La diversité des Mathématiques face à un problème de logique *

Alain Yger
Laboratoire de Mathématiques pures
Université Bordeaux 1, 33405 Talence, France

December 22, 2001

Abstract

L'objet de l'exposé, au travers du problème de la décidabilité en temps polynomial de l'existence d'un zéro commun à un système d'équations algébriques, est de présenter la complémentarité des perceptions de nature algébrique, analytique, géométrique, face à un problème non encore résolu, mais pourtant fondamental, proposé au mathématiciens par les informaticiens ou les spécialistes de calcul formel. Cet exposé vise un public large et non *a priori* (trop) spécialiste du sujet ; il se veut avant tout un humble appel au décloisonnement (tant des objectifs que des méthodes) de plus en plus indispensable dans le monde de la recherche mathématique d'aujourd'hui.

1 Une introduction au problème $P = NP$

Les problèmes de nature algorithmique font intervenir le concept naïf de *machine* sur un anneau commutatif unitaire et ordonné $\mathbf{A}$. L'anneau $\mathbf{A}$ modélise l'univers où vivent les êtres sur lesquels la machine agit.

Les modèles d'anneaux les plus souvent rencontrés sont $\mathbb{Z}$ ou $\mathbb{Z}[x_1, ..., x_s]$, $\mathbf{R}$ ou $\mathbf{R}[x_1, ..., x_s]$; on envisagera aussi ultérieurement le cas des anneaux de caractéristique positive, tels $\mathbb{Z}_p$ ou $\mathbb{Z}_p[x_1, ..., x_s]$, mais nous nous plaçons pour

*Conférence aux journées I.R.E.M d'Aquitaine, 20 Juin 2001

l'instant dans le cadre de la caractéristique 0, cadre naturel où peuvent se cotoyer idées de nature algébrique et de nature analytique.

Suivant la présentation de ce concept tel qu'il est proposé dans [8], une machine au dessus de $\mathbf{A}$ est, si l'on s'en tient au cadre de la dimension finie, la donnée :

- d'un espace d'entrées (en général $\mathbf{A}^l$)
- d'un espace de sorties (en général $\mathbf{A}^n$)
- d'un espace d'états transitoires (en général $\mathbf{A}^m$)
- d'un graphe à N noeuds, le noeud 1 étant l'unique noeud d'entrée, les autres noeuds se classant en noeuds de sortie, noeuds de calcul, ou noeuds de branchement.

À un noeud de calcul k sont associés :

- une flèche du graphe pointant vers le noeud suivant $\beta(k)$
- une application polynomiale g_k de l'espace des états dans lui-même

À un noeud de branchement sont associés :

- deux flèches du graphe pointant vers les deux noeuds $\beta^+(k)$ et $\beta^-(k)$
- une application polynomiale h_k de l'espace des états dans $\mathbf{A}$ (ici le fait que $\mathbf{A}$ soit ordonné est capital) aiguillant la machine vers le noeud $\beta^+(k)$ si $h_k(\text{état}) \geq 0$ ou vers le noeud $\beta^-(k)$ si $h_k(\text{état}) < 0$

À un noeud de sortie, est simplement associée une application linéaire S de l'espace des états dans l'espace des sorties tandis qu'à l'unique noeud d'entrée 1 sont associés

- une unique flèche du graphe pointant vers $\beta(1)$
- une application linéaire injective I de l'espace des entrées dans l'espace des états

On peut élargir ce concept en s'affranchissant de la contrainte de finitude des dimensions et supposer $l, n \in \mathbb{N} \cup \{\infty\}$, mais alors, on prend comme espace des états $\mathbb{N} \times \mathbb{N} \times \mathbf{A}^{\mathbb{N}}$ et l'on introduit dans le graphe (toujours supposé fini) un cinquième type de noeuds ; un tel noeud (numéroté par exemple k) est la donnée

- d'une unique flèche du graphe pointant vers le noeud $\beta(k)$
- d'une application $g = g_k$ de l'espace des états dans lui-même dont l'action consiste à transformer l'état

$$(i, j, x_0, x_1, ..., \overset{j}{x_j}, ...)$$

en l'état

$$(i, j, x_0, x_1, ..., \overset{j}{x_i}, ...)$$

Si l'on oublie la structure d'ordre sur l'anneau (par exemple si $\mathbf{A} = \mathbf{C}$ ou $\mathbf{A} = \mathbb{Z}_p$, avec p premier, le cas $p = 2$ nous ramenant au contexte des machines de Turing), on peut remplacer le protocole de décision aiguillant la machine au niveau d'un noeud de branchement numéroté k par le protocole suivant :

- si x_0(état) $= 0$, la machine est aiguillée vers le noeud $\beta^-(k)$
- si x_0(état) $\neq 0$, la machine est aiguillée vers le noeud $\beta^+(k)$

Étant donnée une machine sur l'anneau $\mathbf{A}$ et un élément e de l'espace des entrées, on dit que la machine s'arrête si elle est initiée en e si l'un des noeuds de sortie est atteint au bout d'un temps minimal noté $T_M(e)$. Si e est une telle entrée, le *coût* de la machine initiée en e est la quantité obtenue comme

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

où $h_M(e)$ représente le maximum des "hauteurs" de tous les éléments de l'anneau impliqués dans les états successifs qui ont permis le cheminement depuis e jusqu'à la sortie $s_M(e)$ au bout du temps $T_M(e)$.

Il convient donc d'introduire une notion de hauteur sur l'anneau $\mathbf{A}$; si $\mathbf{A} = \mathbf{Z}$, la notion de hauteur (choisie de manière telle que la fonction coût corresponde au concept d'entropie quantifiant le désordre en physique ou en dynamique) est matérialisée par le nombre de bits nécessaires pour coder cet entier ; on peut par exemple prendre comme hauteur d'un entier a la quantité

$$h(a) := \log(|a| + 1)\,.$$

Pour les rationnels (ou même pour les nombres algébriques), il est immédiat de définir une notion de hauteur logarithmique (si $x = p/q$, la hauteur de

x est le maximum des hauteurs de p et q, si x est un nombre algébrique, c'est par exemple la somme du logarithme du degré de x et du maximum des hauteurs des coefficients du polynôme minimal à coefficients entiers annulant x, etc...). Ce ne sont ici que des approches naïves que nous reprendrons de manière plus sérieuse plus loin au paragraphe 3 de cet exposé. Si $\mathbf{A} = \mathbf{R}$, on décide que la hauteur de tout réel est 1, ce qui reflète le fait naturel que le coût de la multiplication par un réel ne dépende pas de la taille de ce réel.

Nous sommes donc maintenant en mesure de définir deux types de classe en ce qui concerne les problèmes de décision.

Un problème de décision sur l'anneau $\mathbf{A}$ est la donnée d'une paire de sous-ensembles (X, X_{oui}) , $X_{\text{oui}} \subset X$, de l'espace $\mathbf{A}^l$ (ici l est fini ou infini, cet espace sera appelé à jouer le rôle d'espace des entrées pour une machine) ; un algorithme résolvant le problème de décision est par définition une machine M, initiable à partir de tout point e de X, finissant par s'arrêter lorsqu'elle est initiée en un tel point, et fournissant alors une sortie $s_M(e) \in \{0, 1\}$, avec

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

Trois exemples de problèmes de décision capitaux retiendront notre attention :

- Le problème de décider si oui ou non une collection de m polynômes en n variables à coefficients complexes, $P_1, ..., P_m$, engendre un idéal propre dans $\mathbb{C}[X_1, ..., X_n]$, ce qui équivaut à ce que le système d'équations algébriques correspondant admette une solution dans $\mathbb{C}^n$. Dans ce cas, l'anneau est $\mathbb{C}$, mais l'on peut envisager de remplacer $\mathbb{C}$ par n'importe quel anneau commutatif intègre, tel $\mathbb{Z}, \mathbb{Z}[x_1, ..., x_s], \mathbb{Z}_p, \mathbb{Z}_p[x_1, ..., x_s]$; par idéal propre, on entend dans ce cas idéal propre dans $\mathbf{K}[x_1, ..., x_n]$, où $\mathbf{K}$ est le corps des fractions de l'anneau $\mathbf{A}$. Ce problème de décision est le *problème des zéros de Hilbert*, ou encore le *nullstellensatz*.

- Étant donnée une collection de $m+1$ polynômes en n variables à coefficients complexes, $P_0, ..., P_m$, décider si le polynôme P_0 appartient oui ou non à l'idéal engendré par les polynômes $P_1, ..., P_m$ dans $\mathbb{C}[X_1, ..., X_n]$ (même remarque en ce qui concerne le fait de pouvoir remplacer $\mathbb{C}$ par un anneau intègre commutatif quelconque). Ce problème est le *problème de l'appartenance* ou encore le *membership problem*.

- Étant donnée une matrice symétrique $[d_{k,l}]_{1\leq k,l\leq n}$ à coefficients dans $]0,+\infty[$ et un réel positif d, décider si oui ou non il existe un cycle σ dans le groupe symétrique $\mathcal{S}_n$ tel que

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

  On peut interpréter la donnée de la matrice $[d_{k,l}]_{1\leq k,l\leq n}$ comme la table des distances kilométriques entre n villes et c'est pourquoi ce problème célèbre de décision est connu comme le *problème du voyageur de commerce*.

Nous pouvons introduire, lorsque l'anneau $\mathbf{A}$ est un anneau sur lequel l'on peut définir une hauteur (c'est le cas de $\mathbb{R}$, de $\mathbb{C}$, de $\mathbb{Z}$, de $\mathbb{Z}_p$, anneaux auxquels on peut aussi adjoindre s paramètres transcendants algébriquement indépendants) deux classes de problèmes de décision posés sur $\mathbf{A}$, la classe P et la classe NP :

- un problème de décision (X, X_{oui}) sur l'anneau $\mathbf{A}$ est dans la classe P ("P" pour "décidable en temps polynomial") s'il existe un algorithme résolvant ce problème de décision tel que la machine correspondante vérifie

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

  où l est la fonction "longueur" (c'est-à-dire le nombre d'éléments non nuls dans le vecteur d'entrée $e \in \mathbf{A}^l$, $1 \leq l \leq \infty$) et h la fonction "hauteur" déjà introduite.

- un problème de décision (X, X_{oui}) sur l'anneau $\mathbf{A}$ est dans la classe NP ("NP" pour "décidable en temps polynomial non-déterministe") s'il existe deux entiers $l, l' \in \mathbb{N}\cup\{\infty\}$, une machine M sur $\mathbf{A}$ admettant un espace d'entrées contenant $X \times \mathbf{A}^{l'}$ et contenu dans $\mathbf{A}^l \times \mathbf{A}^{l'}$, avec
  - la machine s'arrête si initiée en tout (e,ω) de $X \times \mathbf{A}^{l'}$
  - $s_M(e,\omega) \in \{0,1\}$ pour tout $(e,\omega) \in X \times \mathbf{A}^{l'}$
  - $s_M(e,\omega) = 1 \Longleftrightarrow e \in X_{\text{oui}}$
  - il existe $q \in \mathbb{N}$, $C > 0$ tels que, pour tout e dans X_{oui}, il existe un aléa $\omega \in \mathbf{A}^{l'}$, avec $s_M(e,\omega) = 1$ et $C_M(e,\omega) \leq C(l(e) + h(e))^q$

Un problème de décision (X, X_{oui}) sur $\mathbf{A}$ est dit NP-complet si

- d'une part, c'est un problème de la classe NP
- d'autre part, étant donné un autre problème $(\widetilde{X}, \widetilde{X}_{\text{oui}})$ de la classe NP, il existe une application ψ de $\widetilde{X}$ dans X telle que
  - $\psi(e) \in X_{\text{oui}} \Longleftrightarrow e \in \widetilde{X}_{\text{oui}}$
  - ψ est la restriction à $\widetilde{X}$ de la fonction s_M associée à une machine M opérant en temps polynomial ; on peut voir cette seconde clause comme une clause d'universalité dans la catégorie des problèmes de décision de la classe NP.

Il est clair que la classe P est une sous-classe de la classe NP. Le problème du voyageur de commerce est un exemple de problème de la classe NP sur l'anneau $\mathbb{R}$ ([8], proposition 3). On sait par contre très peu concernant la question naturelle suivante : une telle inclusion $P \subset NP$ est-elle stricte ou non ? Ce que l'on appelle la conjecture de logique $P \neq NP$ est la conjecture suivant laquelle la classe P est strictement incluse dans la classe NP s'agissant des problèmes de décision sur $\mathbb{Z}_2$.

On sait par contre [8] que le problème du Nullstellensatz est NP-complet sur $\mathbb{C}$ (ceci reste d'ailleurs vrai sur un corps quelconque) ; ainsi donc, prouver la conjecture $P \neq NP$ sur $\mathbb{C}$ revient à prouver que le problème des zéros de Hilbert ne saurait se résoudre en temps polynomial. Cette question est toujours ouverte et sera la pierre d'angle de la suite de cet exposé. Il en est de même concernant le problème des zéros de Hilbert sur $\mathbb{Z}_2$: la conjecture $P \neq NP$ se reformule en disant que le problème de décision qu'est de savoir si une famille de m polynômes en n variables à coefficients dans $\mathbb{Z}_2$ a ou non un zéro commun dans $(\mathbb{Z}_2)^n$ peut être résolu en temps polynomial.

Une autre classe intéressante à laquelle appartient le problème de décision des zéros de Hilbert (comme d'ailleurs celui de l'appartenance) est la classe BPP (problèmes des décision solubles par une machine aléatoire avec une probabilité d'erreur bornée). Plus concrètement, étant donnée une suite de m polynômes en n variables à coefficients complexes (resp. entiers) de degré au plus D, il existe une machine (resp. une machine de Turing) qui permet (avec un risque d'erreur en $D^{-D^{O(n)}}$) de tester si oui ou non ces polynômes ont un zéro commun dans $\mathbb{C}^n$ ([23], section 7.2). On peut souligner que la

conjecture :

$$NP \subset BPP \text{ est un énoncé faux}$$

(dans le cas classique, c'est-à-dire sur $\mathbb{Z}_2$) implique

$$NP \neq P\,.$$

sur $\mathbb{C}$. Si l'on sait qu'en un certain sens pratique P et BPP représentent presque la même classe, on voit que la résolution de $NP \neq P$ sur $\mathbb{C}$ conditionnerait probablement celle de la conjecture $NP \neq P$ classique, ce qui montre que se placer délibérément dans un cadre analytique (le cadre complexe) pourrait ne pas être un handicap à la preuve de la conjecture $NP \neq P$ (voir [29] pour plus de précisions sur des références relatives à ces derniers points).

2 Effectivité des problèmes de décision type "nullstellensatz" ou "membership" (avant 1988)

Quand bien même l'un des "slogans" des mathématiques de l'après-guerre demeurait, en forme de boutade, "*Il faut éliminer l'élimination*", il reste que c'est à cette méthode initiée par Hilbert, puis développée par Greta Hermann en 1926 [17], que revient la première solution effective au problème de décision qu'est le théorème des zéros.

On sait en effet que les deux assertions suivantes sont équivalentes, étant donnés m polynômes en n variables $P_1, ..., P_m$ à coefficients dans un corps commutatif $\mathbf{K}$:

- (i) les polynômes P_j n'ont aucun racine commune dans $\overline{\mathbf{K}}^n$, ou $\overline{\mathbf{K}}$ est un clôture algébrique du corps $\mathbf{K}$
- (ii) il existe des polynômes $Q_1, ..., Q_m \in \mathbf{K}[X_1, ..., X_n]$ tels que

$$1 = P_1Q_1 + \cdots + P_mQ_m\,. \tag{2.1}$$

La preuve repose sur le fait suivant : si $p_1, ..., p_M$ sont M polynômes en une variable tels que p_1 soit unitaire, le fait que $p_1, ..., p_m$ aient une racine commune est équivalent au fait que le polynôme

$$\text{Sylv}\,(p_1, p_1 + Y_2p_2 + \cdots + Y_Mp_M) \in \mathbf{K}[Y_2, ..., Y_M]$$

(résultant de Sylvester de p_1 et de $p_1 + Y_2 p_2 + \cdots + Y_M p_M$) soit le polynôme identiquement nul ; on élimine ainsi les variables les unes après les autres et la meilleure borne que l'on puisse obtenir via cette méthode concernant le maximum des degrés des polynômes Q_j figurant dans (2.1) (en général) est celle obtenue par Greta Hermann, à savoir

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

Ce résultat de Greta Hermann, combiné avec le fait que la recherche des Q_j satisfaisant (2.1) une fois leurs degrés précisés se ramenait à la résolution d'un système d'équations linéaires (forcément compatible, c'est précisément ce qu'assure le résultat garde-fou de G. Hermann), montre qu'il existe certes un algorithme pour résoudre le problème de décision que constitue le nullstellensatz sur $\mathbb{C}$, mais que la complexité de cet algorithme est doublement exponentielle. Le coût $C_M(e)$ au dessus d'une entrée est contrôlé en $C \exp(\exp(C(l(e)+h(e))))$ pour revenir aux concepts de longueur et de hauteur introduits dans l'introduction, que l'on regarde d'ailleurs le problème posé sur $\mathbb{C}$ ou sur $\mathbb{Z}$, en vertu du principe suivant lequel un système linéaire compatible avec entrées dans un corps a nécessairement une solution dans ce corps. Si l'on regarde le problème sur $\mathbb{C}$, la taille $l(e) + h(e)$ d'une entrée $(P_1, ..., P_m)$ constituée de polynômes de degrés respectifs $D_1, ..., D_m$ en n variables est en effet

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

si on regarde le problème sur $\mathbb{Z}$, il faut tenir compte de $h(e)$, maximum des nombres $\log(1+|\alpha|)$, où α parcourt la famille de tous les coefficients non nuls de toutes les entrées polynomiales de e.

Concernant le problème de l'appartenance (dont le problème de décision des zéros de Hilbert est un sous-produit), les choses se présentent d'emblée de manière plus difficile à contrôler au niveau effectif : en effet, en 1988, Mayr et Meyer [27], dans un papier qui a fait date car il a marqué la fin d'un certain nombre d'illusions, ont su générer, pour chaque de l'entier $D \geq 5$, pour chaque entier $k > 1$, $10k + 1$ binômes en $10k$ variables, $F_{D,0}, ..., F_{D,10k}$, à coefficients entiers, de maximum des degrés égal à D, tels que, pour chaque valeur de D et de k, X_1 appartienne à l'idéal $(F_{D,0}, ..., F_{D,10k})$, mais que

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

Il y avait d'ailleurs un exemple du même type (mais plus simple, remis au goût du jour par D. Masser et P. Philippon autour de 1985) concernant le problème de décision de Hilbert : si D est un entier positif fixé et si $P_1, ..., P_n$ sont les n polynômes

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

alors

$$1 = P_1Q_1 + \cdots + P_nQ_n \Longleftrightarrow \max \deg Q_j \geq D^n - D^{n-1}\,; \tag{2.4}$$

il s'agit là d'un exemple "négatif" concernant la possibilité de résoudre le problème de décision des zéros de Hilbert en temps sous-exponentiel ; on peut aussi modifier cet exemple en remplacant P_n par $H - X_{n-1}X_n^{D-1}$, $H \in \mathbb{N}^*, H \geq 2$ et constater que l'on a pas d'espoir de trouver un entier non nul a tel que $a = P_1Q_1 + \ldots + P_nQ_n$, $Q_j \in \mathbb{Z}[X_1, ..., X_n]$ et que $\log(|a| + 1)$ soit en deça d'un ordre de grandeur du type $D^{n-1} \log H$ (voir [16, 14] pour ces questions de bornes inférieures aussi directement liées aux problèmes d'approximation en théorie de la transcendance, on peut même remplacer D^{n-1} par D^n si l'on est un peu plus soigneux (voir [24], exemple 3.10). Il y a de toutes façons toujours une marge importante entre ces bornes inférieures (2.4) et les bornes supérieures (2.2), marge qui n'existe plus en ce qui concerne le problème de l'appartenance entre les estimations supérieures (2.2) (si tant est qu'elles existent encore, ce n'est plus le problème du null-stellensatz, mais celui, autrement plus complexe, de l'appartenance!) et les estimations inférieures (2.3).

3 De la perception algébrique aux perceptions géométrique ou analytique ; la "découverte" inattendue de D. Brownawell et J. Kollár

Un réflexe naturel lorsque l'on se pose le problème de décider si m polynômes $P_1, ..., P_m$ en n variables à coefficients complexes ont un zéro commun ou non est de transposer ce problème en un problème de nature géométrique (c'en est un d'ailleurs). Malheureusement le maniement des objets géométriques

de manière effective (recherche de bornes,...) oblige à les penser inclus dans une variété compacte ; les candidats naturels sont l'espace projectif $\mathbb{P}^n(\mathbb{C})$, les variétés toriques projectives associées à un éventail constitué de cônes rationnels recouvrant $\mathbb{R}^n$.

Si l'infini se trouve matérialisé comme un hyperplan (à savoir l'hyperplan $\{x_0 = 0\}$ si $[x_0 : \ldots : x_n]$ sont les coordonnées homogènes d'un point, ou une union de diviseurs en relation avec les faces de dimension 1 de l'éventail comme c'est le cas dans une variété torique compactifiant le tore $\mathbf{T} = (\mathbb{C}^*)^n$ qui d'ailleurs agit sur elle), on peut aussi penser le concept d'infini comme le penserait un observateur vivant dans l'espace affine. Nous y reviendrons, mais plaçons nous pour l'instant dans le contexte projectif.

Les polynômes $P_1, ..., P_m$ définissent m cycles Z_1,...,Z_m dans l'espace projectif ; décider si $P_1, ..., P_m$ ont ou non un zéro commun dans $\mathbb{C}^n$ revient à décider si oui ou non les supports des cycles Z_i ne se coupent qu'à l'infini.

La théorie de l'intersection, telle qu'elle a été développée dans le cas propre, puis dans le cas impropre par Fulton [11] ou plus récemment l'école polonaise (voir par exemple [31]) permet de construire un cycle intersection $Z_1 \bullet \ldots \bullet Z_m$; n'apparaîssent dans ces constructions –c'est naturel puisqu'il s'agit de constructions géométriques– que les êtres que la géométrie permet d'identifier (éventuellement affectés de leurs multiplicités) ; tout ce qui, dans da décomposition algébrique d'un idéal, relève de ce que l'on entend par "composante immergée" n'est ainsi pas pris en compte dans cette construction, où, s'il l'est, l'est de manière telle que sa prise en compte soit gouvernée par ce qui relève de la partie géométriquement visible, celle qui correspond aux composantes isolées de l'idéal ; on rappelle que si

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

sont les idéaux premiers associés à la décomposition d'un idéal (dans l'un des anneaux noethériens $\mathbb{C}[x_0, ..., x_n]$, $\mathbb{C}[X_1, ..., X_n]$, ou l'anneau des germes de fonctions holomorphes en n variables en un point par exemple), les composantes isolées correspondent aux éléments minimaux (au sens de l'inclusion) de la famille $\{\mathcal{P}_1, ..., \mathcal{P}_s\}$; l'union de leurs ensembles de zéros matérialise la partie "visible" de l'idéal, pensé en termes d'idéal attaché à un cycle. Le contrôle des multiplicités, nécessaire à la construction du cycle intersection, s'effectue via le théorème de Bézout, c'est à dire de manière multiplicative.

Si la construction du cycle intersection nous fait perdre une part de l'information algébrique contenue dans l'idéal homogène engendré par les homogénéisés des polynômes P_j, $j = 1, ..., m$, il n'en reste pas moins que subsiste une information sous-jacente à la notion de "contour apparent" en géométrie descriptive. Une des idées clef qui ont prévalu parallèlement à la théorie de l'élimination, lorsque l'on a pensé privilégier le maniement d'inégalités plutôt que d'identités, est le concept d'*idéal de Chow* attaché à un cycle. Ce concept est intimement lié à la notion géométrique capitale (remontant à Gaspard Monge) qu'est celle de *contour apparent*. Rappelons brièvement comment est défini l'idéal de Chow d'un cycle effectif Z de dimension pure $0 \leq k < n$ de $\mathbf{P}^n(\mathbb{C})$ en un point x de son support. Pour simplifier, nous supposerons que $\mathbb{P}^n(\mathbb{C})$ est remplacé par un ouvert de carte $U \subset \mathbb{C}^n$ autour de l'origine (correspondant au point x). Supposons que $Z = \sum_j \alpha_j C_j$ et notons $|Z|$ le support de Z, soit l'union des sous-ensembles analytiques irréductibles C_j. Si π est une application linéaire surjective de $\mathbb{C}^n$ dans $\mathbb{C}^{k+1}$ telle que 0 soit un point isolé de $\mathrm{Ker}\,\pi \cap |Z|$ (on dit encore une *projection admissible*), il existe un voisinage W de l'origine dans $\mathbb{C}^n$ tel que la restriction de π à $W \cap |Z|$ soit une application propre de $W \cap |Z|$ sur $\pi(W)$. À chaque composante irréductible C_j du cycle contenant 0, correspond un nombre μ_{π,C_j} qui est le nombre de feuillets du revêtement

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

Alors, la projection $\pi(C_j \cap W)$ est un sous ensemble analytique de dimension k de $\pi(W)$, c'est à dire une hypersurface, que l'on peut donc définir par une équation f_{π_j} dans $\pi(W)$ (au voisinage de 0). On peut relever cette équation et définir une fonction analytique dans W (éventuellement restreint) par

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

En considérant toutes les projections admissibles possibles, on construit un idéal dans l'anneau des germes de fonctions holomorphes en 0, que l'on appelle *idéal de Chow* associé au cycle Z à l'origine (ou ici au point x, puisque ce point a été considéré comme la nouvelle origine), défini par

$$I^{\mathrm{chow}}(Z)_0 = (F(\pi, \cdot), \; \pi \text{ admissible}) \, .$$

On peut ainsi associer au cycle $Z_1 \bullet \ldots \bullet Z_m$ un faisceau d'idéaux

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

sur $\mathbb{P}^n(\mathbb{C})$; le "retour" de l'objet géométrique vers l'objet algébrique est assuré via un résultat du à Ewa Cygan [9] que l'on peut donner sous deux formes, une forme algébrique et une forme analytique :

- en tout point x de l'intersection des supports des cycles Z_j, l'idéal $\mathcal{I}_x^{\text{chow}}(Z_1 \bullet \cdots \bullet Z_m)$ est inclus dans la clôture intégrale de l'idéal engendré par les idéaux $\mathcal{I}_x(Z_j)$, $j = 1, ..., m$;
- si $(p_{x,j,l})_l$ désigne, pour chaque $j = 1, ..., m$, un système générateur de l'idéal $\mathcal{I}_x(Z_j)$, il existe $C_x > 0$, W_x voisinage de x, tels que

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

Comme on l'a vu, le théorème de Bézout assure que si

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

sont les degrés respectifs des polynômes $P_1, ..., P_m$, le degré du cycle-intersection $Z_1 \bullet \cdots \bullet Z_m$ est majoré par $D_1 \cdots D_n$.

C'est un autre résultat, de nature analytique cette fois, qui a permis à D. Brownawell en 1988 de prouver qu'il existe un algorithme en temps simplement exponentiel (et non plus doublement exponentiel) pour résoudre le problème de décision du théorème des zéros de Hilbert sur $\mathbb{C}$; si $\mathbf{A}$ est un anneau local régulier de dimension k et si I est un idéal quelconque de A, la clôture intégrale de l'idéal I^k est incluse dans I (mieux : celle de I^{k+p-1} est incluse dans I^p pour tout $p \in \mathbb{N}^*$). Rappelons ici qu'un élément a de l'anneau $\mathbf{A}$ est dans la clôture intégrale d'un idéal I s'il existe une relation de dépendance intégrale du type

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

Si $\mathbf{A}$ est l'anneau des germes de fonctions holomorphes à l'origine de $\mathbb{C}^n$ et si I est un idéal monomial, le résultat ci-dessus, du à Joël Briançon et Henri Skoda en 1974 [7], puis transposé à un cadre algébrique plus général (bien que la preuve en reste d'obédience analytique) par J. Lipman, B. Teissier, A. Sataye en 1981 [26, 25], est une conséquence –seulement malheureusement dans ce cas particulier– du théorème de Carathéodory affirmant que, dans un espace affine réel de dimension n, tout élément de l'enveloppe convexe d'une partie peut être réalisé comme combinaison barycentrique d'au plus $n+1$ éléments

de cette partie. Ici encore, un résultat issu de l'analyse convexe réalise la passerelle attendue entre la réalisation d'inégalités (de nature analytique) et l'obtention d'identités (de nature algébrique).

Le résultat qu'obtient D. Brownawell en 1988 [6] est le suivant : étant donnés m polynômes à coefficients complexes de degrés respectifs $D_1 \geq D_2 \geq \cdots \geq D_m$ sans zéro commun dans $\mathbb{C}^n$, il existe m polynômes $Q_1, ..., Q_m$ de degrés au plus $nD_1 \cdots D_n$ tels que

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

Un résultat de nature similaire (mais de preuve plus franchement de nature géométrique) a été obtenu par J. Kollár un an plus tard [20] : le degré d'un système de Q_j réalisant (3.5) peut être majoré par

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

Ceci prouve que le problème de décision des zéros de Hilbert se résout non seulement en temps doublement exponentiel, mais en temps simplement exponentiel ; les bornes supérieures se rejoignent donc avec les bornes inférieures (2.4). Ce résultat vint comme une surprise car l'exemple de Mayr-Meyer laissait planer des doutes sur la possibilité de descendre en dessous des bornes (2.2) proposées par G. Hermann. Il aurait aussi pu venir comme un encouragement vers une preuve du fait que ce problème de décision est un problème de type P sur $\mathbb{C}$; ceci n'a pas été le cas, car la conjecture penche toujours vers $P \neq NP$ sur $\mathbb{C}$ comme nous le verrons ultérieurement. Néanmoins, le résultat fondamental de D. Brownawell et J. Kollár, présenté sous une forme "repensée" dans [21, 18] (à la lumière des développements de la théorie de l'intersection qui ont marqué les années 1990-2000), a drainé nombre de questions liées en particulier à la transposition de ces résultats du cas $\mathbf{A} = \mathbb{C}$ au cas où $\mathbf{A}$ est un anneau sur lequel on dispose d'une notion raisonnable de hauteur (tel $\mathbb{Z}$ ou $\mathbb{Z}[X_1, ..., X_s]$, $\mathbb{Z}_p[X_1, ..., X_s]$).

Le problème de décision que constitue le problème de l'appartenance semble, lui, buter inexorablement en ce qui concerne sa complexité sur les exemples proposés par Mayr-Meyer. Pourtant l'algorithme de division euclidienne a trouvé son accomplissement avec l'algorithme de Buchberger conduisant à la construction, pour un idéal de $\mathbf{K}[X_1, ..., X_n]$ (où $\mathbf{K}$ est un corps commutatif), l'ensemble des monômes étant équipé d'une structure d'ordre (par exemple

l'ordre lexicographique), de ce que l'on appelle une *base standard* (ou *base de Gröbner*) pour l'idéal. Ainsi donc, si la connaissance d'une base standard d'in idéal permet la solution immédiate de tout problème de division relatif à cet idéal, l'exemple de Mayr-Meyer montre qu'il n'est pas *a priori* possible d'envisager un contrôle raisonnable de la complexité de l'algorithme de Buchberger (autre que du type doublement exponentiel). Il faut cependant souligner combien les idées qui, dès 1970, ont prévalu concernant la mise en forme algorithmique du théorème de division de Weierstrass (en particulier la thèse d'André Galligo en 1973 [12]) ont joué un rôle capital tant du point de vue du calcul formel que de la géométrie des singularités ; ce sont en effet les mêmes idées qui soutendent de manière fondamentale la preuve proposée en 1969 par H. Hironaka du théorème de résolution des singularités en caractéristique zéro (dans le cadre algébrique, puis analytique). Tout récemment cependant, Michel Hickel [18], raffinant un résultat antérieur de F. Amoroso [1] a prouvé que, si $P_1, ..., P_m \in \mathbf{C}[X_1, ..., X_n]$ étaient des polynômes de degrés respectifs $D_1 \geq \cdots \geq D_m$ et Q un polynôme de l'idéal $(P_1, ..., P_m)$, il était possible de trouver des polynômes $Q_1, ..., Q_m$ tels que

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

avec

$$\max \deg Q_j \leq n(\deg Q + D_1 \cdots D_n)\,.$$

4 Les outils de l'interpolation et de la dualité au service de la solution du problème des zéros

Deux idées-phares en mathématiques appliquées ont permis d'éclairer d'un jour nouveau (dans les années 1990-2000) les questions relatives à la solution des problèmes de décision évoqués ci-dessus. Il faudrait d'ailleurs plutôt parler de la "redécouverte" d'idées introduites et maintes fois exploitées à la fin du XIX-ème siècle ou au début du XX-ème siècle par des mathématiciens tels Cayley, Kronecker, Jacobi ou Macaulay. Le traité d'algèbre de O. Netto [28] contient d'ailleurs une foule d'idées que l'on retrouvera exploitées presque un siècle plus tard. Ces deux idées sont

- la formule d'interpolation de Lagrange (exploitée autant comme formule de division que d'interpolation)

- le principe de dualité (sous-jacent aussi au concept de distribution)

La formule d'interpolation de Lagrange fournit une solution alternative au problème de la résolution de l'identité de Bézout dans l'algèbre $\mathbb{C}[X]$; si P_1 et P_2 sont deux polynômes sans zéros communs alors

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

où $\mathcal{L}_{P_j}(1/P_i\,;\,\cdot)$ est l'interpolateur de Lagrange de $1/P_i$ aux zéros (éventuellement multiples) du polynôme P_j $(i \neq j)$. Quant à la formule de Cauchy

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

on peut la concevoir comme une formule de dualité :

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

l'action de la masse de Dirac en z sur l'objet-test f se ré-exprimant comme l'action sur l'objet-test $f(\zeta)d\zeta$ du "symbole résiduel"

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

(action que matérialise, mais il s'agit seulement d'une matérialisation analytique d'un objet de fait algébrique, la prise d'intégrale curviligne).

Une seconde idée (aussi attribuée à Lagrange), exprimée dans ce langage inspiré du concept de dualité, est que, si P et Q sont deux polynômes (toujours en une variable) tels que $\deg Q < \deg P - 2$, alors

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

On peut relire ce fait, mais cette fois sous l'angle de la géométrie différentielle, en disant que la somme complète des résidus de la forme $Q/P d\zeta$ sur la variété compacte $\mathbf{P}^1(\mathbb{C})$ est nulle ; cela devient donc un théorème d'indice, que déjà Jacobi [19] avait su transposer au cadre (toujours géométrique) multi-dimensionnel.

C'est une combinaison de ces diverses idées qui a permis d'établir dès 1991, une solution arithmétique au problème de décision de Hilbert, donnant une

estimation (pas encore optimale, mais sur la voie de l'être) en termes non plus seulement de degrés, mais cette fois de hauteurs, lorsque le problème se trouvait posé sur un anneau $\mathbf{A}$ équipé d'une hauteur. Si $P_1, ..., P_m$ sont m polynômes sans zéros communs dans une clôture intégrale du corps des fractions de $\mathbf{A}$, de degrés au plus D, il existe un élément a non nul de $\mathbf{A}^*$, il existe m polynômes $Q_1, ..., Q_m$ à coefficients dans $\mathbf{A}$, de degrés au plus $n(2n+1)D^n$ tels que

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

et que

$$a = P_1 Q_1 + \cdots + P_m Q_m \,,$$

où h désigne le maximum des hauteurs des coefficients des entrées [3, 4].

C'est la manière dont s'est élaboré progressivement depuis 1990 le concept de hauteur, en relation avec les développements de la théorie arithmétique de l'intersection qui a permis le raffinement de ce type de résultat et en quelque sorte son tout récent achèvement avec le travail de T. Krick, Luis-Miguel Pardo et Martín Sombra [24]. Leur résultat précise le degré des polynômes Q_j, qui devient cette fois

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

ainsi que l'estimation de hauteur, raffinée en

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

La théorie de l'intersection arithmétique, telle que l'ont développé G. Faltings, puis J. B. Bost, H. Gillet, C. Soulé [10, 13, 5], illustre bien la complémentarité entre arithmétique et analyse ; cette complémentarité est déjà inhérente à une formule bien classique, la formule du produit : si $|\cdot|_p$, p premier, désigne la valeur absolue ultramétrique sur $\mathbb{Q}$ normalisée de manière à ce que

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

où $\nu_p(k)$ désigne l'exposant de p dans la décomposition en facteurs premiers de l'entier $|k|$, on a bien sûr, pour tout nombre rationnel non nul,

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

où $|\cdot|_\infty$ désigne la valeur absolue usuelle (archimédienne) sur $\mathbb{Q}$, formule qui s'écrit encore

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

Le premier facteur est de nature arithmétique, le second de nature algébrique. La même complémentarité est sous-jacente dans une formule cruciale en théorie du potentiel pluri-complexe, à savoir la formule de Jensen : si P est un polynôme à coefficients complexes

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

alors

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

ici encore, si P est un polynôme à coefficients entiers, le membre de gauche reflète une information de nature analytique, tandis que le membre de droite (qui peut aussi, du fait de la formule du produit évoqué ci-dessus mais transposée au cadre d'une extension algébrique de $\mathbb{Q}$ au lieu de $\mathbb{Q}$, s'exprimer en termes de valeurs absolues ultramétriques) reflète une information de nature arithmétique. On note aussi que si P est un polynôme homogène de degré D, la fonction

$$\log|P|^2$$

(intervenant dans la formule de Jensen) est une solution de l'équation de Green

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

où ω désigne la forme volume dans l'espace projectif $\mathbb{P}^n(\mathbb{C})$, ce qui résulte d'une autre formule (à transposer au cadre multi-dimensionnel et à lire cette fois sur $\mathbb{P}^n(\mathbb{C})$ et non plus dans le cadre affine) que l'on peut considérer comme un jeu de balancier analytique -arithmétique qui est la suivante : si P est un polynôme en une variable à coefficients complexes, de racines $\alpha_1, ..., \alpha_n$ (avec les multiplicités $\mu_1, ..., \mu_n$, alors, au sens des distributions

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

où δ_{α_j} désigne la masse de Dirac au point α_j. Pour calculer la hauteur d'un cycle arithmétique Z de codimension k, on l'intersecte avec un sous espace

U défini en coordonnées homogènes par

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

où les u_l sont des coefficients génériques entiers ; on obtient ainsi un cycle arithmétique de dimension 0,

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

dont la hauteur (arithmétique) sera

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

pour contrebalancer cette contribution arithmétique et définir une notion de hauteur qui soit intrinsèque (c'est-à-dire ici ne dépende pas de U), on ajoute à cette hauteur arithmétique la contribution (elle de nature analytique)

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

où G_Z est un $(k-1,k-1)$ courant, régulier hors du support du cycle Z, orthogonal aux formes harmoniques, et solution de l'équation de Green

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

où $[Z]$ désigne le courant d'intégration sur le cycle (cette fois vu comme cycle géométrique en non plus arithmétique) Z. La hauteur du cycle Z est par définition la somme

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

Le point majeur concernant ce concept de hauteur est qu'il conduit à la formulation d'un théorème de Bézout non plus analytique, mais cette fois arithmétique : la hauteur de l'intersection de deux cycles arithmétiques Z_1 et Z_2 (une fois cette intersection convenablement définie) est majorée par

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

Ce résultat fondamental est à la base des résultats effectifs concernant la solution au problème de décision des zéros de Hilbert lorsque celui-ci est

posé sur $\mathbb{Z}$. Nous voulions surtout mettre en évidence à travers cette présentation très succinte la complémentarité évidente des points de vue analytique et arithmétique ; de fait, il faudrait plutôt parler des points de vue géométrique et arithmétique car le concept de courant de Green que nous venons d'introduire est intimement lié à la construction de métriques sur des fibrés, dans la droite ligne d'un théorie ébauchée par Arakelov dans le cadre des courbes algébriques [2].

5 Retour aux problèmes de complexité

Le fait que l'on dispose de versions quasi-optimales concernant l'effectivité du théorème des zéros de Hilbert, tant du point de vue géométrique (en termes de contrôle des degrés) qu'arithmétique (en termes du contrôle des hauteurs si le problème se trouve posé sur un anneau équipé d'une notion de hauteur) n'est qu'en relation indirecte avec le problème de l'existence (ou non) d'une machine capable de résoudre ces problèmes de division en temps polynomial.

Le fait cependant que l'on dispose de bornes inférieures pour l'estimation des degrés ou des hauteurs dans la résolution effective de l'identité de Bézout incite à penser que le problème de décision des zéros de Hilbert n'est pas dans la classe P. M. Shub et Smale ont d'ailleurs démontré que le fait que le problème de décision des zéros de Hilbert soit dans la classe P se répercutait au niveau de la complexité d'une suite d'entiers très simple, la suite $(k!)_{k\geq 1}$.

Définition 5.1 *Une suite d'entiers $(a_k)_{k\geq 1}$ est dite simple à calculer si et seulement si il existe une suite de "dénominateurs" $(m_k)_{k\geq 1}$, un entier q, tel qu'il existe, pour chaque $k = 1, ...,$, une suite finie d'entiers $(x_{k,l})_{0\leq l\leq N_k}$ avec*

- $x_{0,k} = 1$
- $x_{N_k,k} = m_k a_k$
- $N_k \leq (\ln k)^q$
- *chaque $x_{l,k}$, $1 \leq l \leq N_k$ se calcule sous la forme $x_{l,k} = x_{i,k} \bullet x_{j,k}$, avec $0 \leq i, j < l$ et $\bullet$ désigne une des trois opérations de base que sont l'addition, la soustraction ou la multiplication.*

Le résultat de Shub et Smale [30] s'énonce sous la forme suivante :

Théorème 5.1 *Si le problème de décision de Hilbert au dessus de* $\mathbb{C}$ *était dans la classe* P*, alors la suite* $(k!)_{k\geq 1}$ *serait simple à calculer.*

La notion de "simplicité" d'une suite numérique va nous permettre une interprétation différente des questions relatives à l'effectivité de problèmes tels que le problème des zéros de Hilbert.

Nous avons pour l'instant (évoquant les résultats de D. W. Brownawell, J. Kollár, C. A. Berenstein-A. Yger, T. Krick-L.M. Pardo-M. Sombra) parlé d'effectivité en mentionnant comment le degré (ou la hauteur) des sorties étaient contrôlées par les degrés (ou les degrés plus les hauteurs) des entrées. Il en résultait une majoration du coût d'une machine résolvant le problème de décision du fait soit d'un argument d'algèbre linéaire, soit de l'explicitation d'une formule comme c'est le cas dans [3, 4]. Il existe d'autres "éléments de mesure" pour évaluer la complexité d'une entrée constituée d'une matrice de polynômes en n variables à coefficients dans $\mathbb{C}$ ou dans $\mathbb{Z}$: par exemple, l'enveloppe convexe de leur support (c'est à dire l'enveloppe convexe dans $(\mathbb{R}^+)^n$ de l'ensemble des points de $\mathbb{N}^n$ correspondant aux multi-exposants de monômes effectivement présents dans les divers polynômes correspondant aux entrées de la matrice fournit bien souvent un élément de mesure beaucoup moins grossier que le degré.

Une autre manière de "coder" la complexité d'un système d'entrées polynomiale consiste à coder le procédé même de construction, puis d'évaluation, des diverses entrées de la matrice. Cette idée s'est fait jour depuis les années 1970, avec les travaux de J. Heintz, J. Morgenstern, C. P. Schnorr,..., est s'est développée intensivement depuis ; on peut par exemple se reporter aux références [22, 15, 14] pour trouver à la fois une présentation des outils et un regard prospectif sur le rôle qu'une telle approche pourrait avoir concernant les questions d'approximation diophantienne par exemple (remarquons que ce sont souvent des questions de cette nature qui ont motivé les travaux de D. W. Brownawell, P. Philippon, Berenstein-Yger,...).

La notion clef est celle de *straight line program* à système de paramètres $\mathcal{F}$ ("programme en droite ligne à système de paramètres $\mathcal{F}$") ; cette notion s'inspire de celle que nous avons introduite pour définir la notion de simplicité d'une suite. Un tel programme est la donnée d'un graphe $\mathcal{G}$, couplée avec celle d'un système d'instructions aux portes du graphe (système d'instructions noté $\mathcal{Q}$). Nous supposerons travailler à nombre de variables

n fixé. Le graphe présente donc $n+1$ portes d'entrée $\mathcal{Q}$ numérotées par les variables $X_1, ..., X_n$ et la constante 1. La *profondeur* d'une porte (ou noeud) ν du graphe est par définition la longueur du plus long chemin joignant ν à l'une des portes d'entrée ; on peut numéroter les portes du graphe par des paires d'entiers (i, j), où i représente la profondeur de la porte et j est un second paramètre utilisé pour classer (dans l'ordre lexicographique $<_{\text{lex}}$) les portes de profondeur fixée ; à la porte (i, j) est associée une opération :

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

oú les $A_{i,j}^{r,s}$, $B_{i,j}^{r,s}$ sont des variables intermédiaires, dites *paramètres* du programme, les $Q_{r,s}$, $Q^{r,s}$ étant des polynômes pré-calculés aux portes du graphe antérieures à la porte (i, j). Un polynôme f à coefficients entiers est dit évalué par ce programme (les paramètres étant précisés dans un sous-ensemble $\mathcal{F}$ de $\mathbb{Z}$) s'il existe une porte (i, j) et des choix de paramètres $A = (A_{k,l}^{r,s})$ et $B = (B_{k,l}^{r,s})$, avec $(r, s) <_{\text{lex}} (k, l) <_{\text{lex}} (i, j)$ tels que

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

On peut définir la *taille* s du programme (comme la taille du graphe), sa *profondeur* d (comme la profondeur du graphe), et enfin, si le sous-ensemble $\mathcal{F}$ est un sous-ensemble fini de $\mathbb{Z}$ précisé, la *hauteur* du programme comme le maximum des hauteurs (naïves) de tous les éléments de $\mathcal{F}$.

Le problème de décision de Hilbert peut alors être résolu (par exemple) en les termes suivants [23] : si $P_1, ..., P_m$ sont m-polynômes en n variables à coefficients entiers, de degré au plus $D \geq n$, de hauteur au plus h, il existe des polynômes $Q_1, ..., Q_m$ et un entier non nul a, obtenus comme des sorties de *straight-line programs* de taille, profondeur, hauteur, bornées respectivement par $md^{O(n)}$, $O(n \log D)$, $\max(D^{0(n)}, h)$, tels que

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

On pourrait aussi se poser le même problème, mais en supposant cette fois que les entrées $P_1, ..., P_m$ sont obtenues à partir de *straight-line programs* de taille, profondeur et hauteur respectivement bornés par s, d, h ; peut-on évaluer, en fonction de ces paramètres et de paramètres géométriques tels que le degré affine δ ou algébriques tels que le maximum des degrés D, les sorties relatives à un certain problème d'effectivité ? Oui, dans certains cas,

si l'on intègre en sus une information de nature géométrique : par exemple, si $P_1, ..., P_n$ sont n polynômes définissant un ensemble fini de zéros, il existe, pour chaque $j = 1, ..., n$, un *straight-line program* de longueur en $(nD\delta s)^{O(1)}$, de hauteur en $O(n(\log(nD) + d)\log\delta)$ permettant de calculer un polynôme $P \in \mathbb{Z}[X_j]$ s'annulant aux zéros communs de $P_1, ..., P_n$ dans $\mathbb{C}^n$.

Au terme de cet exposé, où l'on voit que les idées mathématiques poussées à leur terme pour fournir par exemple le résultat de Krick-Pardo-Sombra [24] finissent par s'essouffler, on sent qu'il est nécessaire de penser en termes informatiques (plus précisément en termes de théorie des langages) ces problèmes de complexité. La balle est aujourd'hui dans le camp des spécialistes du calcul formel et ce sont peut-être des idées issues de ce champ qui permettront des progrès mathématiques concernant les problèmes majeurs de l'approximation diophantienne encore en suspens, tels par exemple la célèbre conjecture de Schanuel, impliquant dans un de ces cas les plus simples l'indépendance algébrique (sur $\mathbb{Q}$) de e et π, de $\log 2$ et $\log 3$, etc... Ici encore, l'analyse pourrait, comme elle a déjà tenté de le faire, mais cette fois sans succès, jouer le même rôle d'aiguillon que celui qu'elle a su jouer face aux problèmes d'effectivité, sinon de complexité, impliqués dans le processus de décision du nullstellensatz ou du problème de l'appartenance.

References

[1] 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.

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

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

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

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

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

[7] 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.

[8] 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.

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

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

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

[12] 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.

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

[14] 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.

[15] 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.

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

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

[18] 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.

[19] 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.

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

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

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

[23] 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.

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

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

[26] 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.

[27] 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.

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

[29] 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).

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

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