The diversity of Mathematics respect to a problem in logic

Alain Yger
Laboratoire Bordelais d'Analyse et Géométrie
Université Bordeaux 1, 33405 Talence, France

September 24, 2003

Abstract

The aim of this lecture, through the problem of deciding in polynomial time the existence of a common zero for a system of algebraic equations, is to present how algebraic, analytic or geometric points of view may complement each other respect to a still unsolved but fondamental problem which was submitted to mathematicians by computer scientists or formal calculus specialists. This talk adresses a large audience, which does not need *a priori* to be too familiar with the subject ; it intends mainly to be an humble call for the decompartmentalization (respect to objectives as well as methods) which appears to be more and more necessary nowadays in mathematical research.

I would like to take the opportunity of this manuscript to thank warmly Prof. Adelina Fabiano, Prof. Jacques Guenot, and all members of the *Laboratorio di Applicazioni dalla Matematica all'Ingegneria* (University of Calabria) and to tell them once more how conferences or courses in such places as Cosenza, Camigliatello or Diamante have inspired reflexions about this work.

1 An introduction to the problem $P = NP$

Problems of algorithmic nature lead to the introduction of the naive concept of *machine* over some commutative, unitary and ordered ring $\mathbf{A}$. Such a ring

A appears as a model for the world where elements on which the machine acts lie.

Models of rings that one meets the most frequently are $\mathbb{Z}$ or $\mathbb{Z}[x_1, ..., x_s]$, $\mathbb{R}$ or $\mathbb{R}[x_1, ..., x_s]$; one will also consider the case of rings with positive characteristic, such as $\mathbb{Z}_p$ or $\mathbb{Z}_p[x_1, ..., x_s]$; nevertheless, we stick for the moment to the frame of characteristic zero, which looks to us to be the natural setting for ideas of analytic or algebraic nature to coexist.

Following the presentation of this concept such as it has been introduced in [10], a machine over **A** corresponds (provided one sticks to the finitely dimensional case) to the following set of data :

- a space of *inputs* (generally $\mathbf{A}^l$ for some $l \in \mathbb{N}^*$)
- a space of *outputs* (generally $\mathbf{A}^n$ for some $n \in \mathbb{N}^*$)
- a space of *transient states* (generally $\mathbf{A}^m$ for some $m \in \mathbb{N}^*$)
- a graph with N nodes, node 1 being the unique entry node, other nodes being classified into *exit* nodes, *computation* nodes or *branching* nodes.

To a *computation* node k, one may associate :

- an arrow of the graph pointing towards the next node $\beta(k)$
- a polynomial map g_k from the space of transient states into itself.

To a *branching* node k, one may associate :

- two arrows of the graph which respectively point towards the nodes $\beta^+(k)$ and $\beta^-(k)$
- a polynomial map h_k from the space of transient states into **A** (here the fact that **A** is an ordered ring plays a capital role), which switches the machine either to the node $\beta^+(k)$ when $h_k(\text{state}) \geq 0$ or to the node $\beta^-(k)$ when $h_k(\text{state}) < 0$.

To any *exit* node, one may associate a unique linear map S from the space of transient spaces into the space of outputs ; the unique *entry* node 1 is paired with

- an arrow of the graph pointing towards $\beta(1)$

- an injective linear map I from the space of inputs into the space of transient states.

One may enlarge this concept by getting free from the constraint that represents the finiteness of dimension, that is suppose $l, n \in \mathbb{N} \cup \{\infty\}$; the price to pay is to take as space of transient states the space $\mathbb{N} \times \mathbb{N} \times \mathbf{A}^{\mathrm{N}}$ and introduce in the graph a new class of nodes (nodes of the *fifth class*) ; such a node (labelled for example as k) corresponds to the following data :

- an arrow of the graph that points towards the node $\beta(k)$
- a map $g = g_k$ from the space of transient states into itself whose action consists in the transformation of the state
$$(i, j, x_0, x_1, ..., \overset{j}{x_j}, ...)$$
into the state
$$(i, j, x_0, x_1, ..., \overset{j}{x_i}, ...)$$

If there is no natural order relation on the ring (for example when $\mathbf{A} = \mathbb{C}$ or $\mathbf{A} = \mathbb{Z}_p$ with p prime, the case $p = 2$ leading to the familiar context of Turing machines), one may replace the decision protocol that switches the machine at the level of a *branching* node (labelled as k) by the following one :

- if $h_k(\text{state}) = 0$, the machine switches towards the node $\beta^-(k)$
- if $h_k(\text{state}) \neq 0$, it switches towards the node $\beta^+(k)$.

Given a machine M over the ring $\mathbf{A}$ and some element e in the space of inputs, the machine is said to *stop when initiated at* e when, as soon as it starts with e as input, then some *exit* node is reached after some minimal time $T_M(e)$ (time being indexed with the number of steps the machine proceeds) ; whenever e is such an entry, the *cost* of the machine (when initiated in e) is by definition the quantity

$$C_M(e) := T_M(e) \times h_M(e) \,,$$

where $h_M(e)$ denotes the maximal "height" of all elements in the ring $\mathbf{A}$ which have been involved in all transient states which appear as intermediate states before the machine reaches the *exit* node that will lead to the output $s_M(e)$ (in the output space) within the time $T_M(e)$.

Therefore, it is necessary to introduce a notion of "height" on the ring $\mathbf{A}$. When $\mathbf{A} = \mathbb{Z}$, such a notion of height is chosen so that the corresponding cost function refers to the concept of entropy that quantifies chaos in physics or thermodynamics ; one takes as height of some integer $a \in \mathbb{Z}$ the number of bits that are necessary to code it ; one can define for example the height of $a \in \mathbb{Z}$ as

$$h(a) := \log_2(|a| + 1) \text{ or } \log(|a| + 1)\,.$$

For rational numbers (or even algebraic numbers), one can immediately extend this notion of height : for example, if $x = a/b$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ (in the reduced form) the height of x will be $\max(h(a), h(b))$; when x is an algebraic number, $h(x)$ will be the sum of the logarithm of the degree of x, together with the maximum of the logarithmic heights of all integer coefficients involved in the expression of the minimal polynomial of x over $\mathbb{Q}$. These are just naives definitions for the logarithmic height (in the arithmetic context) that we will make more rigorous later in section 3. When $\mathbf{A} = \mathbb{R}$, one decides that the height of any real number equals 1, which reflects the obvious fact that the cost of the multiplication by a real number is independent of its size.

We now have within hands all elements in order to be able to define what is a decision problem over some ring $\mathbf{A}$ and precise two classes of decision problems, namely the P class and the NP class.

A *decision problem* over $\mathbf{A}$ is a pair of subsets (X, X_{yes}) , $X_{\text{yes}} \subset X$, of the space $\mathbf{A}^l$ (here l may be finite or infinite) ; such a space $\mathbf{A}^l$ will play the role of the space of inputs for some machine over $\mathbf{A}$. What we will call an algorithm solving the decision problem will be a machine M which can be initiated from any input $e \in X$, which eventually stops when initiated from such an element, providing then an output $s_M(e)$ such that :

$$s_M(e) = 1 \Longleftrightarrow e \in X_{\text{yes}}\,.$$

We will focuse on three important decision problems :

- The problem which consists in deciding whether a given collection of m polynomials $P_1, ..., P_m \in \mathbb{C}[X_1, ..., X_n]$ generates a proper ideal or not, which is equivalent to check whether, yes or no, the system of algebraic equations $\{P_1(\zeta) = \cdots = P_m(\zeta) = 0\}$ has a solution in $\mathbb{C}^n$. For this problem, the ring is $\mathbb{C}$, but one may as well consider any commutative integral domain $\mathbf{A}$, such as $\mathbb{Z}$, $\mathbb{Z}[x_1, ..., x_s]$, $\mathbb{Z}_p[x_1, ..., x_s]$; a proper ideal means in this case proper in $\mathbf{K}[X_1, ..., X_n]$, where $\mathbf{K}$ is the fraction field of $\mathbf{A}$. This decision problem is known as *Hilbert's zeroes problem* or the *algebraic nullstellensatz.*

- Given a collection of $m+1$ polynomials in $\mathbb{C}[X_1, ..., X_n]$, $P_0, ..., P_m$, decide whether P_0 lies, yes or no, in the ideal generated by $P_1, ..., P_m$ in $\mathbb{C}[X_1, ..., X_n]$ (notice that here again, one can replace $\mathbb{C}$ by any commutative integral domain $\mathbf{A}$). This problem is known as the *membership problem.*

- Given a symetric matrix $[d_{k,l}]_{1\leq k,l\leq n}$ with coefficients in $]0, +\infty[$ and a strictly positive real number d, decide whether, yes or no, there is a cycle σ in the symetric group $\mathcal{S}_n$ such that

$$\sum_{i=1}^{n} d_{i,\sigma(i)} \leq d\,.$$

  One may interpret the matrix $[d_{k,l}]_{1\leq k,l\leq n}$ as a table indicating mutual distances between n cities, which is the reason why this decision problem is known as the *travelling salesman problem.*

As soon as the ring $\mathbf{A}$ can be equipped with a notion of height (such is the case for $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$, $\mathbb{Z}_p$, to which one can also add s transcendental algebraically independent parameters), one may introduce two classes among the category of decision problems over $\mathbf{A}$, namely the P and NP-classes :

- a decision problem (X, X_{yes}) over the ring $\mathbf{A}$ is said to be in the P-class ("P" for "decidable in Polynomial time") if there exists an algorithm that solves it and is such that the M over $\mathbf{A}$ which does the job satisfies

$$\exists q \in \mathbb{N}\,,\ \exists C > 0\,,\ \forall e \in X\,,\ C_M(e) \leq C(L(e) + h(e))^q\,,$$

  where L is the *lenght* function, that is $L(e)$ denotes the number of non zero elements in the input data $e \in \mathbf{A}^l$, $1 \leq l \leq \infty$, and h is the *height* function which was introduced earlier ;

- a decision problem (X, X_{yes}) over the ring $\mathbf{A}$ is said to be in the NP-class ("NP" for "decidable in Non deterministic Polynomial time") if there exist two integers $l, l' \in \mathbb{N} \cup \{\infty\}$, a machine M over $\mathbf{A}$ with input space $E(M)$ such that $X \times \mathbf{A}^{l'} \subset E(M) \subset \mathbf{A}^{l} \times \mathbf{A}^{l'}$ ($\mathbf{A}^{l'}$ playing the role of the probality space) such that

– the machine eventually stops when it is initiated at any (e, ω) in $X \times \mathbf{A}^{l'}$

– $s_M(e, \omega) \in \{0, 1\}$ for any $(e, \omega) \in X \times \mathbf{A}^{l'}$

– $s_M(e, \omega) = 1 \Longleftrightarrow e \in X_{\text{yes}}$

– there exist $q \in \mathbb{N}$, $C > 0$ such that, for any e in X_{yes}, one can find an element $\omega \in \mathbf{A}^{l'}$, such that $s_M(e, \omega) = 1$ and

$$C_M(e, \omega) \leq C(L(e) + h(e))^q \,.$$

A decision problem (X, X_{yes}) over $\mathbf{A}$ is said to be NP-complete if

- on one hand, it lies in the NP-class over $\mathbf{A}$;
- on the other hand, given any problem $(\widetilde{X}, \widetilde{X}_{\text{yes}})$ in the NP-class over $\mathbf{A}$, one can find a map ψ from $\widetilde{X}$ into X such that

  – $\psi(e) \in X_{\text{yes}} \Longleftrightarrow e \in \widetilde{X}_{\text{yes}}$

  – ψ happens to be the restriction to $\widetilde{X}$ of the function s_M which corresponds to some machine M over $\mathbf{A}$ that operates in polynomial time ;

  one can see this second clause as some universal property within the category of decision problems in the NP-class over $\mathbf{A}$.

It is clear that the P-class over $\mathbf{A}$ is a subclass of the NP-class over $\mathbf{A}$. The *travelling salesman problem* appears to be an example of a problem in the NP-class over $\mathbb{R}$ (see [10], proposition 3). On the other hand, very little is known about the natural following question : is the inclusion $P \subset NP$ strict or not ? What is known as the classical logic conjecture $P \neq NP$ is the one that asserts that the class P over $\mathbb{Z}_2$ is strictly included in the NP-class over $\mathbb{Z}_2$; one can also state analog conjectures for rings such as $\mathbb{Z}, \mathbb{C}$,... One could call it the “classical” conjecture when $\mathbf{A} = \mathbb{Z}_2$, the “arithmetic” conjecture when $\mathbf{A} = \mathbb{Z}$, the “algebraic” conjecture when $\mathbf{A} = \mathbb{C}$.

We know from [10] that the *algebraic nullstellensatz* problem is NP-complete over $\mathbb{C}$ (this holds in fact over any commutative field) ; therefore, to prove the conjecture $P \neq NP$ over $\mathbb{C}$ amounts to prove that the *algebraic nullstellensatz* problem over $\mathbb{C}$ cannot be solved (over $\mathbb{C}$) in polynomial time. This remains an open question, which will be the corner stone (it may be better to say the stumbling block) around which the sequel of our talk is organized. Such is the case for the *nullstellensatz problem* over $\mathbb{Z}_2$; the classical conjecture $P \neq NP$ can be reformulated saying that the problem to decide whether a collection of m algebraic equations in n variables with coefficients in $\mathbb{Z}_2$ has a solution (or not) in $(\mathbb{Z}_2)^n$ cannot (generally speaking) be solved in polynomial time.

Another interesting class to which belongs the *algebraic nullstellensatz* problem is the BPP-class (which means it is a decision problem that can be solved by some stochastic machine with some bounded probabilistic risk of error). To be more concrete, given a collection of m polynomials in n variables with complex (resp. integer) coefficients, with degrees bounded by D, there exists a machine over $\mathbb{C}$ (resp. a Turing machine) which allows to test (with a risk of error one can estimate in $D^{-D^{O(n)}}$) whether, yes or no, these polynomials have a common zero in $\mathbb{C}^n$ ([28], section 7.2). One can also underline that the conjecture

$$NP \subset BPP \; is \; a \; false \; assertion$$

(in the classical case, that is $\mathbb{Z}_2$) implies

$$NP \neq P\,.$$

over $\mathbb{C}$. If one keeps in mind that, from the pratical point of view, P and BPP almost represent the same class, one can see why the solution of $NP \neq P$ over $\mathbb{C}$ would provide some hint towards the problem P *versus* NP in the classical case (that is over $\mathbb{Z}_2$). This shows that to settle such problems within some algebrico-analytic ($\mathbf{A} = \mathbb{C}$) or arithmetic ($\mathbf{A} = \mathbb{Z}$) frame may as well give some insight towards the formal problem itself (see [35] for more details or references respect to these various aspects).

2 How far the solution to problems like "nullstellensatz" or "membership" could be effective before 1988 ?

Though "Let's eliminate elimination" appeared either as a joke, either as some kind of advertizing slogan, in mathematics since the fifties, it remains that it was elimination theory (through a method initiated by Hilbert, then developped by Greta Hermann in 1926 [22], for a more modern presentation see also [33]) that provided the first effective solution (and the only one for many years) to the *algebraic nullstellensatz* decision problem over $\mathbb{C}$.

It is well known (since Hilbert) that, given m polynomials $P_1, ..., P_m$ in n variables with coefficients in some field $\mathbf{K}$, the two following assertions are equivalent :

- (i) the polynomials P_j, $j = 1, ..., m$, have no common root in $\overline{\mathbf{K}}^n$, where $\overline{\mathbf{K}}$ denotes some integral closure of the field $\mathbf{K}$;
- (ii) there exist polynomials $Q_1, ..., Q_m \in \mathbf{K}[X_1, ..., X_n]$ such that

$$1 = P_1 Q_1 + \cdots + P_m Q_m \, . \tag{2.1}$$

The proof lies on the following fact : if $p_1, ..., p_M$ are M polynomials in one variable with coefficients in some integral domain $\mathbf{A}$ such that p_1 is monic, the fact that $p_1, ..., p_m$ have a common root in $\overline{\mathrm{Frac}\, \mathbf{A}}$ is equivalent to the fact that the polynomial

$$\mathrm{Sylv}\,(p_1, p_1 + Y_2 p_2 + \cdots + Y_M p_M) \in \mathbf{A}[Y_2, ..., Y_M]$$

(Sylvester resultant of p_1 and $p_1 + Y_2 p_2 + \cdots + Y_M p_M$) is identically zero ; this allows to eliminate variables one after each other ; the best bound one can obtain from this elimination method respect to the degrees of the polynomials Q_j involved in (2.1) (in general) is precisely the bound that was obtained by Greta Hermann, that is

$$\max \deg Q_j \leq 2(2D)^{2^{n-1}} \, , \quad D := \max \deg P_j \, . \tag{2.2}$$

Note that if $D = 2$ and $n = 100$, such a doubly exponential bound is huge $(2 \times 4^{2^{99}})$! This resultat of Greta Hermann, combined with the fact that the search of polynomials Q_j satisfying (2.1) once the degrees have been precised amounts to solve a system of linear equations over $\mathbf{K}$ (this system being compatible, what ensures as a safeguard Hermann's result), shows that though there exists indeed some algorithm to solve the *algebraic nullstellensatz* decision problem over $\mathbb{C}$, the complexity of such an algorithm appears to be doubly exponential. The cost $C_M(e)$ over some input e is controlled in $C \exp(\exp(C(l(e) + h(e))))$ if one goes bact to the lenght and height concepts that we introduced above ; this remains true whether we think about the problem over $\mathbb{C}$ or $\mathbb{Z}$ (that is in algebraic or arithmetic terms), because of the well known linear algebra principle that asserts that any compatible linear system of equations with coefficients in a given field admits necesseraly a solution with coefficients in this field. Looking at the problem over $\mathbb{C}$, the size $L(e) + h(e)$ of an input $e = (P_1, ..., P_m)$ whose coefficients are polynomials in $\mathbb{C}[X_1, ..., X_n]$ with respective degrees $D_1, ..., D_m$ is

$$L(e) + h(e) = 1 + \sum_{i=1}^{m} \binom{n + D_i}{D_i} \ ;$$

looking at the problem over $\mathbb{Z}$, one has also to take into account $h(e)$, which is the maximum of all $\log(1 + |\alpha|)$, where α runs over the family of all non zero coefficients of all the polynomials entries of e (which are in this case in $\mathbb{Z}[X_1, ..., X_n]$).

As for the *membership problem* (of which the Hilbert's zeroes decision problem appears as a by-product), things look at first glance more difficult to get under control from the effectiveness point of view : actually, in 1988, E. Mayr and A. Mayer, in a momentous paper (since it put a final point to some hopes one could have), were able to generate, given any integer $D \geq 5$, any integer $k > 1$, a collection of $10k + 1$ binomials in $10k$ variables, $F_{D,0}, ..., F_{D,10k}$, with integer coefficients, with degrees bounded by D, such as, for any D and any k, X_1 belongs to the ideal $(F_{D,0}, ..., F_{D,10k})$, but

$$X_1 = \sum_{j=0}^{10k} F_{D,j} Q_j \Longrightarrow \max \deg Q_j \geq (D - 2)^{2^{k-1}} \ . \tag{2.3}$$

There was on the other hand already a telescopic example of the same kind (even simpler, which was introduced or re-introduced around 1985 by D.W. Masser and P. Philippon) about the *nullstellensatz problem* itself : whenever D is a strictly positive integer and $P_1, ..., P_n$ are the n polynomials in n variables

$$\begin{aligned} P_1(X) &= X_1^D \ , \ P_2(X) = X_1 - X_2^D \ , ... \\ P_{n-1}(X) &= X_{n-2} - X_{n-1}^D, \ P_n(X) = 1 - X_{n-1} X_n^{D-1} \ , \end{aligned}$$

then

$$1 = P_1 Q_1 + \cdots + P_n Q_n \Longrightarrow \max \deg Q_j \geq D^n - D^{n-1} \ ; \tag{2.4}$$

here is a “negative” example respect to the hope to solve *Hilbert’s zeroes decision problem* within sub-exponential time ; one can also modify such an example taking $P_n := H - X_{n-1}X_n^{D-1}$, where $H \in \mathbb{N}^*, H \geq 2$ and then conclude that there is no hope to find any non zero integer a such that $a = P_1Q_1 + \ldots + P_nQ_n$, $Q_j \in \mathbb{Z}[X_1, ..., X_n]$ and that, at the same time, $\log(|a|+1)$ has less than $D^{n-1}\log H$ as order of magnitude (see [21, 19] for such questions about low bounds, which are also intimely connected with the search for measures of approximation in transcendance theory) ; note that one can even replace D^{n-1} by D^n if one is more careful (see [29], example 3.10).

Anyway, there remains always an important gap between low bounds (2.4) and upper bounds (2.2) respect to the *nullstellensatz* problem over $\mathbb{C}$ or $\mathbb{Z}$. Such a gap does not exist any more if one thinks of the *membership problem* : there is no such gap between upper bounds of the Hermann’s type (2.2) (let us assume here the solution of the *membership problem* can be carried with similar degree estimates, which is not totally evident, since the problem looks harder since it is an algebraic problem than the Hilbert’s zeros problem which is a geometric one) and low bounds (2.3).

3 From the algebraic vision to the geometric or analytic perceptions : the unexpected “discovery” of D. W. Brownawell and J. Kollár

A natural reflex for one who faces the problem to decide whether m polynomials $P_1, ..., P_m$ in n variables with complex coefficients have a common zero or no is to transpose such a question into a problem of geometric nature (which intrinsically it is indeed). Unfortunately, geometric objects are usually more easy to handle (respect to the search for effectiveness, degree bounds, even size estimates,...) in a compact environment, that is working on a compact algebraic variety, than in the affine setting ; natural candidates for the compact environment are the projective space $\mathbb{P}^n(\mathbb{C})$ (dealing with degree estimates to quantify effectiveness) or any toric projective smooth (or at least simplicial) variety associated with some fan whose cones are such their union covers $\mathbb{R}^n$ (dealing with volume estimates of Newton polyedra as quantifiers for the effectiveness), equipped with an action of the torus $\mathbf{T} := (\mathbb{C}^*)^n$ on it.

The concept of *infinity* is achieved in such a compact environment either as some hyperplane in the projective space (namely the hyperplane $\{x_0 = 0\}$ if $[x_0 : \ldots : x_n]$ are taken as the homogeneous coordinates of a point in $\mathbb{P}^n(\mathbb{C})$, the affine space $\mathbb{C}^n$ being the open set $\{x_0 \neq 0\}$), either as a union of supports of toric Weil divisors (indexed by the one-dimensional cones of the fan or, which is the same, by the homogeneous coordinates involved in the homogeneous coordinate ring, attached to the toric variety, [13]) in the toric case. It is important to notice that in either of these two situations, there is another vision of the concept of *infinity*, through the perception of it that would have any observator living in the affine space ($\mathbb{C}^n$ in the first case, $\mathbf{T}^n$ in the second case) ; this alternative vision of infinity seems more in accordance with the analyst's point of view, we will come back to this remark later on.

Let us put ourselves for the moment in the projective context. Polynomials $P_1, ..., P_m$ define m cycles Z_1,...,Z_m in the projective space $\mathbb{P}^n(\mathbb{C})$; decide whether $P_1, ..., P_m$ do have, yes or no, a common zero in $\mathbb{C}^n$ amounts to decide whether, yes or no, the supports of these cycles intersect elsewhere than at infinity.

Intesection theory, such as it has been developped in the proper case, then in the improper case by Fulton [16] or by P. Vogel and more recently the Cracow school (see for example [37]) leads to the definition of an intersection cycle $Z_1 \bullet \ldots \bullet Z_m$; the only elements that appear in such constructions –it is not surprizing since they are of geometric nature– are those that geometry may identify (may be equipped with multiplicities that can be reached as Lelong numbers through analytic tools) ; anything which in the algebraic decomposition of an ideal depends on what we call an *embedded component* will not be taken into account in such a geometric construction or, if it happens to be, it will be in a such a way that dealing with it is controlled by the "geometrically visible" part of the ideal, which corresponds to the isolated primes in its decomposition ; let us recall that if

$$\mathcal{P}_1, ..., \mathcal{P}_s$$

are the prime ideals involved in the decomposition of some ideal (in one of the noetherian rings $\mathbb{C}[x_0, ..., x_n]$, $\mathbb{C}[X_1, ..., X_n]$, or the ring of germs of holomorphic functions in n variables at some point in $\mathbb{C}^n$ for example), the isolated primes correspond to minimal elements (respect to the inclusion) in the family $\{\mathcal{P}_1, ..., \mathcal{P}_s\}$; the union of their zero sets materializes the "visible" part of the ideal, if one thinks in terms of the correspondence ideals *versus* cycles. Control of multiplicities (which appears to be the main ingredient if one thinks about effectivity in terms of degree estimates) in such an intersection process relies basically on Bézout theorem, that is on a multiplicative operation.

Even though one loses (through the construction process of the intersection cycle) some significative part of the algebraic information that carries the structure of the homogeneous ideal generated by the homogeneizations of the P_j, $j = 1, ..., m$, one keeps track of some algebrico-geometric information, lying in the concept of *apparent contour* which was so familiar to geometers (such as Gaspard Monge who formalized it and the Italian algebraic geometry school) or even painters. One of the key concepts that emerged, as soon as one realized it could cost less (from the effectivity point of view) to look for inequalities (as an analyst looking at infinity from the affine space would do) instead of algebraic identities (as one does in classical elimination theory, or thinking about infinity in algebraic terms), was the concept of *Chow ideal* ; such a concept is intimely linked with the geometric concepts of *apparent contour* and *polar varieties.*

Let us recall briefly how the *Chow ideal* of a purely dimensional k-cycle Z, $0 \leq k < n$ in $\mathbb{P}^n(\mathbb{C})$, at a point x of its support. In order to simplify, we will assume that $\mathbb{P}^n(\mathbb{C})$ is replaced by some local chart $U \subset \mathbb{C}^n$ about the origin (corresponding to a neighborhood of x in $\mathbb{P}^n(\mathbb{C})$). Suppose $Z = \sum_j \alpha_j C_j$ and let $|Z|$ be the support of Z, that is the union of irreducible analytic subsets C_j. Let π be a linear surjective map from $\mathbb{C}^n$ to $\mathbb{C}^{k+1}$ such that $\underline{0}$ is an isolated point in $\operatorname{Ker}\pi \cap |Z|$ (such a map π is called an *admissible projection*) ; there exists a neighborhood W of $\underline{0}$ in $\mathbb{C}^n$ such that the restriction of π to $W \cap |Z|$ is a proper map from $W \cap |Z|$ into $\pi(W)$. One can associate to any irreducible component C_j that contains $\underline{0}$ a positive integer μ_{π, C_j} which is the number of sheets of the covering

$$\pi_{|C_j \cap W} : \; C_j \cap W \mapsto \pi(W)$$

(such a number μ_{π, C_j} can be as well understood in analytic terms as a Lelong number). Then, by Remmert's theorem, the projection $\pi(C_j \cap W)$ is a k-dimensional analytic subset of $\pi(W)$, that is an hypersurface, which can be defined by some irreducible equation f_{π_j} in $\pi(W)$ (in a neighborhood of $\underline{0}$) ; one can lift up to W such an equation and define some analytic function in W (which may have been somehow restricted) as

$$F(\pi, z): \ z \mapsto \prod_j f_{\pi_j}(\pi(z))^{\alpha_j \mu_{\pi, c_j}} .$$

Considering all possible *admissible projections*, one constructs an ideal in the ring of germs of holomorphic functions at the origin in $\mathbb{C}^n$ (namely the ideal generated by all the germs of the different $F(\pi, \cdot)$ as π runs over the set of all *admissible projections*) ; this is the so called *Chow ideal* of the cycle C at x (or at least its transcription in a local chart about x).

In particular, one can associate to the cycle $Z_1 \bullet \ldots \bullet Z_m$ the ideal sheaf

$$\mathcal{I}(Z_1 \bullet \cdots \bullet Z_m)^{\mathrm{chow}}$$

on $\mathbb{P}^n(\mathbb{C})$; the partial return from this algebrico-geometric object to the algebraic object which consists in the ideal sheaf

$$(\mathcal{I}(Z_1), ..., \mathcal{I}(Z_m))$$

is realized thanks to a result due to Ewa Cygan [14] that one may formulate in two different ways, one of algebraic nature, the other one of analytic nature :

- At any point x in the intersection of the supports of the m cycles Z_j, $j = 1, ..., m$, the ideal $\mathcal{I}_x^{\mathrm{chow}}(Z_1 \bullet \cdots \bullet Z_m)$ lies in the integral closure of the ideal generated by the different $\mathcal{I}_x(Z_j)$, $j = 1, ..., m$;
- whenever $(p_{x,j,l})_l$ denotes, for any $j = 1, ..., m$, a set of generators for the ideal $\mathcal{I}_x(Z_j)$, $j = 1, ..., m$, there exist $C_x > 0$, W_x neighborhood of x in $\mathbb{P}^n(\mathbb{C})$, such that

$$\forall y \in W_x, \ \max_{j,l} |p_{x,j,l}(y)| \geq C_x d(y, |Z_1| \cap \ldots \cap |Z_m|)^{\deg (Z_1 \bullet \cdots \bullet Z_m)} .$$

As we already mentionned it, Bézout theorem implies that if

$$D_1 \geq D_2 \geq \cdots \geq D_m$$

are the respective degrees of the polynomials $P_1, ..., P_m$, the degree of the intersection-cycle $Z_1 \bullet \cdots \bullet Z_m$ is bounded from above by $D_1 \cdots D_{\min(n,m)}$, which implies that one has also, for any x in the intersection of the supports of the m cycles Z_j, $j = 1, ..., m$, and the $p_{x,j,l}$, $j = 1, ..., m$, C_x and W_x as above

$$\forall y \in W_x,\ \max_{j,l} |p_{x,j,l}(y)| \geq C_x d(y, |Z_1| \cap \ldots \cap |Z_m|)^{D_1 \cdots D_{\min(n,m)}} .$$

It was another result, of more analytic nature, that was used by D. W. Brownawell in 1988 to complete such a picture and show that there exists an algorithm within simply exponential time (instead of doubly exponential time) in order to solve the decision *nullstellensatz* problem over $\mathbb{C}$. As we mentionned it in Ewa Cygan's result (first formulation), the notion of *integral closure* of an ideal is deeply connected with the "analytic perception" of this ideal, namely its *Chow ideal.* Let us recall this notion of *integral closure* : given a commutative ring $\mathbf{A}$ and some ideal I, an element $a \in I$ belongs to the *integral closure* of I in $\mathbf{A}$ (this is also an ideal somewhere between I and its radical) if and only if a satisfies some relation of integral dependency of the form :

$$a^N + y_1 a^{N-1} + \cdots + y_N = 0\,, \quad y_j \in I^j\,,\ j = 1, ..., N\,, \quad N \in \mathbb{N}^*\,.$$

Whenever $\mathbf{A}$ is a regular local ring with dimension k and I is any ideal in A, the integral closure of I^k lies in I (moreover, for any $p \in \mathbb{N}^*$, the integral closure of I^{k+p-1} lies in I^p). When $\mathbf{A}$ is the ring $\mathcal{O}_n$ of germs of holomorphic functions at the origin in $\mathbb{C}^n$ and I is generated by monomials, this result is an easy consequence of Caratheodory's theorem which asserts than, in any affine n-dimensional real space, any element in the convex enveloppe of a subset can be realized as a barycentric combination of at most $n+1$ elements from this subset. Which means that it is (in this very particular case) a result from convex analysis which helps to build the expected bridge between the realization of inequalities of analytic nature (such as in the second formulation of E. Cygan's theorem) and that of algebraic identities (such as the effectiveness of the membership of one element to an ideal). What is very deep is that this key result about the integral closure of a monomial ideal has been extended to any ideal in the ring $\mathcal{O}_n$ by Joël Briançon et Henri Skoda en 1974 [9], and seven years later, transposed to the more general setting of ideals in regular local rings by J. Lipman, B. Teissier, A. Sataye en 1981 [31, 30] (note that the arguments used in [31] are inspired by analytic ideas and that there does not exist yet any crystal-clear proof, let say for example a proof inspired by combinatorics arguments, of the fundamental, but somehow mysterious, Lipman-Sataye-Teissier theorem.

The result obtained by D. W. Brownawell in 1988 in [8] can be stated as follows : given m polynomials in $\mathbb{C}[X_1, ..., X_n]$ with respective degrees $D_1 \geq D_2 \geq \cdots \geq D_m$ without any common zero in $\mathbb{C}^n$, there exist m polynomials $Q_1, ..., Q_m$ with degree at most $nD_1 \cdots D_{\min(n,m)}$ such that

$$1 = P_1 Q_1 + \ldots + P_m Q_m \, . \tag{3.5}$$

Note that the factor n here comes from Briançon-Skoda's theorem. A similar result (with a proof based on the use of cohomology with supports, which was also later rephrased by P. Philippon using as main tool the notion of Koszul complex) was obtained one year later by J. Kollár : when $P_1, ..., P_m$ define a proper ideal in $\mathbb{C}[X_1, ..., X_n]$, one can always achieve (3.5) with Q_j which degrees are bounded from above by

$$\prod_{j=1}^{\min(n,m)} \max(3, D_j) \, .$$

It follows that the *Hilbert's zeroes* decision problem over $\mathbb{C}$ can always be solved within simply, instead of double, exponential time ; upper bounds essentially fit with lower bounds (2.4). Such a result came as a surprize since the Mayr-Meyer example seemed to close the possibility to get under the upper bounds (2.2) that were suggested by G. Hermann. It could also have come as good news towards a proof that the *nullstellenstatz* decision problem could be in the P-class over $\mathbb{C}$; this did not really happen to be the case, since different hints (issued from the arithmetic or algorithmic point of view) are in favor of the fact that it is not (so that $P \neq NP$ over $\mathbb{C}$ would be true). Nevertheless, the fundamental results of D. W. Brownawell and J. Kollár, which are also presented in some revisited form in [26, 23] (in the light of new developments in intersection theory which occured in the nineties), became the motivation for a lot of questions, which were linked in particular to the transposition of these results to the arithmetic setting, that is when $\mathbf{A}$ is a commutative infinite ring equipped with a notion of height (such as $\mathbb{Z}, \mathbb{Z}[x_1, ..., x_s], \mathbb{Z}_p[x_1, ..., x_s]$). We will develop results in such directions in the next section.

As for the *membership* problem over $\mathbb{C}$, respect to its complexity, it seems inexorably knock against lower bounds involved in the Mayr-Meyer example.

Nevertheless, the Euclidean division algorithm found its accomplishment in Buchberger's method (developped around 1970), leading to the construction, for any ideal in $\mathbf{K}[X_1, ..., X_n]$, $\mathbf{K}$ being a commutative field and the set of monomials being equipped with some ordering structure (such as the lexicographic one), of a *standard base* (or *Gröbner base*) for the ideal (for an introduction to these notions, see for example [12] or [1]).

Therefore, since the knowledge of a standard basis for some ideal I implies the possibility to solve at once any division problem where only I is involved (for example decide if, yes or no, some given polynomial Q belongs to I, that is answer to the *membership problem*), it is clear that Mayr-Meyer's example shows that one cannot give in general a reasonable control on the complexity of Buchberger's algorithm. Nevertheless, it is important to underline how ideas which, since the early seventies, were key tools in the algorithmic carrying out of Weierstrass division theorem (see A. Galligo's thesis in 1973 [17]) have also played a fundamental role, as much from the point of view of formal calculus than geometry of singularities ; the same ideas where also those which subtend Hironaka's proof in 1969 of resolution of singularities in characteristic zero (in the algebraic and analytic settings).

One should also mention, respect to the *membership problem* over $\mathbb{C}$, that very recently, M. Hickel in [23], refining an anterior result due to F. Amoroso [2], proved that if $P_1, ..., P_m \in \mathbf{C}[X_1, ..., X_n]$ were m polynomials with respective degrees $D_1 \geq \cdots \geq D_m$ and $Q \in (P_1, ..., P_m)$, then one can find m polynomials $Q_1, ..., Q_m$ such that

$$Q^n = P_1 Q_1 + \ldots + P_m Q_m$$

with

$$\max \deg Q_j \leq n(\deg Q + D_1 \cdots D_{\min(n,m)}) \,.$$

Such a result shows again the strenght of Briançon-Skoda's theorem ; though simply exponential bounds cannot be reached for the effectiveness of the membership, it is always possible to express Q^n in the ideal $(P_1, ..., P_m)$ with simply exponential degree estimates for the Q_j's as soon as Q lies locally in the integral closure of the ideal I, that is when the analytic inequality

$$|Q(z)| \leq C(z) \max_{1 \leq j \leq m} |P_j(z)|$$

is valid in $\mathbb{C}^n$ for some locally bounded function C.

4 How interpolation and duality tools can be used towards solving Hilbert's zeroes problem

Two brilliant ideas (also and even mainly developped in applied mathematics) put under a new light (within the decade 1990-2000) algebraic or arithmetic questions relative to the solution of the two decision problems (*nullstellensatz* and *membership*) we mentionned in previous sections. One should better speak about the "rediscovery" of a whole circle of ideas that had been extensively developped between the end of the ninetieth century or and the beginning of the twentieth century by mathematicians such as Cayley, Kronecker, Jacobi or Macaulay. O. Netto's treatise of algebra [34] contains moreover a lot of ideas that one will find exploited again almost one century later. These two ideas are

- Lagrange's interpolation formula (used as a division formula as well as an interpolation formula) ;
- the duality principle (which lies also behind basic concepts in applied mathematics such those of distributions and currents) ; one should also mention the geometric concept of *polarization*, which appears as another realization of such a duality principle and that Radon transform illustrates so well in the applied field.

Lagrange's interpolation formula provides an alternative solution to the resolution of Bézout identity in $\mathbb{C}[X]$ (besides the classical euclidean algorithm) ; if P_1 and P_2 are two polynomials in $\mathbb{C}[X]$ without common zero in $\mathbb{C}$, then

$$1 = P_1 \mathcal{L}_{P_2}(1/P_1\,;\,\cdot) + P_2 \mathcal{L}_{P_1}(1/P_2\,;\,\cdot)\,,$$

where $\mathcal{L}_{P_j}(1/P_i\,;\,\cdot)$ is the Lagrange interpolator $1/P_i$ at the zeroes (which may be multiple) of the polynomial P_j $(i \neq j)$. As for Cauchy's formula (or more generally in higher dimensions Cauchy-Fantappié formula),

$$f(z) = \frac{1}{2i\pi} \int_{|\zeta - z| = \epsilon} \frac{f(\zeta)d\zeta}{\zeta - z}\,,$$

one can think about it as a duality formula (note that the concept of polarization lies besides the interpretation of Cauchy-Fantappié transforms) ; the basic Cauchy formula in one variable may be rewritten as

$$\langle \delta(z), f\rangle = \mathrm{Res}\left[\begin{matrix} f(\zeta)d\zeta \\ \zeta - z\end{matrix}\right],$$

so that the action of the Dirac mass at the point z on the test-object f can be expressed as the action on the test-object $f(\zeta)d\zeta$ of the *residual symbol*

$$\mathrm{Res}\left[\begin{matrix} \cdot \\ (\cdot) - z\end{matrix}\right]$$

(such an action happens to be materialized –but this is only the analytic materialization of some true algebraic object– by the computation of a path integral).

A second idea (also attributed to Lagrange) that one can aloso formulate in such a formalism inspired by the duality concept is the following : whenever P and Q are two polynomials in $\mathbb{C}[X]$ such that $\deg Q < \deg P - 2$, then

$$\mathrm{Res}\left[\begin{matrix} Q(\zeta)d\zeta \\ P\end{matrix}\right] = 0\,.$$

One can re-read such a fact (thinking now in terms of differential geometry) saying that the total sum of residues of the meromorphic differential form $Q/Pd\zeta$ on the compact algebraic variety $\mathbb{P}^1(\mathbb{C})$ equals zero (note that this is also a consequence of Stokes's theorem) ; such a result becomes an index theorem, that already Jacobi in [24] knew how to transpose to a (still geometric) multi-dimensional setting.

It is a combination of such various ideas which could be used as soon as 1991 to provide some arithmetic solution to the *Hilberts's zeroes* decision problem ([5], [6]) ; such a solution gave an estimate (which was not optimal, but on the way to be) respect non only to degrees, but also to heights, when the problem was settled over some infinite integral unitary domain $\mathbf{A}$ that could be equipped with a notion of (logarithmic) height : whenever $P_1, ..., P_m$ are m polynomials in $\mathbf{A}[X_1, ..., X_n]$ without common zeroes in some integral closure of Frac $\mathbf{A}$, with total degree at most D, there exist m polynomials $Q_1, ..., Q_m$ in $\mathbf{A}[X_1, ..., X_n]$, with degrees at most $n(2n+1)D^n$, some element $a \in \mathbf{A}^*$ such that

$$\max(h(a), h(Q_j)) \leq \kappa(n) D^{4n+2}(h + \log m + D)$$

and

$$a = \sum_{j=1}^{m} P_j \, Q_j \, ,$$

where h denotes the maximum of the logarithmic heights of all coefficients involved in the input data P_j, $j = 1, ..., m$.

The progressive elaboration (since 1990) of the logarithmic height concept, together with the active development of arithmetic intersection theory following the pionnier work of S. J. Arakelov [3], lead to the search for optimality in the control of the effectiveness of the arithmetic *nullstellensatz* ; the last step came very recently, and got to its achievement with the very recent work of T. Krick, Luis-Miguel Pardo et Martín Sombra [29] ; their result refines the estimate for the maximal degrees of the Q_j, which now becomes

$$\max \deg Q_j \leq 4nD^n \, ,$$

as well as the height estimates (now nearly optimal if one compares them to the lower bounds $D^{n-1} \log H$ for the telescopic Masser-Philippon example suggested at the end of section 2) :

$$\max(h(a), h(Q_j)) \leq 4n(n+1)D^n(h + \log m + (n+7)\log(n+1)D) \, .$$

Arithmetic intersection theory, such as developped by G. Faltings, then J. B. Bost, H. Gillet, C. Soulé [15, 18, 7], appears as a good illustration of the complementarity between arithmetic, geometry and analysis ; such a complementarity is already inherent in a well known formula, the *product formula* : if $| \cdot |_p$, p prime, denotes the ultrametric absolute value on $\mathbb{Q}$ normalized such that

$$|m/n|_p = p^{-\nu_p(m)+\nu_p(n)} \, ,$$

where $\nu_p(k)$ means the exponent of p within the prime factorization of the positive integer $|k|$, one has, for any non zero rational number x,

$$\prod_{p \text{ premier}} |x|_p = \frac{1}{|x|_\infty} \, ,$$

where $| \cdot |_\infty$ denotes the usual (archimedian) absolute value on $\mathbb{Q}$; such a formula can be re-written

$$\Big(\prod_{p \text{ premier}} |x|_p \Big) \times |x|_\infty = 1 \, .$$

The first factor here is of arithmetic nature, the second one of analytic nature. The same kind of complementarity may be also suggested by some crucial formula in pluricomplex potential theory, namely Jensen's formula : if P is an element in $\mathbb{C}[X]$,

$$P(X) = |a_0| \prod_{j=1}^{n} (X - \alpha_j)\,,$$

then

$$\frac{1}{2i\pi} \int_0^1 \log |P(e^{2i\pi\theta})| d\theta = \log |a_0| + \sum_{j=1}^{n} \max(0, \log |\alpha_j|)\,;$$

here again, whenever P is a polynomial with integer coefficients, the left-hand side of this identity reflects some analytic information, while the right-hand side (that one can express, thanks to the product formula transposed from $\mathbb{Q}$ to the more general setting of a number field, in terms of ultrametric absolute values) carries an information of arithmetic nature. One should also notice that, whenever P is an homogeneous polynomial in $\mathbb{C}[X_0, ..., X_n]$ with degree D, the function

$$\log |P|^2$$

(which plays a role in Jensen's formula in the one-dimensional setting) appears as a solution og Green's equation

$$dd^c \log |P|^2 + [Z(P)] = D\omega\,,$$

where ω denotes the volume form in the projective space $\mathbb{P}^n(\mathbb{C})$ and $[Z(P)]$ denotes the integration current (multiplicities been taken into account) on the projective hypersurface $\{P = 0\}$, which amounts to another important formula (which one also needs to transpose to the multi-variate case and to read on $\mathbb{P}^n(\mathbb{C})$ instead than in the affine setting), namely the following : if $P \in \mathbb{C}[X]$ admits $\alpha_1, ..., \alpha_s$ (with respective multiplicities $\mu_1, ..., \mu_s$) as roots in $\mathbb{C}$, then, one has, in the sense of distributions, Lelong-Poincaré formula, that is

$$\Delta \log |P(z)| = 2\pi \sum_{j=1}^{s} \mu_j \delta_{\alpha_j}\,,$$

where δ_{α_j} denotes the Dirac mass at the point α_j and Δ the Laplace operator. In order to compute the logarithmic height of some arithmetic cycle with codimension k in $\operatorname{Proj} \mathbb{Z}[X_0, ..., X_n]$, one needs to intersect it with a generic projective subspace U which is defined in homogeneous coordinates $[x_0 : ... : x_n]$ as

$$U := \{\langle u^0, x\rangle = \cdots = \langle u^{n-k}, x\rangle = 0\}\,,$$

where the u_l are generic integer coefficients ; one gets that way a 0-dimensional arithmetic cycle

$$\sum_{\tau\,,\tau \text{ premier}} n_\tau\, \{\tau\}\,,$$

whose logarithmic height will be defined as

$$\sum_\tau n_\tau \log \tau\,;$$

in order to balance such an arithmetic contribution and define some notion of logarithmic height that could be intrinsic (that is independent of U), one needs to add to this arithmetic expression the (analytic) contribution

$$\frac{1}{2}\int_U G_Z$$

where G_Z denotes a $(k-1, k-1)$-current, with sngular support contained in the support of Z, orthogonal to harmonic forms, and moreover solution of Green's equation

$$dd^c G_Z + [Z] = (\deg Z)\, \omega^k\,,$$

where $[Z]$ means the integration current (multiplicities been taken into account) on the cycle Z (thought now as a geometric cycle instead of an arithmetic cycle). The logarithmic height of the arithmetic cycle Z is then defined as

$$\sum_\tau n_\tau \log \tau + \frac{1}{2}\int_U G_Z + \frac{\deg Z}{2}\sum_{j=k}^{n}\sum_{l=1}^{j}\frac{1}{l}\,.$$

This is the height notion that one can put in the machinery leading to effectiveness in the solving of Bézout identity in the arithmetic (instead of geometric) setting, that is over $\mathbb{Z}$ instead than over $\mathbb{C}$. The key point about such a notion of logarithmic height is that it leads to an arithmetic formulation of Bézout's theorem : the logarithmic height of the intersection of two arithmetic cycles Z_1 and Z_2 (one such an intersection has been conveniently defined) is bounded from above by

$$\deg Z_1\; h(Z_2) + \deg Z_2\; h(Z_1) + \kappa(\operatorname{codim} Z_1, \operatorname{codim} Z_2)\, \deg Z_1\, \deg Z_2\,.$$

Such a fundamental result plays a basic role respect to effectivity results related to the solution of the *nullstellensatz problem* over $\mathbb{Z}$. What we wanted mainly to point out through this very short presentation of concept of logarithmic height was the evident complementarity between the analytic and arithmetic points of view ; in fact, one should better say between the geometric and arithmetic points of view, since the concept of Green's current we just introduced appears to be intimately related to the contruction of metrics on fiber bundels, in the spirit of the theory which was lined up by S. J. Arakelov within the setting of algebraic curves.

5 Back to complexity problems

The fact that we have by now at our disposal quasi-optimal versions concerning the effectiveness of Hilbert's zeroes theorem, from the geometric point of view and arithmetic point of view as well (in terms of a good control on degrees or logarithmic heights as soon as the problem is settled over a ring **A** equipped with some notion of height, either naive or more elaborate) happens to be only indirectly linked the question whether there could exist (yes or no) a machine which could be able to solve such decision problems within polynomial time.

Nevertheless, the fact that we know low bounds for degree or logarithmic size estimates for the effective resolution of Bézout identity could give some hint towards the idea that the *Hilbert's zeroes problem* is not in the P-class over $\mathbb{C}$. We will refer later to more algorithmic hints towards the same direction.

Let us precise here a different point of view, more phrased in terms of complexity. M. Shub and S. Smale proved in [36] that the *Hilbert's zeroes problem* over $\mathbb{C}$ being in the P-class would reflect on the complexity of a very familiar sequence of integers, the sequence $(k!)_{k\geq 1}$. We need first to give a definition :

Définition 5.1 *A sequence of integers $(a_k)_{k\geq 1}$ is said to be "easy to compute" if and only if there exists a sequence of "denominators" $(m_k)_{k\geq 1}$, an integer q, such that there exists, for any $k = 1, ...,$ a finite sequence of integers $(x_{k,l})_{0\leq l\leq N_k}$, with*

- $x_{0,k} = 1$
- $x_{N_k,k} = m_k a_k$

- $N_k \leq (\ln k)^q$
- *any* $x_{l,k}$*,* $1 \leq l \leq N_k$ *can be computed as* $x_{l,k} = x_{i,k} \bullet x_{j,k}$*, with*

  $$0 \leq i, j < l$$

  and $\bullet$ *means one among the three basic operations that are addition, substraction and multiplication.*

M. Shub et S. Smale's result in [36] may be stated as follows :

Théorème 5.1 *If the Hilbert's zeroes decision problem over* $\mathbb{C}$ *was in the* P*-class, then the sequence* $(k!)_{k\geq 1}$ *would be easy to compute.*

Such a notion of "simplicity" for a numerical sequence will lead us to some different interpretation of questions connected with effectivity of problems such as the *Hilbert's zeroes* decision problem.

What we did up to now (listing the results of D. W. Brownawell, J. Kollár, C. A. Berenstein and A. Yger, T. Krick, L.M. Pardo and M. Sombra) was to speak about effectivity mentionning in such problems (Bézout identity, membership) how the degrees (or the logarithmic heights) of the outputs were controlled in terms of the degrees (or the degrees and the logarithmic heights) of the input data. Such estimates imply a bound from above for the cost of a machine solving the corresponding decision problem, either using a linear algebra argument (as soon as degree estimates are known, one knows which linear system of equations to solve) or a direct formula as in [5, 6] based generally speaking on a duality argument (such as multivariate residue calculus). There are indeed over quantifiers in order to "measure" the complexity of some input which consists of a matrix of polynomials in n variables with coefficients either in $\mathbb{C}$ either in $\mathbb{Z}$ (or more generally in some ring $\mathbf{A}$ that one can equip with a logarithmic height) : for example, the convex hull of the supports of these polynomials (that is the convex hull in $(\mathbb{R}^+)^n$ of the set of points in $\mathbb{N}^n$ corresponding to multi-exponents of monomials which appear in the polynomial expressions) may be a quantifier much more precise than the degree.

Another trick one can use to code the complexity of system of polynomial inputs is to code the process itself of construction, then of evaluation, of the different entries of the system : for example the polynomial

$$X^{2^{2^n}} - 1 \in \mathbb{Z}[X]$$

is quite easy to code this way, iterating the process $X \mapsto X^2$ 2^n times, though it has a doubly exponential degree ! Such an idea arose in the seventies, through the works of J. Heintz, J. Morgenstern, C. P. Schnorr,..., and intensively developped since then ; one can for example refer to the references [27, 20, 19] in order to find both a presentation and a prospective outlook about the role such an approach could have respect to diophantine approximation questions (note that the different works of D. W. Brownawell, D. W. Masser, P. Philippon, C. A Berenstein and A. Yger, F. Amoroso we mentionned before took their motivations precisely around such questions).

The key notion here is the concept of *straight line program* with parameter system $\mathcal{F}$; such a concept is inspired by the notion of "simplicity" (in the sense it is easy to compute) of a numerical sequence. Such a program consists in the following data : a graph $\mathcal{G}$, paired with a list of instructions (all of them defining some kind of protocol) one for each different entry gate of the graph (let $\mathcal{Q}$ be such a list of instructions). If one works with a prescribed number of variables n, the graph will present $n+1$ entry gates labelled as $X_1, ..., X_n$ and 1. The *depth* of a node ν of $\mathcal{G}$ denotes the length of the longest path from ν till one of the entry gates. One can label the nodes of the graph by pairs (i,j), where i means the *depth* of the node and j another parameter which is used to classify (in the lexicocraphic order $<_{\rm lex}$) nodes with depth equal to some prescribed value i ; to each gate (i,j), one may associate some operation

$$Q_{i,j} = \Big(\sum_{(r,s)<_{\rm lex}(i,j)} A_{i,j}^{r,s} Q_{r,s}\Big)\Big(\sum_{(r,s)<_{\rm lex}(i,j)} B_{i,j}^{r,s} Q^{r,s}\Big)\,,$$

where $A_{i,j}^{r,s}$, $B_{i,j}^{r,s}$ are intermediate variables, so-called *parameters* of the program, the $Q_{r,s}$, $Q^{r,s}$ being polynomials pre-calculated at the nodes (r,s) of the graph anterior to the node (i,j). A polynomial f with integer coefficients is said to be evaluated by such a program (parameters being taken in some subset $\mathcal{F}$ of $\mathbb{Z}$) if there exist a node (i,j) and some choices of parameters $A = (A_{k,l}^{r,s})$ and $B = (B_{k,l}^{r,s})$, with $(r,s) <_{\rm lex} (k,l) <_{\rm lex} (i,j)$ such that

$$f(X_1, ..., X_n) = Q_{i,j}(A, B, X_1, ..., X_n)\,.$$

One may define then the *size* s of the program (this is the size of the graph), its *depth* d (this is the depth of the graph), and eventually, if $\mathcal{F}$ is a finite subset of $\mathbb{Z}$ which has been precised since the beginning, the *height* of the program as the maximum of the naive logarithmic heights of all elements in $\mathcal{F}$.

One can solve then *Hilbert's zeroes* decision problem for example in the following algorithmic terms (see [28]) : if $P_1, ..., P_m$ are m-polynomials in n indeterminates with integer coefficients, with degree less than $D \geq n$, and logarithmic height less than h, there exists $Q_1, ..., Q_m \in \mathbb{Z}[X_1, ..., X_n]$ and $a \in \mathbb{Z}^*$ (which can be evaluated by a *straight line program* with size, depth, height, respectively bounded by $md^{O(n)}$, $O(n \log D)$, $\max(D^{0(n)}, h)$) such that

$$a = P_1 Q_1 + \ldots P_m Q_m .$$

One could as well ask the same question (is there such $a, Q_1, ..., Q_m$?) assuming that entries $P_1, ..., P_m$ are also obtained through *straight line programs* evaluations (the size, the depth and the height being respectively bounded by s, d, h for the *straight line programs* which are concerned) ; can one estimate, in terms of s, d, h, and other geometric parameters such as the affine degree δ or algebraic such as the maximum of the degrees D, the lenght, the depth or the height of a *straight line program* that allows the possibility to evaluate polynomials Q_j involved in an algebraic identity which could allow to test whether the answer to the decision problem is yes or no ? Yes, sometimes, if we add some geometric constraint : for example, if $P_1, ..., P_n$ are n polynomials defining a discrete (hence finite) algebraic variety in $\mathbb{C}^n$, there exists, for any $j \in \{1, ..., n\}$, a *straight line program* with length in $(nD\delta s)^{O(1)}$, with logarithmic height in $O(n(\log(nD) + d) \log \delta)$ which allows to evaluate some polynomial $P \in \mathbb{Z}[X_j]$ vanishing at all common zeroes of $P_1, ..., P_n$ in $\mathbb{C}^n$.

We should mention here that it has been recently proved (see [11]) that any elimination procedure with natural universal properties inherits (in the algorithmic terms we just mentionned) from a complexity at least simply exponential. Any known elimination procedure leading to optimality in the algorithmic approach appears to be based on the algorithmic elimination "*a la Kronecker*" (or multivariate residue calculus, which amounts basically to the same thing), even though it may use intensively other duality ideas (such as polarization for example in [4]). Could not be that some hint towards an algorithmic formulation of the statement $P \neq NP$ over $\mathbb{C}$?

Let us point out as a conclusion to this lecture that mathematical ideas that were pushed up to reach the optimal result of Krick-Pardo-Sombra [29] seem by now get close to their limits. One could guess that it is now time to think about such complexity questions in terms of informatics (more precisely in terms of programming language or pure logic). The ball's now in the court of formal calculus specialists and one could hope new ideas coming from such world will lead to new progress respect to some key questions in diophantine analysis which remain unsolved, such as the well known Schanuel's conjecture (which would imply in its simplest cases, that is in dimension two, the algebraic independence over $\overline{\mathbb{Q}}$ of e and π, or $\log 2$ and $\log 3$). Here again, one could hope that analysis or geometry would play, as it has been already the case, but up to now unsuccessfully, the same role of "stimulus" it played respect to effectivity or complexity problems that lie behind questions related to such decision problems as *nullstellensatz* or *membership* over $\mathbb{C}$ or $\mathbb{Z}$.

References

[1] W. Adams, Ph. Loustaunau, *An introduction to Gröbner bases*, American Mathematical Society, Providence, 1994.

[2] F. Amoroso, On a conjecture of C. Berenstein and A. Yger, Proc. Mega'94, *Algorithms in algebraic geometry and applications*, Progress in maths 143, Birkäuser, 1996, 17-28.

[3] S. J. Arakelov, Intersection theory of divisors on an arithmetic surface, Math USSR Izv. 8, 1974, 1167-1180.

[4] B. Bank, M. Giusti, J. Heintz, G. Mbakop, Polar varieties and efficient real elimination, manuscript, January 2000.

[5] C. A. Berenstein, A. Yger, Effective Bézout identities in $\mathbb{Q}[z_1, ..., z_n]$, Acta Math. 166, 1991, 69-120.

[6] C. A. Berenstein, A. Yger, Residue Calculus and effective Nullstellensatz, American Journal of Mathematics, 121, 4, 1999, 723-796.

[7] J.-B. Bost, H. Gillet, and C. Soulé, Heights of projective varieties and positive Green forms, J. Amer. Math. Soc. 7, 1994, 903-1027.

[8] D. W. Brownawell, Bounds for the degrees in the Nullstellensatz, Ann. of Math. 126, 1987, 577-591.

[9] J. Briançon, H. Skoda, Sur la clôture intégrale d'un idéal de germes de fonctions holomorphes en un point de $\mathbf{C}^n$, Comptes Rendus Acad. Sci. Paris, série A, 278, 1974, 949-951.

[10] L. Blum, M. Shub, S. Smale, On a theory of computation and complexity over the real numbers : NP-completeness, recursive functions and universal machines, Bulletin American Math. Soc, 21, 1, 1989, 1-46.

[11] D. Castro, M. Giusti, J. Heintz, G. Matera, L. M. Pardo, Universal elimination requires exponential running time, *manuscript*, 2000.

[12] D. A. Cox, J. Little, D. O'Shea, *Ideals, varieties and algorithms : an introduction to computational algebraic geometry and commutative algebra*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[13] D. A. Cox, The homogeneous coordinate ring of a toric variety, J. Algebraic Geom. 4, 1, 1995, 17-50.

[14] E. Cygan, Intersection theory and separation exponent in complex analytic geometry. Ann. Polon. Math. 69, 3, 1998, 287-299.

[15] G. Faltings, Diophantine approximation on Abelian varieties, Ann. of Math. (2) 133, 1991, 549-576.

[16] W. Fulton, *Intersection theory*, second edition, Springer-Verlag, 1998.

[17] A. Galligo, Sur le théorème de préparation de Weierstrass pour un idéal de $k[x_1, ..., x_n]$, *Singularités à Cargèse*, Astérisque 7 et 8, SMF, Paris, 1973, 165-169.

[18] H. Gillet, C. Soulé, Arithmetic intersection theory, Inst. Hautes Études Sci. Publ. Math. 72, 1990, 93-74.

[19] M. Giusti, J. Heintz, K. Hägele, J. E. Morais, L. M. Pardo, J. L. Montaña, Lower bounds for diophantine approximations, Journal of Pure and Applied Algebra 117 & 118, 1997, 217-307.

[20] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, L. M. Pardo, Straight-line programs in geometric elimination theory, Journal of Pure and Applied Algebra 124, 1998, 101-146.

[21] J. Heintz, J. Morgenstern, On the intrinsic complexity of elimination theory, J. Complexity 9, 1993, 471-498.

[22] G. Hermann, Die Frage der endlich vielen Schritte in der theorie der polynomideale, Math. Ann. 95, 1926, 736-788.

[23] M. Hickel, Solution d'un conjecture de C. Berenstein et A. Yger et invariants de contact à l'infini, Ann. Inst. Fourier (Grenoble) 51 (2001), no. 3, 707-744.

[24] C. Jacobi, Theoremata nova algebraica circa systema duarum aequationum inter duas variabiles propositarum, Crelle Journal für die reine und angewandte Mathematik, Bd. 14. p. 281-288, 1835.

[25] J. Kollár, Sharp effective Nullstellensatz, J. Amer. Math. Soc. 1, 1988, 963-975.

[26] J. Kollár, Effective Nullstellensatz for arbitrary ideals. J. Eur. Math. Soc. (JEMS) 1, 1999, no. 3, 313–337.

[27] T. Krick, L. M. Pardo, Une approche informatique pour l'approximation diophantienne, C.R. Acad. Sci. Paris, série A, 318, 1994, 407-412.

[28] T. Krick, L. M. Pardo, A computational method of diophantine approximation, Proc. Mega'94, *Algorithms in algebraic geometry and applications*, Progress in maths 143, Birkäuser, 1996, 193-253.

[29] T. Krick, L. M. Pardo, M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, Duke Math. J. 109 (3), 2001, 521-598.

[30] J. Lipman, A. Sathaye, Jacobian ideals and a theorem of Briançon-Skoda, Michigan Math Journal 28, 1981, 199-222.

[31] J. Lipman, B. Teissier, Pseudo-rational local rings and a theorem of Briançon-Skoda about integral closures of ideals, Michigan Math. J. 28, 1981, 97-116.

[32] E. Mayr et A. Meyer, the complexity of the word problem for commutative semi-groups and polynomial ideals, Adv. in Math. 127, 1988, 305-329.

[33] D. W. Masser, G. Wüstholz, Fields of large transcendance degree generated by values of elliptic functions, Inv. math. 72, 3 (1983), 407-464.

[34] O. Netto, Vorlesungen über Algebra, Teubner, Leipzig, 1900.

[35] S. Smale, Mathematical Problems for the next century, *Mathematics Frontiers and Perspectives 2000*, American Mat. Soc, 2000 (paru aussi dans The Mathematical Intelligencer, 20, 1998, 2, 7-15).

[36] M. Shub, S. Smale, On the intractability of Hilbert's nullstellensatz and an algebraic version of "$NP \neq P$", Duke Math. J. 81, 1995, 47-54.

[37] P. Tworzewski, Intersection theory in complex analytic geometry, Ann. Polon. Math. 62, 1995, 177-191.