x)$.

Example. In the above example, for an input $y < 0$, the machine never stops while for an input $y \geq 0$, it repeatedly replaces the first component of the state y by $y - 1$ during it increases, of one unit, the counter x_2 (initially at zero). As soon as y is negative, the counter minus one is the rendered result.

The *halting set* Ω_M of a machine M is the subset of D of inputs for which the computation stops. The map $\varphi_M : \Omega_M \to R$ is the *input-output map.*

Example. In the above example, the halting set of the machine is the set $\mathbb{R}^+$ of positive reals and the input-output map computes the greatest integer in a positive real y.

A partial map $f : Y \subset A^k \to A^m$ $(k, m \in \mathbb{N}_0 \cup \{\infty\})$ is *computable over* A if there exists a machine M such that

$$Y \subset \Omega_M \quad \text{and} \quad \varphi_{M|_Y} = f.$$

A subset Y of A^k $(k \in \mathbb{N}_0 \cup \{\infty\})$ is *acceptable over* A if there exists a machine whose Y is the halting set. It is *decidable over* A if it and its complement in A^k are both acceptable over A.

The following result, well known in classical recursion theory, still holds in the BSS-model.

Lemma 2.1 *A subset Y of A^k $(k \in \mathbb{N}_0 \cup \{\infty\})$ is decidable over A if and only if its characteristic function over A^k is computable over A.*

3 Universal Machine

In this section, we present the concept of universal machine which, given the code of a machine M over A and an input y of M, has the same behaviour than M on y.

Let's first introduce the *powerfree representation of a polynomial function* $f : A^k \to A$ $(k \in \mathbb{N}_0 \cup \{\infty\})$. Let d be the degree of f and m the number of monomials (of non null coefficient). The representation which belongs to A^∞ is defined by

$$PFR(f) = (d, k, \alpha_1^1, \ldots, \alpha_d^1, a_1, \ldots, \alpha_1^m, \ldots, \alpha_d^m, a_m, 0^\infty)$$

where the α_i^j $(1 \leq i \leq d,\ 1 \leq j \leq m)$ are integers between 0 and k; in fact, via the convention "$y_0 = 1$", $(\alpha_1^j, \ldots, \alpha_d^j, a_j)$ $(1 \leq j \leq m)$ represents the monomial $a_j y_{\alpha_1^j} \ldots y_{\alpha_d^j}$ of f. The (α, a) are lexicographically ordered. Note that if $k = \infty$, it is replaced in $PFR(f)$ by the number of effective variables appearing in f.

The *code* of a machine M over A is the element $c(M)$ of A^∞ defined as follows:

(i) $c(M)_1 = 0$ or 1 according to M is finite or infinite;

(ii) $c(M)_2 = 0$ or 1 according to A is a commutative ring or a field;

(iii) the next components are the *codes* $(n, t_n, \beta_n, l_n, g_n)$ of nodes where

- n refers to the node;
- t_n is the type of the node: 1 if n is the input node, 2 if it is the output node, 3 if it is a computation node, 4 if it is a branch node and 5 if it is a copy node;
- β_n is the next node; if $t_n = 4$, $\beta_n = (\beta_n^-, \beta_n^+)$; if $t_n = 2$, β_n is omitted;
- l_n and g_n are present only for $t_n = 3$; l_n is the length of the description of the map g_n of the computation node n; if A is a ring (respectively a field), g_n is described by its dimension followed by powerfree representations of polynomial functions (respectively of numerators and denominators) appearing in effective components of the state;

(iv) the obtained vector is followed by an infinity of zero's.

Theorem 3.1 [Blum-Shub-Smale-1989, Ceola-1995] *There exists an universal machine M_U over A such that for any machine M of finite (respectively infinite) input space*

$$\begin{cases} \Omega_{M_U} = \{(c(M),(y,0^\infty)) \in A^\infty \times A^\infty : y \in \Omega_M\} \\ \varphi_{M_U}(c(M),(y,0^\infty)) = \varphi_M(y) \end{cases}$$

(respectively

$$\begin{cases} \Omega_{M_U} = \{(c(M),y) \in A^\infty \times A^\infty : y \in \Omega_M\} \\ \varphi_{M_U}(c(M),y) = \varphi_M(y)). \end{cases}$$

4 Recursive Maps

A *basic map over* A is any polynomial map (or rational map if A is a field) $f : A^k \to A^m$ $(k,m \in \mathbb{N}_0)$ as well as the function

$$sign : A \to A : y \mapsto \begin{cases} -1 & \text{if } y < 0 \\ 0 & \text{if } y = 0 \\ 1 & \text{otherwise} \end{cases}$$

if A is ordered. Therefore sums, products, projections, constant functions and the successor function (which adds one to its argument) are basic maps.

The *composition* of partial maps $f : Y_f \subset A^k \to A^l$ $(k,l \in \mathbb{N}_0)$ and $g : Y_g \subset A^l \to A^m$ $(m \in \mathbb{N}_0)$ is the partial map $g \circ f : f^{-1}(Y_g) \subset A^k \to A^m : y \mapsto g(f(y))$.

The *juxtaposition* of partial maps f_i $(1 \leq i \leq I, I \in \mathbb{N}_0) : Y_i \subset A^k \to A^{l_i}$ $(k,l_1,\ldots,l_I \in \mathbb{N}_0)$ is the partial map $\psi(f_1,\ldots,f_I) : \cap_{i=1}^I Y_i \subset A^k \to A^{l_1+\ldots+l_I}$ such that for all $j \in \{1,\ldots,l_1+\ldots+l_I\}$

$$\psi(f_1,\ldots,f_I)_j(y) = f_{i,j-l_1-\ldots-l_{i-1}}(y)$$

where $l_1+\ldots+l_{i-1} < j \leq l_1+\ldots+l_i$ (for $i=0$, $l_1+\ldots+l_{i-1}$ is, by convention, as well 0).

The *primitive recursion* of the partial map $f : Y_f \subset A^k \to A^k$ $(k \in \mathbb{N}_0)$ is the partial map

$$g : Y_g \subset \mathbb{N} \times A^k \to A^k : \begin{cases} (0,y) & \mapsto & y \\ (t+1,y) & \mapsto & f(g(t,y)) \end{cases}$$

where $Y_g = \{(0,y) : y \in A^k\} \cup \{(t+1,y) \in \mathbb{N}_0 \times A^k : (t,y) \in Y_g \text{ and } g(t,y) \in Y_f\}$. So $g(t,y)$ is f composed with itself t times applied to y.

The *mininalization* of the partial map $f : Y_f \subset \mathbb{N} \times A^k \to A$ $(k \in \mathbb{N}_0)$ is the partial map $g : Y_g \subset A^k \to \mathbb{N} : y \mapsto min\{t \in \mathbb{N} : f(t,y) = 0\}$ where $Y_g = \{y \in A^k : \exists t \in \mathbb{N}$ such that $(t,y) \in Y_f$ and $f(t,y) = 0\}$.

The set $\mathcal{P}_A^{<\infty}$ of *recursive maps over A between finite dimensional spaces* is the smallest set of partial maps $f : Y_f \subset A^k \to A^m$ $(k,m \in \mathbb{N}_0)$, containing basic maps over A and stable by composition, juxtaposition, primitive recursion and minimalization.

Remark. If we compare the BSS-theory over the countable ring $\mathbb{Z}$ with Turing's one, we can prove [Blum-Shub-Smale-1989, Ceola-1995] that the set of recursive maps in the sense of Turing's theory coincide with the set $\mathcal{P}_{\mathbb{Z}}^{<\infty}$ of recursive maps in the sense of BSS-theory.

Theorem 4.1 [Blum-Shub-Smale-1989] *If $\mathcal{C}_A^{<\infty}$ is the set of partial maps between finite dimensional spaces and computable over A by a finite dimensional machine, then*

$$\mathcal{C}_A^{<\infty} = \mathcal{P}_A^{<\infty}.$$

Remark. Let $\mathcal{C}_{A,\infty}^{<\infty}$ be the set of partial maps between finite dimensional spaces, computable over A by an infinite dimensional machine. Since a finite dimensional machine is equivalent to an infinite dimensional one, we have the inclusion $\mathcal{C}_A^{<\infty} \subset \mathcal{C}_{A,\infty}^{<\infty}$, which is, in fact, an equality [Blum-Shub-Smale-1989, Michaux-1989].

5 Halting Sets and Output Sets

A subset S of A^k ($k \in \mathbb{N}_0 \cup \{\infty\}$) is a *basic semialgebraic set over A* if it is the set of elements of A^k which satisfy a finite system of polynomial inequalities over A; it is a *semialgebraic set over A* if it is the finite union of basic semialgebraic sets over A.

Let M be a machine over A. If $y \in \Omega_M$, we denote $\gamma(y)$ the path followed in the graph of M during its computation on y. If $\xi \in \{1, \ldots, N\}^T$ ($T \in \mathbb{N}_0$), we denote V_ξ the set of inputs y of Ω_M such that $\gamma(y) = \xi$. Thus

$$\Omega_M = \bigcup_{T \in \mathbb{N}_0} \bigcup_{\xi \in \{1,\ldots,N\}^T} V_\xi.$$

Proposition 5.1 [Blum-Shub-Smale-1989] *If M is a machine over A, then each V_ξ ($\xi \in \{1, \ldots, N\}^T$, $T \in \mathbb{N}_0$) is a semialgebraic set over A (basic if the maps at computation nodes are polynomial) and φ_M restricted to V_ξ is a rational map. Moreover, without loss of generality, the denominator of this map can be assumed to vanish nowhere on V_ξ.*

Corollary 5.2 [Blum-Shub-Smale-1989] *Any acceptable set over A is a countable union of basic semialgebraic sets over A.*

Proposition 5.3 *Any semialgebraic set over A is acceptable over A.*

Proposition 5.4 [Mercier-1989] *All countable unions of basic semialgebraic sets over $\mathbb{R}$ are NOT acceptable over $\mathbb{R}$.*

Proposition 5.5 [Michaux-1990] *Any FINITELY generated countable union of semialgebraic sets over $\mathbb{R}$ is acceptable over $\mathbb{R}$.*

Proposition 5.6 [Michaux-1990] *A countable union of basic semialgebraic sets over $\mathbb{R}$ is acceptable over $\mathbb{R}$ if and only if the set of real coefficients which appear in the defining inequalities (of the basic semialgebraic sets) lie in a finitely generated subring of $\mathbb{R}$.*

In particular [Cucker-1992], any subset of $\mathbb{Z}$ becomes decidable over $\mathbb{R}$ and any function from $\mathbb{N}$ to $\mathbb{N}$ is computable over $\mathbb{R}$.

The *output set of a machine M over A* is the subset $\varphi_M(\Omega_M)$ of its output space. It is clear that any halting set Ω_M of a machine M is the halting and output set of another machine M' obtained by the juxtaposition of a machine computing identity and of M. In fact, we have a characterization of subrings of $\mathbb{R}$ for which the halting and output sets coincide.

Theorem 5.7 [Saint Jones-1995] *A subring A of $\mathbb{R}$ is such that the class of halting sets is equal to the class of output sets if and only if one of the following conditions holds:*

(i) A is a real closed field;

(ii) A is of finite transcendence degree (over $\mathbb{Q}$) and it is a recursive ring relative to the Dedekind cuts of members of a transcendence base of A over $\mathbb{Q}$.

Proposition 5.8 [Blum-Shub-Smale-1989] *Over a real closed field, the class of halting sets is equal to the class of output sets.*

6 Undecidable Sets

Proposition 6.1 [Blum-Smale-1993] *Any algebraic number ring A (i.e. a finite algebraic extension of $\mathbb{Z}$) has a subset which is first-order definable over A (in the natural language for ordered rings) but undecidable over A.*

Proposition 6.2 [Ceola-1995] *Any subset of $\mathbb{R}$ dense in $\mathbb{R}$ and with empty interior is undecidable over $\mathbb{R}$.*

Corollary 6.3 [Ceola-1995] *The set $\mathbb{Q}$ of rational numbers is undecidable over $\mathbb{R}$.*

Remark. The set $\mathbb{Q}$ is hence an example of an acceptable set which is not decidable. Other examples of this type are given by the *Cantor Middle third set* and the complement of some *Julia sets* [Blum-Shub-Smale-1989].

A *decision problem over A* is a pair (Y, Y') such that $Y' \subset Y \subset A^k$ $(k \in \mathbb{N}_0 \cup \{\infty\})$. It is decidable if the characteristic function of Y' over Y is computable over A.

Theorem 6.4 [Meer-Michaux-1997] *The halting decision problem (HP, HP') over A defined by*

$$\begin{cases} HP &= \{(c(M), y) \in A^\infty \times A^\infty : M \text{ machine over } A\} \\ HP' &= \{(c(M), y) \in HP : (y_1, \ldots, y_k) \in \Omega_M \text{ with } A^k \text{ as input space of } M\} \end{cases}$$

is undecidable.

7 Computability of a Map and Decidability of its Graph

Over a ring A, the *graph* of a map $f : Y \subset A^k \to A^m$ $(k, m \in \mathbb{N}_0 \cup \{\infty\})$ is the subset of $A^k \times A^m$ defined by

$$\mathcal{G}_f = \{(y, f(y)) \in A^k \times A^m : y \in Y\}.$$

We point here a major difference between the classical model and the model of Blum, Shub and Smale. In the first one, we have [Lewis-Papadimitriou-1981] the equivalence between the computability of a map f and the decidability of its graph $\mathcal{G}_f$. In the latter one, the computability of f still implies the decidability of $\mathcal{G}_f$ but the converse depends on the ring. It is false over $\mathbb{R}$ but true over any algebraically closed field.

Proposition 7.1 [Ceola-Leconte-1997] *If a map $f : A^k \to A^m$ $(k, m \in \mathbb{N}_0 \cup \{\infty\})$ is computable over A, then its graph $\mathcal{G}_f$ is decidable over A.*

Lemma 7.2 [Ceola-1995] *If a function $f : Y \subset \mathbb{R} \to \mathbb{R}$ is computable over $\mathbb{R}$, then any subset Y' of Y, with non empty interior, contains a non empty open interval on which f is rational.*

In a model of computation over $\mathbb{R}$, close to BSS-one [Herman-Isard-1970], it is mentionned that the square root is not computable but has a decidable graph. Using Sturm's theorem [Jacobson-1974], this example can be generalized as follows.

Proposition 7.3 [Ceola-1995] *For each $n \geq 2$, define the function $f_n : \mathbb{R}^{n+1} \to \mathbb{R}$ by*

$$f_n(a_0, \ldots, a_n) =$$

$$\begin{cases} inf\{t \in \mathbb{R} : a_0 + a_1 t + \ldots + a_n t^n = 0\} & \text{if } a_0 + a_1 t + \ldots + a_n t^n \text{ has a real zero} \\ 0 & \text{otherwise.} \end{cases}$$

Each function f_n is not computable over $\mathbb{R}$ but has a decidable graph over $\mathbb{R}$.

In the rest of this section, the ring A is seen as a structure whose functions are the binary sum and product and whose constants are elements of A. It is an *algebraically closed field* if A is a field such that every non constant polynomial in $A[X]$ has a zero in A. *Quantifier elimination* means that there exists an effective procedure such that, given a formula

$$q_1 x_1 \ldots q_r x_r \;\; F(x_1, \ldots, x_r, y)$$

where $q_1, \ldots, q_r$ are quantifiers in $\{\forall, \exists\}$ and $F(x_1, \ldots, x_r, y)$ is a first-order formula allowing constants to denote elements of A, without quantifiers, outputs an equivalent first-order formula $G(y)$ without quantifiers. It is known [Kreisel-Krivine-1967, Seidenberg-1954] that such effective quantifier elimination algorithms exist if A is an algebraically closed field. Moreover it is clear that the truth of a first-order sentence without quantifiers can be tested by a machine in the sense of Blum, Shub and Smale. Therefore the truth of every first-order sentence over an algebraically closed field can be tested.

The next result is true for a ring with an effective quantifier elimination algorithm; in particular, it holds over the ordered ring of the reals [Renegar-1989] and over an algebraically closed field.

Proposition 7.4 [Ceola-Leconte-1997] *Let A a ring with quantifier elimination and M a machine over A deciding a set $Y \subset A^k$ $(k \in \mathbb{N}_0 \cup \{\infty\})$. There exists an effective procedure which, given $y' \in A^{k'}$ $(k' \leq k)$ and $T \in \mathbb{N}_0$, finds the paths of length T, followed by M on inputs of the form $(y', y'') \in Y$ as well as the length k'' of the corresponding y''.*

Remark. A more general version of the previous result holds for a machine M computing the characteristic function of Y' over Y where $Y' \subset Y \subset (A^k \cap \Omega_M)$ $(k \in \mathbb{N}_0 \cup \{\infty\})$. In this case, one searches the paths followed by M on inputs of the form $(y', y'') \in Y'$.

Remark. Note that in the previous result, the y'' are not computed. It is done in the next result thanks to the algebraically closedness of A.

Theorem 7.5 [Ceola-Lecomte-1997] *Over an algebraically closed field A, a map $f : A^k \to A^m$ $(k, m \in \mathbb{N}_0 \cup \{\infty\})$ whose graph is decidable is computable.*

Corollary 7.6 [Ceola-Lecomte-1997] *Over an algebraically closed field A, a computable bijective map $f : A^k \to A^m$ $(k, m \in \mathbb{N}_0 \cup \{\infty\})$ has a computable inverse map f^{-1}.*

8 Basic Notions of Complexity

Let M be a machine over A and y an input of M. If $y \in \Omega_M$, the *halting time* $T_M(y)$ *of M on y* is the length of the path $\gamma(y)$. For an input $y \notin \Omega_M$, $T_M(y) = \infty$. The *height* $h(y)$ *of an element y of* $\mathbb{Z}$ (respectively $\mathbb{Q}$) is $\log_2(|\, y \,| + 1)$ (respectively $sup(h(p), h(q))$ if $y = p/q$ with p and q relatively prime integers). As for as the height of a real, it is 1. The *height of an element y of A^k* $(k \in \mathbb{N}_0 \cup \{\infty\})$ is the $sup\{h(y_i) : i \geq 1\}$.

Remark. The height of an element can be interpreted as proportional to the memory unit necessary to code it. Indeed, over $\mathbb{Z}$, it is of the order of the number of bits required to represent an integer while over $\mathbb{Q}$, it is of the order of the number of bits necessary to represent the numerator and denominator. As for the height over $\mathbb{R}$, it indicates that each real is representable with an infinite precision.

The size $t(y)$ of an element y of A^k $(k \in \mathbb{N}_0 \cup \{\infty\})$ is the product of its length by its height. The *cost function $C_M(y)$ of a machine M over A on the input y* is

$$C_M(y) = h_M(y) T_M(y)$$

where $h_M(y)$ is the maximum height of states met during the working of M on y. A map $f : Y \subset A^k \to A^m$ $(k, m \in \mathbb{N}_0 \cup \{\infty\})$ is *polynomially computable over A* if it is computable by a machine M over A for which there exists a polynomial function p with coefficients in $\mathbb{N}$ such that

$$\forall y \in Y \ : \ C_M(y) \leq p(t(y)).$$

Remark. In the case of the ring $\mathbb{R}$, since $C_M(y) = T_M(y)$, a map defined over $Y \subset \mathbb{R}^k$ $(k \in \mathbb{N}_0)$ polynomially computable is in fact computable in constant time.

Remark. Beside the time needed to compute, one can consider, as in classical theory, the space used during the computation. But it is irrelevant since [Michaux-1989, Michaux-1991] there exists an universal constant c such that for any decision problem and for any input, the size of space needed to the computation is at most the size of the input plus c. So this implies that any decision problem (over any ordered ring) can be solved in linear space. Unfortunately the price to pay is an exponential loss of time in the computations.

9 Decision Problems in Class P_A

A decision problem (Y, Y') over A is *in class P_A* (*determinisitic Polynomial time*) if the characteristic function of Y' over Y is polynomially computable over A.

Theorem 9.1 [Meer-1990] *If (Y, Y') is a decision problem over $\mathbb{R}$ such that $Y' \subset Y \subset \mathbb{R}$, then it is in class $P_{\mathbb{R}}$ if and only if there exists a finite union I of intervals of $\mathbb{R}$ such that*

$$Y' = Y \cap I.$$

Corollary 9.2 *Decision problems $(\mathbb{R}, \mathbb{Z})$, $(\mathbb{R}, \mathbb{Q})$, $(\mathbb{R}, \mathbb{N})$ et $(\mathbb{Q}, \mathbb{Z})$ are not in class $P_{\mathbb{R}}$.*

Remark. We yet knew that $(\mathbb{R}, \mathbb{Q})$ was even not decidable over $\mathbb{R}$; as for as $(\mathbb{R}, \mathbb{N})$, we can deduce from the fact that it is not in class $P_{\mathbb{R}}$ that the entire part of a positive real is not polynomially computable over $\mathbb{R}$.

Let F_d ($d \in \mathbb{N}$) be the subset of A^∞ of powerfree representations of multivariable polynomial functions over A of degree at most d. The set $F_{d,0}$ (respectively $F_{d,0,+}$) is the subset of F_d of powerfree representations of polynomial functions having a zero (respectively a zero with positive components) in A.

Proposition 9.3 [Ceola-1995, Triesch-1990] *For any $d \in \{1, 2, 3\}$, the decision problem $(F_d, F_{d,0})$ over $\mathbb{R}$ is in class $P_{\mathbb{R}}$.*

10 Decision Problems in Class NP_A

A decision problem $(Y. Y')$ over A is *in class NP_A (Nondeterninistic Polynomial time)* if there exist a machine M whose input space is $A^k \times A^k$ and a polynomial function p with coefficients in $\mathbb{N}$ such that

$$\begin{cases} \forall (y, y') \in Y \times A^k : & \begin{cases} \varphi_M(y, y') & \in & \{0, 1\} \\ \varphi_M(y, y') & = & 1 \Leftrightarrow y \in Y' \end{cases} \\ \\ \forall y \in Y' \, \exists y' \in A^k : & \begin{cases} \varphi_M(y, y') & = & 1 \\ C_M(y, y') & \leq & p(t(y)). \end{cases} \end{cases}$$

Theorem 10.1 [Ceola-1995] *Any decision problem over A in class P_A is in class NP_A.*

The *code* $c(S)$ of a matrix $S \in A_s^r$ is the element of A^∞ obtained by juxtaposing its dimensions r and s, elements of its columns and an infinity of zero's.

Proposition 10.2 [Blum-Shub-Smale-1989, Ceola-1995] *The travelling salesman decision problem (TS, TS') over $\mathbb{R}$ defined by*

$$\begin{cases} TS & = & \{(s, c(S)) \in \mathbb{R}^\infty : S \text{ symmetrical matrix} \in (\mathbb{R}^+)_r^r, r \in \mathbb{N}_0, s \in \mathbb{R}_0^+\} \\ \\ TS' & = & \{(s, c(S)) \in TS : \text{there exists a non orientated circular permutation } \nu \\ & & \text{of length } r \text{ of } \{1, \ldots, r\} \text{ such that } \sum_{j=1}^{r-1} S_{\nu(j)\nu(j+1)} + S_{\nu(r)\nu(1)} \leq s\} \end{cases}$$

is in class $NP_{\mathbb{R}}$.

11 Decision Problems in Class NPC_A

A decision problem (Y, Y') over A is *reducible* to the decision problem (Z, Z') over A if there exists a map $f : Y \longrightarrow Z$ polynomially computable over A such that $y \in Y'$ if and only if $f(y) \in Z'$. The decision problem (Z, Z') over A is *in class* NPC_A (*Nondeterministic Polynomial time and Complete*) if it is in class NP_A and if every decision problem (Y, Y') in class NP_A is reducible to (Z, Z').

Since any problem in class NP_A is reducible to a problem in class NPC_A, if there exists a decision procedure for this latter, it is also valid for any problem in class NP_A. And more precisely, if there exists a resolution algorithm which is implementable in polynomial time for a problem in class NPC_A and if composition conserves the polynomial character, then any problem in class NP_A is polynomially decidable. In other words, $P_A = NP_A$. But, up to now, as in the classical model, it is only a conjecture.

Theorem 11.1 [Blum-Shub-Smale-1989, Ceola-1995] *For any $d \geq 4$, the decision problem $(F_d, F_{d,0})$ over $\mathbb{R}$ is in class $NPC_{\mathbb{R}}$.*

Remark. The previous result is analogous to Cook's theorem about the 3-satisfiability problem which is NPC in the classical setting [Garey-Johnson-1979]. Here the proof consists of connecting the working of a BSS-machine over A to a system of polynomial inequalities over A such that the machine stops if and only if the system (and so an associated polynomial function of powerfree representation in F_d) has a solution.

Corollary 11.2 [Meer-1993b] *For any $d \geq 4$, the decision problem $(F_d, F_{d,0,+})$ over $\mathbb{R}$ is in class $NPC_{\mathbb{R}}$.*

Remark. Since the algorithm of Tarski-Seidenberg [Seidenberg-1954] allows us to eliminate, over a real closed field, variables of a polynomial system, it solves $(F_d, F_{d,0})$ $(d \geq 4)$ and so decision problems in class $NP_{\mathbb{R}}$ are decidable; moreover they are decidable in single exponential time [Blum-Shub-Smale-1989]. Up to now, no one has proved that this algorithm is polynomially implementable. If it is (or if there exists one), the class $P_{\mathbb{R}}$ and $NP_{\mathbb{R}}$ coincide since in this precise case, composition conserves the polynomial character. The next result characterizes rings A for which decision problems in class NP_A are decidable. The ring A is seen as a structure whose functions are the binary sum and product and whose constants are elements of A.

Theorem 11.3 [Goode-1994] *Decision problems over A in class NP_A are decidable if and only if A admits effective quantifier elimination for first-order formulae over A.*

Theorem 11.4 [Blum-Shub-Smale-1989, Shub-Smale-1997] *The k^{th} Hilbert's Nullstellensatz decision problem (HN_k, HN'_k) $(k \in \mathbb{N}_0)$ over an algebraically closed field A defined by*

$$\begin{cases} HN_k = \{(PFR(f_1), \ldots, PFR(f_r)) \in A^\infty : f_1, \ldots, f_r (r \in \mathbb{N}_0) \text{ polynomial functions over } A \text{ of } k \text{ variables and degree } d_1, \ldots, d_r \text{ respectively}\} \\ HN'_k = \{(PFR(f_1), \ldots, PFR(f_r)) \in HN_k : \text{there exists } y \in A^k \text{ such that for all } i \in \{1, \ldots, r\} : f_i(y) = 0\} \end{cases}$$

is in class NPC_A.

Remark. It is a general fact that the Hilbert's Nullstellensatz decision problem is not in class P_A if and only if classes P_A and NP_A are different. More precisely, over $A = \mathbb{C}$, the belonging of this problem to class $P_{\mathbb{C}}$ is a conjecture which can be reduced to the algebraic problem of finding the "hardness to compute" the sequence $(k!)_{k\in\mathbb{N}}$ of integers [Shub-Smale-1997]. This is interesting because it combines a problem from number theory with the $P_{\mathbb{C}} \neq NP_{\mathbb{C}}$ question.

12 Conclusions

This presentation is far away from to be complete. For more results and references, you can consult the recent survey of Meer and Michaux [Meer-Michaux-1997], in particular for separation results, lower bounds and descriptive complexity theory. Let's point out variations about the basic definition of machines as additive and linear machines [Koiran-1994, Meer-1992, Meer-1993b] or as machines performing trigonometric functions [Meer-1993a]. Another variant consists of using a different (maybe more realistic) cost measure [Koiran-1993]. Machines including round-off errors and approximate solutions or probabilistic features should be examined carefully [Blum-Shub-Smale-1989]. And finally let's stress on the forthcoming book of Blum, Cucker, Shub and Smale [Blum-Cucker-Shub-Smale-1997].

References

[Blum-Cucker-Shub-Smale-1997] L. Blum, F. Cucker, M. Shub and S. Smale, *Complexity and real computation* (Springer Verlag, forthcoming book).

[Blum-Shub-Smale-1989] 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*, Bulletin (new series) of the american mathematical society, volume 21, 1-46, 1989.

[Blum-Smale-1993] L. Blum and S. Smale, *The Gödel incompleteness theorem and decidability over a ring*, From topology to computation, Proceedings of the smalefest, Springer Verlag, 321-339, 1993.

[Ceola-1995] C. Ceola, *Calculabilité et complexité au sens de Blum, Shub et Smale*, Mémoire présenté pour l'obtention du grade de maître en sciences mathématiques, Université de Liège, 1994-1995.

[Ceola-Leconte-1995] C. Ceola and P.B.A. Leconte, *Computability of a function and decidability of its graph in the model of Blum, Shub and Smale*, Publication n°95.012, Institut de Mathématique, Université de Liège, 1995.

[Ceola-Leconte-1997] C. Ceola and P.B.A. Leconte, *Computability of a map and decidability of its graph in the model of Blum, Shub and Smale*, to appear in Theoretical computer science.

[Cucker-1992] F. Cucker, *The arithmetical hierarchy over the reals*, Journal of logic and computation, volume 2, $n°3$, 375-395, 1992.

[Garey-Johnson-1979] M.R. Garey and D.S. Johnson, *Computers and intractability. A guide for the theory of NP-completeness* (W.H. Freeman Company, New-York, 1979).

[Goode-1994] J.B. Goode, *Accessible telephone directories*, Journal of symbolic logic, volume 59, $n°1$, 92-105, 1994.

[Herman-Isard-1970] G.T. Herman and S.D. Isard, *Computability over arbitrary fields*, Journal (second series) of the london mathematical society, volume 2, 73-79, 1970.

[Jacobson-1974] N. Jacobson, *Basic algebra I* (W.H. Freeman and Company, San Francisco, 1974).

[Koiran-1993] P. Koiran, *A weak version of the Blum-Shub-Smale model*, FOCS'93, 486-495, 1993 and NeuroCOLT TR series, volume NC-TR-94-5, 1994.

[Koiran-1994] P. Koiran, *Computing over the reals with addition and order*, Theoretical computer science, volume 133, 35-47, 1994.

[Kreisel-Krivine-1967] G. Kreisel and J.L. Krivine, *Elements of mathematical logic* (London, North-Holland Pub. Co., 1967).

[Lewis-Papadimitriou-1981] H. R. Lewis and C. H. Papadimitriou, *Elements of the theory of computation* (Prentice Hall, Inc., New Jersey, 1981).

[Meer-1990] K. Meer, *Computations over $\mathbb{Z}$ and $\mathbb{R}$: a comparison*, Journal of complexity, volume 6, 256-263, 1990.

[Meer-1992] K. Meer, *A note on a $P \neq NP$ result for a restricted class of real machines*, Journal of complexity, volume 8, 451-453, 1992.

[Meer-1993a] K. Meer, *Real number models under various sets of operations*, Journal of complexity, volume 9, 366-372, 1993.

[Meer-1993b] K. Meer, *Komplexitätsbetrachtungen für reelle maschinenmodelle*, D82 (Diss. RWTH Aachen), Verlag Shaker, Aachen, 1993.

[Meer-Michaux-1997] K. Meer and C. Michaux, *A survey on real structural complexity theory*, Bulletin of the belgian mathematical society, Simon Stevin, Journées montoises d'informatique théorique 1994, volume 4, $n°1$, 113-148, 1997.

[Mercier-1989] D. Mercier, *Les machines sur* $\mathbb{R}$, Mémoire présenté pour l'obtention du grade de licencié en sciences mathématiques, Université de l'état à Mons, 1988-1989.

[Michaux-1989] C. Michaux, *Une remarque à propos des machines sur* $\mathbb{R}$ *introduites par Blum, Shub et Smale*, C.R. de l'académie des sciences de Paris, tome 309, série I, 435-437, 1989.

[Michaux-1990] C. Michaux, *Machines sur les réels et problèmes NP-complets*, Séminaire de structures algébriques ordonnées 1988-1989, Equipe de logique, Université Paris VII, prépublication, $n°2$, janvier 1990.

[Michaux-1991] C. Michaux, *Ordered rings over which output sets are recursively enumerable*, Proceedings of the american mathematical society, volume 112, 569-575, 1991.

[Renegar-1989] J. Renegar, *On the computational complexity and geometry of the first-order theory of the reals I, II, III*, Technical report $n°853$, $n°854$, $n°856$, School of operations research and industrial engineering, Cornell, 1989.

[Saint Jones-1995] R. Saint Jones, *Theory of computation for the real numbers and subrings of the real numbers following Blum/Shub/Smale*, Dissertation, University of Berkeley, 1995.

[Seidenberg-1954] A. Seidenberg, *A new decision method for elementary algebra*, Annals of mathematics, volume 60, $n°2$, 365-374, 1954.

[Shub-Smale-1997] M. Shub and S. Smale, *On the intractability of Hilbert's Nullstellensatz and an algebraic version of "*$NP \neq P$*?"*, to appear in Duke journal.

[Triesch-1990] E. Triesch, *A note on a theorem of Blum, Shub and Smale*, Journal of complexity, volume 6, 166-169, 1990.