Algebraic settings for the problem "$P \neq NP$?"

Rapport par Hugo Labrande

17 novembre 2011

Résumé

Ce rapport expose les résultats démontrés dans l'article [1] ; une attention toute particulière est portée à la preuve de l'élimination des constantes transcendantes.

1 Introduction

Le problème "$P \neq NP$?" est probablement le problème le plus important (et le plus célèbre) en théorie de la complexité. Il s'agit, informellement, de déterminer si certains problèmes algorithmiques considérés à l'heure actuelle comme difficiles peuvent être en fait résolus en temps polynomial – a fortiori, déterminer si les nombreux problèmes démontrés NP-complets dans de nombreux domaines sont ou non des problèmes difficiles et définitivement hors de portée. Les conséquences d'une preuve de l'égalité ou de l'inégalité de ces deux classes de complexité sont nombreuses et affectent une grande variété de domaines, comme la cryptographie, la bioinformatique, l'ingénierie, etc. ; de plus, la question semble difficile à régler, dans un sens comme dans un autre, puisque cette question résiste depuis des décennies aux chercheurs. La difficulté de la question et ses profondes implications pour une grande partie de l'informatique en font un problème très étudié : le Clay Institute inscrivit ce problème dans sa liste des 7 "problèmes du millénaire", problèmes qui apparaissent comme les plus grands défis mathématiques du troisième millénaire. Pour une discussion plus fine des conséquences d'une preuve sur cette question, le lecteur pourra se référer à l'article de référence [4].

On s'intéresse ici à un modèle de calcul introduit pour la première fois dans un article de 1989 [2] : le modèle BBS (Blum-Shub-Smale). Il s'agit d'un modèle de calcul considérant comme atomiques les éléments d'un anneau A, et où l'on considère certaines opérations comme atomiques : par exemple, on peut se placer sur $\mathbb{R}$ et considérer comme atomiques les opérations arithmétiques $+, -, \times$ and " $= 0$? (qui teste si un réel est nul). La définition d'un tel modèle de calcul est simple, puisqu'on considère simplement une machine de Turing où des réels (et non plus des bits) sont dans les cases du ruban bi-infini, et on considère que la machine peut réaliser les opérations atomiques ; cette définition est intuitive, et permet de retrouver les définitions des classes P et NP – notées dans ce cas P_A et NP_A – adaptées à ce modèle de calcul. Il s'agit là d'une généralisation du modèle de calcul "canonique", qui est recapturé ici en prenant $A = \mathbb{Z}_2$; l'intérêt d'une telle généralisation est que cela permet en quelque sorte d'instancier le problème sur d'autres

structures et de l'étudier par d'autres méthodes : il s'agit d'un modèle fertile, qui permet par exemple de découvrir des interactions directes entre la théorie de la complexité et certains problèmes algorithmiques qui surgissent en mathématiques.

Ainsi, la construction de ces modèles de calcul offre de nouveaux cadres pour la reformulation de la question "$P \neq NP$?". Il est intéressant de noter que la question peut être réglée dans le cadre de certains modèles : par exemple, si l'on considère que notre modèle de calcul est une machine de Turing sur $\mathbb{R}$ et que les opérations $+, -,$" $= 0$?" sont considérées atomiques, on peut montrer que dans ce cas $P \neq NP$, en exhibant un problème ("Twenty Questions") qui est dans $NP \setminus P$. Par contre, dans d'autres modèles de calcul proches de celui-ci, on ne connaît pas encore la réponse à la question, ce qui pousse à continuer l'étude de ce problème dans ces cas-là.

2 Etat de l'art et résultats prouvés dans l'article

L'article dont nous discutons ici s'intéresse à la question "$P \neq NP$?" sur différents anneaux de base – plus précisément, dans le cas où les éléments manipulés appartiennent à un corps K algébriquement clos et que l'on autorise $+, -, \times$ et " $= 0$?" comme opérations atomiques. Plutôt que de résoudre la question, l'article s'intéresse à des réductions de la question "$P \neq NP$ sur K?" vers son équivalent sur un autre corps algébriquement clos, i.e. des résultats de la forme $P_K = NP_K \Leftrightarrow P_L = NP_L$ où K et L sont des corps algébriquement clos : la résolution du problème sur un corps particulier entraîne la résolution du problème sur toute une variété d'autres corps. Ce résultat impliquerait des contraintes sur les programmes que l'on considère dans l'optique de résoudre la question "$P \neq NP$?" (par exemple sur les constantes utilisées par le programme), ce qui on peut l'espérer donnerait une idée plus claire du problème.

Une première tentative pour éclaircir cette question est dûe à Michaux [5]. Dans cet article, publié l'année qui précède l'article considéré ici, deux résultats importants sont prouvés :

1. Soient K et L deux corps algébriquement clos tels que $K \subset L$. Alors $P_K = NP_K \Rightarrow P_L = NP_L$. La preuve de ce résultat présentée par l'article est une preuve fonctionnant dans le cadre de la théorie des modèles ; l'article que nous exposons ici présente une preuve similaire dans la section 8 de l'article.
2. Soient K et L deux corps (K algébriquement clos[1]) tels que $\mathbb{C} \subset K \subset L$. Alors $P_L = NP_L \Rightarrow P_K = NP_K$.

Si l'on combine ces deux résultats, on a le résultat suivant :

Théorème 2.1. *Soient K et L deux corps algébriquement clos tels que $\mathbb{C} \subset K \subset L$. Alors on a $P_K = NP_K \Leftrightarrow P_L = NP_L$.*

1. En fait, d'après un résultat de Bruno Poizat cité dans l'article (Thm. 9), si l'on suppose $P_L = NP_L$ dans ce cas, on a forcément L algébriquement clos ; la preuve de ce résultat sort du cadre de cet article, mais elle utilise un résultat de Mcintyre disant qu'un corps infini qui admet l'élimination des quantificateurs est algébriquement clos.

C'est ce résultat qui est ici amélioré par l'article : les auteurs prouvent pour la première fois le théorème suivant (Thm. 1) :

Théorème 2.2. $P_{\mathbb{C}} = NP_{\mathbb{C}} \Leftrightarrow P_{\overline{\mathbb{Q}}} = NP_{\overline{\mathbb{Q}}}$.

Ceci signifie que l'ajout de constantes transcendantes n'aide pas la résolution de problèmes NP, et que si ces problèmes peuvent être résolus en temps polynomial, il existe un algorithme permettant de les résoudre en temps polynomial en n'utilisant que des entiers (car la division peut être simulée en temps polynomial). Il s'agit d'un résultat important et, en un sens, le résultat ultime concernant l'élimination des constantes – l'outil principal utilisé par les auteurs dans l'article.

Ce résultat est une grande avancée : auparavant, on savait que "$P_K \neq NP_K$?" se réduisait à "$P_{\mathbb{C}} \neq NP_{\mathbb{C}}$?" pour tous les corps K algébriquement clos contenant $\mathbb{C}$; dorénavant, on a que pour ces corps, "$P_K \neq NP_K$?" se réduit à "$P_{\overline{\mathbb{Q}}} \neq NP_{\overline{\mathbb{Q}}}$?". On a même mieux : si l'on considère un corps K algébriquement clos contenant $\overline{\mathbb{Q}}$, on peut très facilement adapter la preuve présentée dans l'article pour montrer que, dans ce cas aussi, "$P_K \neq NP_K$?" se réduit à "$P_{\overline{\mathbb{Q}}} \neq NP_{\overline{\mathbb{Q}}}$?" ; on a ainsi le théorème suivant (qui peut être vu comme une généralisation du résultat de Michaux) :

Théorème 2.3. *Soient K et L deux corps algébriquement clos tels que $\overline{\mathbb{Q}} \subset K \subset L$. Alors*

$$P_K = NP_K \Leftrightarrow P_L = NP_L \Leftrightarrow P_{\overline{\mathbb{Q}}} = NP_{\overline{\mathbb{Q}}}.$$

En particulier, puisque tout corps algébriquement clos de caractéristique nulle contient $\overline{\mathbb{Q}}$, on a que, en caractéristique nulle, "$P_K \neq NP_K$?" se réduit à "$P_{\overline{\mathbb{Q}}} \neq NP_{\overline{\mathbb{Q}}}$?" : l'extension de la chaîne des équivalences des égalités des classes de complexité au cas $K = \overline{\mathbb{Q}}$ permet de recapturer tous les corps de caractéristique nulle.

Contrairement aux preuves données dans des articles précédents ([5] par exemple), les preuves données dans l'article (et, finalement, le point de vue de l'article) sont des preuves algébriques. L'interface entre les problèmes algébriques et la théorie de la complexité est réalisée par le problème dit *problème du Nullstellensatz d'Hilbert* sur le corps algébriquement clos K, que l'on notera HN/K, qui peut être formulé ainsi : étant donné un ensemble fini de polynômes de degré n sur K, déterminer si ils ont un zéro en commun. A peu près à la même période, deux des auteurs montrèrent que ce problème est NP-complet sur $\mathbb{C}$ [6] : ainsi, tout problème de la classe NP peut se réduire à un Nullstellensatz, et si le problème du Nullstellensatz peut être résolu en temps polynomial, on a $P = NP$ sur $\mathbb{C}$, et a fortiori sur tout corps algébriquement clos de caractéristique nulle.

Les auteurs prouvent également dans cet article deux théorèmes qui forment un pont avec la théorie de la complexité algébrique de Valiant, qui introduit la notion de plus court programme (ou suite d'opérations) nécessaire à calculer un certain entier ou polynôme à coefficients entiers. Les auteurs introduisent le problème "Twenty Questions" pour la première fois dans cet article, et s'en servent pour prouver les deux théorèmes suivants :

Théorème 2.4. *Soit $k \in \mathbb{N}$. Si $k!$ est ultimement difficile à calculer, alors $HN/\mathbb{C}$ est difficile, et $P \neq NP$ sur $\mathbb{C}$, et donc sur tout corps de caractéristique nulle.*

Théorème 2.5. *Soit $f \in \mathbb{Z}[X]$. Si $\mathcal{Z}(f) \leq \tau(f)^c$ pour une certaine constante c universelle, alors $P \neq NP$ sur $\mathbb{C}$, et donc sur tout corps de caractéristique nulle.*

La preuve de ces deux théorèmes fait appel au problème "Twenty Questions", et est en vérité la même que celle qui a été vue en cours ; ainsi, nous ne nous attarderons pas sur ces deux théorèmes, et présenterons dans la suite de ce rapport uniquement la preuve du théorème 1 de l'article, c'est à dire :

Théorème 2.6. $P_{\mathbb{C}} = NP_{\mathbb{C}} \Leftrightarrow P_{\overline{\mathbb{Q}}} = NP_{\overline{\mathbb{Q}}}$.

3 "$\overline{\mathbb{Q}} \Rightarrow \mathbb{C}$"

La preuve que $P_{\overline{\mathbb{Q}}} = NP_{\overline{\mathbb{Q}}} \Rightarrow P_{\mathbb{C}} = NP_{\mathbb{C}}$ qui est présentée dans l'article est une preuve faisant appel à quelques notions d'algèbre avancée. En fait, le théorème qui est prouvé est plus général :

Théorème 3.1. *Soient $K \subset L$ deux corps algébriquement clos. Si $P_K = NP_K$ alors $P_L = NP_L$.*

Nous ne reproduirons pas la preuve ici, car elle est assez difficile d'accès ; elle utilise des notions plutôt complexes de géométrie algébrique, et utilise une formulation "mathématique" du Nullstellensatz d'Hilbert (faisant intervenir des variétés d'idéaux et des radicaux d'idéaux) plutôt que la formulation "algorithmique" (équivalente) utilisée jusqu'à présent. Le lecteur intéressé pourra se référer au chapitre 7 de [3] : la preuve exposée est à peu près la même, mais un appendice explique quelques notions de géométrie algébrique utilisées ici (topologie de Zariski, théorème de la base de Hilbert, et la formulation classique du Nullstellensatz d'Hilbert).

Notons l'existence d'une preuve de ce résultat en utilisant des notions tirées de la théorie des modèles ; cette preuve fut trouvée par Michaux [5], et les auteurs reproduisent ici une preuve similaire. Cette preuve utilise un principe de complétude (le "Strong Transfer Principle") qui apparaît en théorie des modèles durant l'étude des corps algébriquement clos ; ce principe est le suivant : si $K \subset L$ sont deux corps algébriquement clos et que ϕ est une phrase de la logique du premier ordre avec des constantes dans K, alors ϕ est vraie sur K si et seulement si ϕ est vraie sur L. Il suffit ensuite de montrer que si M est une machine qui résout le Nullstellensatz sur K en temps borné, M fonctionne également en temps borné avec des entrées dans L et M renvoie 1 si et seulement si l'entrée est une solution du Nullstellensatz sur L.

4 "$\mathbb{C} \Rightarrow \overline{\mathbb{Q}}$" : élimination des constantes

4.1 Stratégie de preuve

La stratégie des auteurs est une stratégie d'élimination des constantes : il s'agit de montrer qu'un programme avec des constantes dans $\mathbb{C}$ ne permet pas de calculer plus de choses (et de résoudre plus de problèmes) qu'un programme avec des constantes dans

$\overline{\mathbb{Q}}$. Il s'agit ainsi de montrer que l'on peut simuler des constantes de $\mathbb{C}$ au sein d'un programme ayant des constantes dans $\overline{\mathbb{Q}}$ (et donc finalement que, calculatoirement, on peut se passer d'utiliser des constantes appartenant à $\mathbb{C}$ – même si bien entendu cela peut être plus pratique).

Cette stratégie semble une stratégie nouvelle lors de la parution de l'article ; les auteurs consacrent ainsi une section de leur article aux "cas simples", c'est à dire l'élimination des constantes provenant d'une extension algébrique d'un corps K. Il s'agit ainsi de montrer que l'on peut simuler les constantes algébriques et les fractions au sein d'un programme avec des constantes dans K : les auteurs montrent ainsi qu'on peut se réduire au corps K au lieu de sa clôture algébrique ou de son corps des fractions. Nous ne reproduirons pas ici la preuve, car elle est strictement analogue à celle vue en cours.

Ce résultat sera utile pour prouver le théorème central de l'article, mais il n'en est pas la pierre angulaire : l'outil utilisé par les auteurs pour prouver ce théorème est un résultat d'élimination des constantes transcendantes. Il s'agit ainsi de montrer que :

Proposition 4.1. *Soit $K \subset \overline{\mathbb{Q}}$ (i.e. sans constantes transcendantes) et $K \subset L$ avec L un corps. Si un problème de décision sur L peut être résolu à l'aide d'un programme utilisant des constantes appartenant à L, alors le même problème de décision sur K peut être résolu à l'aide d'un programme utilisant des constantes appartenant seulement à K ; le surcoût en temps est en t^c, où c est une constante.*

Une fois ce résultat montré, on pourra ainsi montrer que :

Théorème 4.2. *Si $P_{\mathbb{C}} = NP_{\mathbb{C}}$ alors $P_{\overline{\mathbb{Q}}} = NP_{\overline{\mathbb{Q}}}$.*

Démonstration. Si $P_{\mathbb{C}} = NP_{\mathbb{C}}$ le Nullstellensatz d'Hilbert sur L peut être résolu en temps polynomial par un programme utilisant des constantes dans L ; ainsi, le Nullstellensatz d'Hilbert sur K peut être résolu en temps polynomial par un programme, celui-ci utilisant des constantes dans L. On utilise ensuite la proposition précédente pour obtenir un programme utilisant des constantes dans K uniquement, résolvant le Nullstellensatz d'Hilbert sur K, et fonctionnant en temps polynomial (également par la proposition précédente). □

Le début de la preuve d'élimination des constantes a été esquissé en cours : on le reproduit brièvement ici. Considérons un programme A qui résout le problème de décision sur L ; ce programme utilise un nombre fini de constantes sur L, et finalement on peut considérer que $L = K(\mu_1, \mu_2, ..., \mu_m)$. Certaines de ces constantes sont algébriques, et peuvent être éliminées par le processus exposé précédemment ; les autres sont transcendantes et algébriquement indépendantes, formant ce qu'on appelle une base de transcendance. On peut donc supposer que $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$ où les (α_i) sont algébriquement indépendants ; les éléments de L sont donc des fractions rationnelles en la base de transcendance (que l'on peut également simuler par le processus exposé précédemment, obtenant des polynômes). Le point crucial est de pouvoir tester si un polynôme en la base de transcendance est nul ; si l'on peut faire un tel test, on peut simuler complètement un programme avec constantes dans L par un programme avec constantes dans K. Les auteurs montrent

que l'on dispose d'un tel test de nullité dans le cas $K = \overline{\mathbb{Q}}$ qui nous intéresse ; ce test de nullité est pris en charge par le théorème suivant, dit *théorème du témoin* :

Théorème 4.3. *Soit $F(x,t) = F(x_1, ..., x_r, t_1, ..., t_l)$ un polynôme en $r + l = n$ variables à coefficients dans $\mathbb{Z}$, et soit $F_x \in \overline{\mathbb{Q}}[t_1, ..., t_l]$ (défini par $F_x(t) = F(x,t) \forall x \in \overline{\mathbb{Q}}$). Soit N un entier positif tel que $\log N \geq 4n\tau^2 + 4$ (où τ est la longueur du plus court programme calculant F).*

Alors $\forall x \in \overline{\mathbb{Q}}$, il existe $w_1 \in \{2^N, x_1^N, ..., x_r^N\}$ tel que le point $w = (w_1, ..., w_l)$ (où $w_i = w_{i-1}^N$) est tel que $F_x(w) = 0 \Rightarrow F \equiv 0$. (On appelle alors w un témoin pour F.)

4.2 Notion de hauteur d'un nombre algébrique

Afin de prouver le théorème du témoin, les auteurs utilisent la notion de *hauteur d'un nombre algébrique*, qui est une notion classique de géométrie algébrique. Ici, on considèrera simplement qu'une fonction de hauteur est une fonction $H : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ qui vérifient les propriétés suivantes :

1. $H(0) = H(1) = 1, H(2) = 2, H(w) \geq 1, H(w) = H(-w), H(1/w) = H(w)$
2. $\frac{H(v)}{2H(w)} \leq H(v+w) \leq 2H(v)H(w)$
3. $H(w^k) = H(w)^k, H(vw) \leq H(v)H(w)$
4. $H(vw) \geq \frac{H(v)}{H(w)}$ if $w \neq 0$

On définit enfin pour tout polynôme $g \in \overline{\mathbb{Q}}[t]$ la hauteur du polynôme g comme le produit des hauteurs de ses coefficients.

Un exemple de fonction de hauteur est la fonction qui, à un élément de $\overline{\mathbb{Q}}$ (de polynôme minimal $\sum_{i=0}^n a_i X^i$, $a_i \in \mathbb{Z}$) associe $\max_i |a_i|$ [2] Les fonctions de hauteur sont fréquemment utilisées en géométrie algébrique, et interviennent dans les preuves de plusieurs résultats classiques de géométrie algébrique (comme le théorème de Mordell-Weil pour les courbes elliptiques), ainsi que dans d'autres domaines – on peut même les utiliser pour prouver que l'ensemble des nombres algébriques est dénombrable.

On prouve ensuite quelques propriétés sur les hauteurs de polynômes.

Proposition 4.4. *Pour tout $g \in \overline{\mathbb{Q}}[t]$ de degré d et tout $w \in \overline{\mathbb{Q}}$ on a $H(g(w)) \leq 2^d H(g)H(w)^d$.*

Démonstration. On utilise l'algorithme de Hörner pour évaluer le polynôme :

$$\begin{aligned} H(g(w)) &= H(((...(a_d w + a_{d-1})w + a_{d-2})w + ...)w + a_0) \\ &\leq 2H(a_0)H(w)H(((...(a_d w + a_{d-1})w + a_{d-2})w + ...)w + a_1) \\ &... \\ &\leq 2^d H(a_0)H(w)H(a_1)H(w)...H(a_d)H(w) \end{aligned}$$

2. Notons que cette fonction coïncide avec la hauteur "classique" sur $\mathbb{Q}$, $H(p/q) = max(|p|, |q|)$ où p et q sont premiers entre eux.

□

Proposition 4.5. *Pour tout $g \in \overline{\mathbb{Q}}[t]$ de degré d (non constant) et $w \in \overline{\mathbb{Q}}$, on a $H(g(w)) \geq \frac{H(w)}{2^d H(g)}$.*

Démonstration.

$$\begin{aligned} H(g(w)) &= H(a_d w^d + \sum_{i=0}^{d-1} a_i w^i) \\ &\geq \frac{H(a_d w^d)}{2H(\sum_{i=0}^{d-1} a_i w^i)} (\text{par 2.}) \\ &\geq \frac{H(w^d)}{2H(a_d)H(\sum_{i=0}^{d-1} a_i w^i)} (\text{par 4.}) \\ &\geq \frac{H(w)^d}{2^d H(a_d) H(w)^{d-1} H(a_0)...H(a_{d-1})} (\text{par la Prop. précédente}) \\ &\geq \frac{H(w)}{2^d \times H(g)} \end{aligned}$$

□

Corollaire 4.6. *Si $H(x) \geq 2^d H(g)$, alors $g(x) \neq 0$ à moins que g soit nul.*

Cette remarque n'est pas innocente, et on voit comment une condition sur la hauteur d'un certain nombre algébrique bien choisi peut nous conduire à une conclusion similaire à celle du théorème du témoin : si la condition sur la hauteur de x est vérifiée, on a que si g s'annule en x, c'est que g est identiquement nul, faisant de x un témoin pour g. On voit ici que la hauteur est véritablement le bon outil pour exprimer que x est un témoin pour g ; c'est ce que l'on utilise dans la suite de la preuve pour démontrer le théorème du témoin.

4.3 Preuve du théorème du témoin

On définit la hauteur d'un vecteur d'éléments de $\overline{\mathbb{Q}}$ comme étant :

$$H((x_1, ..., x_r)) = max_i H(x_i)$$

On définit également la hauteur d'un polynôme multivarié comme le produit des hauteurs des coefficients devant les monômes. Enfin, pour un polynôme multivarié G, on définit la quantité $D(G) = 2^{\tau(G)}$, où $\tau(G)$ est la longueur minimale d'une chaîne d'opérations calculant le polynôme. On a immédiatement que le degré de G est inférieur à $D(G)$, et que le nombre de monômes de G est borné par $D(G)^n$ où n est le nombre de variables de G.

Soit $G \in \overline{\mathbb{Q}}[t_1, ..., t_n]$; pour $x = (x_1, ..., x_r)$ un vecteur d'éléments de $\overline{\mathbb{Q}}$, on introduit le polynôme suivant :

$$G_x(t_{r+1}, ..., t_n) = G(x_1, ..., x_r, t_{r+1}, ..., t_n).$$

On remarque que cet énoncé est similaire aux conditions du théorème du témoin. La proposition suivante prouve un résultat sur la hauteur de G_x :

Proposition 4.7. *Soit* $G \in \overline{\mathbb{Q}}[t_1, ..., t_n]$ *et* $x = (x_1, ..., x_r) \in \overline{\mathbb{Q}}^r$ *; on a* $H(G_x) \leq H(G)(2H(x))^{D'}$, *où* $D' = D(G)^{n+1}$.

La preuve de cette proposition est très similaire à celle de la Proposition 4.4 ; il s'agit de borner la hauteur des coefficients de G_x (par la même méthode), puis d'en faire le produit. Notons l'apparition d'un terme dépendant de $D(G)$, qui apparait lorsqu'on essaie de borner la hauteur d'un "monôme en $x_1, ..., x_r$".

On prouve un dernier résultat sur la hauteur d'un polynôme multivarié :

Proposition 4.8. *Soit* $G \in \overline{\mathbb{Q}}[t_1, ..., t_r]$ *; alors* $\log_2 H(G) \leq 2^{2n\tau^2}$.

Démonstration. Ce résultat se prouve par induction sur τ. Supposons que G est le produit de deux polynômes obtenus en $\tau - 1$ étapes (le seul cas problématique), i.e. $G = FF'$ avec

$$\begin{aligned} F(x_1, ..., x_r) &= \sum_{\alpha=(\alpha_1,...,\alpha_r)} a_\alpha \prod_{i=0}^{r} x_i^{\alpha_i} \\ F(x_1, ..., x_r) &= \sum_{\beta=(\beta_1,...,\beta_r)} b_\beta \prod_{i=0}^{r} x_i^{\beta_i}, \end{aligned}$$

on écrit la hauteur du coefficient indexé par un certain γ de G :

$$\begin{aligned} H\Big(\sum_{\beta=(\beta_1,...,\beta_r)} a_{\gamma-\beta} b_\beta &\leq \prod_{\beta} 2H(a_{\gamma-\beta})H(b_\beta) (\text{par 2. et 3.}) \\ &\leq 2^{D^n} H(F)H(F') (\text{car le nombre de monômes de } G \text{ est borné par } D^n.) \end{aligned}$$

Le logarithme de la hauteur de G est alors borné par $D^n \log 2^{D^n} H(F)H(F')$ (là encore, car le nombre de monômes de G est borné par D^n), et en utilisant l'hypothèse d'induction sur F et F' on démontre la proposition. □

Nous avons maintenant tous les outils pour démontrer le théorème du témoin. Fixons $x = (x_1, ..., x_r)$ un vecteur d'éléments de $\overline{\mathbb{Q}}$. Soit w_1 l'élément de hauteur maximale dans l'ensemble $\{2^N, x_1^N, ..., x_r^N\}$; on a alors $H(w_1) > 1$ (car $H(w_1) \geq H(2^N) = 2^N$), et $H(w_j) > H(w_{j-1})$. Soit $F(x, t)$ défini comme dans les hypothèses du théorème du témoin :

$$F(x_1, ..., x_r, t_1, ..., t_l) = \sum_{\alpha=(\alpha_i),\beta=(\beta_i)} a_{\alpha,\beta} \left(\prod_{i=0}^{r} x_i^{\alpha_i} \right) \left(\prod_{i=0}^{l} t_i^{\beta_l} \right).$$

On définit un polynôme $G_{\overline{\beta}}^j$, $\overline{\beta}$ étant un vecteur de $(l - j)$ éléments, comme :

$$G_{\overline{\beta}}^j(t) = \sum_{\alpha=(\alpha_i),\beta=(\beta_1,...,\beta_j,\overline{\beta_{j+1}},...,\overline{\beta_l})} a_{\alpha,\overline{\beta}} x_1^{\alpha_1} ... x_r^{\alpha_r} w_1^{\beta_1} ... w_{l-1}^{\beta_{l-1}}.$$

Ce polynôme dépend d'un vecteur d'éléments $(\overline{\beta_{j+1}}, ..., \overline{\beta_l})$: on note que l'on remplace dans $F(x_1, ..., x_r, w_1, ..., w_{j-1}, t, t_{j+1}..., t_l)$ les $(l-j)$ dernières variables par des éléments quelconques, on obtient un polynôme qui sera un $G^j_{\overline{\beta}}$, pour un certain choix de β (et un choix de $a_{\alpha,\beta}$). On note également que l'on a $G^{l-1}_{\overline{\beta}}(w_l) = F(x,t)$.

On a le lemme suivant :

Lemme 4.9. *Pour tout choix de j et $\overline{\beta}$, $H(w_j) > 2^D H(G^j_{\overline{\beta}})$.*

Démonstration. La preuve est essentiellement technique, et nous ne la reproduisons pas. Cette inégalité découle de l'application des deux propositions précédentes, ainsi que la définition des w_j et de N dans les hypothèses du théorème du témoin. □

Nous voilà prêts à conclure et prouver le théorème du témoin :

Démonstration. Il nous faut prouver que w est un témoin : supposons que $F_x(w) = 0$.

Considérons le polynôme $G^l_\emptyset$: le lemme 4.9 permet d'affirmer que $H(w_l) > 2^D H(G^l_\emptyset)$. En appliquant le corollaire 4.6 (le dernier de la partie précédente), on a que $G^l_\emptyset(w_l) \neq 0$ sauf si $G^l_\emptyset$ est le polynôme nul. Mais comme $G^l_\emptyset(w_l) = F(x,w) = F_x(w) = 0$, on a que $G^l_\emptyset \equiv 0$; en particulier :

$$\sum_{\alpha=(\alpha_i),\beta=(\beta_1,...,\overline{\beta_l})} a_{\alpha,\beta} x_1^{\alpha_1}...x_r^{\alpha_r} w_1^{\beta_1}...w_{l-1}^{\beta_{l-1}} = 0$$

w_{l-1} est alors un zéro de $G^{l-1}_{(\overline{\beta_l})}$; en itérant le même raisonnement on montre que $G^1_{(\overline{\beta_1},...,\overline{\beta_l})}$ est le polynôme nul, et ce pour tout choix de vecteur $(\overline{\beta_i})$. Comme les choix de vecteur $(\overline{\beta}$ décrivent l'ensemble des valeurs prises par F_x, on a que $F_x \equiv 0$, ce qui prouve le théorème. □

Au final, on a prouvé le théorème du témoin. Ce théorème permet ensuite d'éliminer les constantes transcendantes : tester la nullité d'un polynôme (la dernière étape qui restait à faire) revient alors à considérer le polynôme F_x (où le vecteur x est celui de la base de transcendance), trouver un témoin grâce au théorème du témoin, et évaluer le polynôme en le témoin : si le résultat de l'évaluation est nul, le polynôme est identiquement nul. Ceci complète la simulation du programme avec constantes transcendantes telle qu'annoncée par le théorème 4.1 ; le théorème 4.2 suit, ce qui montre que $P = NP$ sur $\mathbb{C}$ implique $P = NP$ sur $\overline{\mathbb{Q}}$.

5 Conclusion

Nous avons présenté ici le résultat principal de l'article [1]. Quelques preuves ont été omises, notamment celles vues en cours, mais nous avons essayé d'expliquer la partie centrale de l'article (la preuve du théorème du témoin) de façon aussi complète que possible. On regrettera que ce rapport n'aie pu présenter, pour des raisons de place

principalement mais aussi car les concepts manipulés sont mathématiquement avancés, la preuve algébrique de la réciproque du théorème 1 de l'article.

Bien que cet article démontre plusieurs théorèmes utiles et introduit des notions plus généralement utilisables ("Twenty Questions"), le concept majeur introduit par l'article reste le thème de l'élimination des constantes. Le cas des constantes algébriques est simple ; quant au cas des constantes transcendantes, il nécessite un théorème dit "du témoin", qui permet de trouver un certificat de nullité d'un polynôme faisant intervenir des constantes transcendantes, certificat qui lui-même n'est pas transcendant et appartient au corps de base : ceci permet la simulation des constantes transcendantes à l'aide de constantes du corps de base. Au final, l'élimination des constantes permet de montrer que la question "$P \neq NP$?" a la même réponse dans tous les corps algébriquement clos de caractéristique nulle – par exemple $\overline{\mathbb{Q}}$ et $\mathbb{C}$, un résultat nouveau étendant la chaîne d'équivalences connue jusqu'alors.

Références

[1] L. Blum, F. Cucker, M. Shub, S. Smale, *Algebraic settings for the problem "$P \neq NP$"*, Proceedings of the 25th AMS-SIAM Summer Seminar in Applied Mathematics, Park City 1995, ed. : J. Renegar, M. Shub, S. Smale.

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

[3] L. Blum, F. Cucker, M. Shub, and S.Smale, *Complexity and Real Computation*, Springer-Verlag (1998).

[4] R. Impagliazzo, *A personal view of average-case complexity*, pp.134, 10th Annual Structure in Complexity Theory Conference (SCT'95), 1995.

[5] C. Michaux, *$P \neq NP$ over the nonstandard reals implies $P \neq NP$ over $\mathbb{R}$*, Theor. Comput. Sci. 133, 1 (October 1994), 95-104.

[6] M. Shub, S. Smale, *On the intractability of Hilbert's Nullstellensatz and an algebraic version of "P=NP"*, Duke Mathematical Journal, vol. 81, pp. 47–54, 1996.

[7] G. J. Woeginger, *The P-versus-NP page*, http ://www.win.tue.nl/ gwoegi/P-versus-NP.htm.