THE JOURNAL OF SYMBOLIC LOGIC
Volume 65, Number 4, Dec. 2000

LE PROBLÈME DES GRANDES PUISSANCES ET CELUI DES GRANDES RACINES

NATACHA PORTIER

Résumé. Soit f une fonction de $\mathbf{N}$ dans $\mathbf{N}$ qui ne soit pas calculable en temps polynomial, et a un élément d'un corps différentiel K de caractéristique nulle. Nous appelons problème des grandes puissances l'ensemble des uples $\bar{x} = (x_1, \ldots, x_n)$ de K tels que $x_1 = a^{f(n)}$, et problème des grandes racines l'ensemble des uples $\bar{x}$ de K tels que $x_1^{f(n)} = a$. Ce sont deux exemples de problèmes que l'utilisation de la dérivée ne permet pas de résoudre plus rapidement. Nous montrons que le problème des grandes racines n'est pas polynomial au sens des corps différentiels, même si nous autorisons un nombre polynomial de paramètres, et que le problème des grandes puissances n'est pas polynomial au sens des corps différentiels, même au niveau non uniforme. Les démonstrations utilisent la stabilité polynomiale de la théorie des corps de caractéristique nulle, montrée par L. Blum, F. Cucker, M. Shub et S. Smale, ainsi que le lemme de réduction qui permet de ramener un polynôme différentiel des variables $\bar{x}$ à un polynôme des variables $\bar{x}$ et de leurs dérivées.

Abstract. Let f be a function from $\mathbf{N}$ to $\mathbf{N}$ that can not be computed in polynomial time, and let a be an element of a differential field K of characteristic 0. The problem of large powers is the set of tuples $\bar{x} = (x_1, \ldots, x_n)$ of K so that $x_1 = a^{f(n)}$, and the problem of large roots is the set of tuples $\bar{x}$ of K so that $x_1^{f(n)} = a$. These are two examples of problems that the use of derivation does not allow to solve quicker. We show that the problem of large roots is not polynomial for the differential field K, even if we use a polynomial number of parameters, and that the problem of large powers is not polynomial for the differential field K, even for non-uniform complexity. The proofs use the polynomial stability (i.e., the elimination of parameters) of field of characteristic 0, shown by L. Blum, F. Cucker, M. Shub and S. Smale, and the reduction lemma, that transforms a differential polynomial in variables $\bar{x}$ into a polynomial in variables $\bar{x}$ and their derivatives.

Soit K un corps commutatif de caractéristique nulle. Il existe des questions auxquelles nous pouvons répondre à l'aide de peu d'opérations. Par exemple, si $a_0, \ldots, a_n$ et b sont des éléments de K, nous pouvons savoir si b est racine du polynôme $a_0 + a_1X + \cdots + a_nX^n$ grâce à l'algorithme de Horner avec n additions, autant de multiplications, et un test d'égalité à 0. Nous représentons ces calculs par un graphe, que nous appelons circuit. Les opérations que nous autorisons sur un corps sont la soustraction, l'addition, la multiplication, et le test d'égalité à 0. Nous pouvons alors chercher quel est le nombre minimal d'opérations à effectuer pour résoudre une question donnée. Si nous enrichissons notre corps d'une dérivée, nous avons une opération supplémentaire. La complexité des calculs reste-t-elle la même ? Nous étudions deux exemples, celui des grandes puissances et celui des

Received September 30, 1998; revised April 4, 1999.

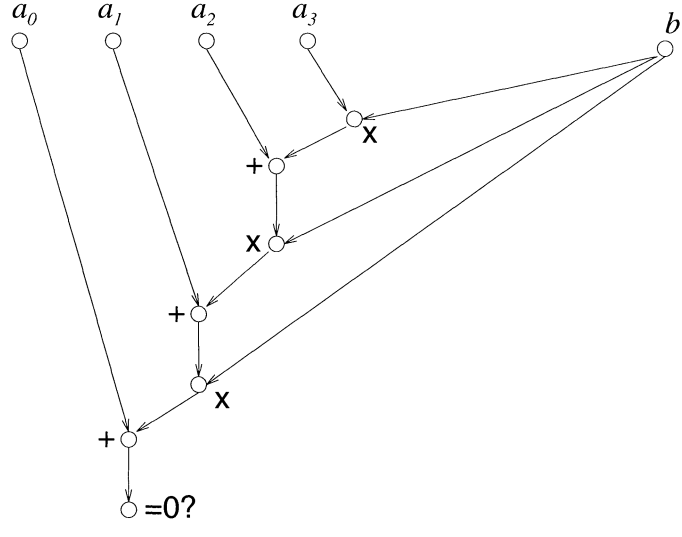
Travail réalisé à l'Institut Gerard Desargues, UPRES-A 5028, Université Claude Bernard, Lyon I, 43 Bd du 11 novembre 1918, 69 622 Villeurbanne Cedex, France.

0022-4812/00/6504-0010/$2.10

grandes racines, pour lesquels la dérivée n'accélère pas les calculs. Le modèle de calcul est celui qui apparaît dans le livre de B. Poizat [5], et qui utilise les suites de circuits.

DÉFINITION 1. Un *circuit sur le corps K* est un graphe orienté sans cycle orienté. Les sommets sont appelés portes, et les arêtes flèches. Ce n'est pas nécessairement un arbre : une porte peut émettre plusieurs flèches. Les portes qui ne reçoivent pas de flèches sont les entrées. Elles sont étiquetées par un élément de K ou par une variable. Les autres portes sont étiquetées par une opération arithmétique, $+$, $\times$ ou $-$ et reçoivent deux flèches, ou par un test "$= 0$?" et n'en reçoivent qu'une. Il n'y a qu'une seule porte qui n'émette pas de flèche : c'est la sortie, et elle est étiquetée par un test.

Voici par exemple un circuit qui teste si le polynôme $a_0 + a_1X + a_2X^2 + a_3X^3$ s'annule en b :



Nous notons par $C(a_1, \ldots, a_r, x_1, \ldots, x_n)$ un circuit qui a $n + r$ entrées dont les r premières sont étiquetées par les éléments $a_1, \ldots, a_r$ de K et les n suivantes par des variables. Le calcul sur une entrée $(b_1, \ldots, b_n)$ s'effectue de la façon suivante : à l'entrée étiquetée par x_i nous associons l'élément b_i, pour i compris entre 1 et n. Puis nous associons à chaque porte de C un élément de K, en procédant de proche en proche. Si nous avons associé aux portes p_1 et p_2 les éléments α et β, et si p est une porte d'addition qui reçoit ses flèches de p_1 et p_2, nous lui associons la somme de α et de β dans K. Nous procédons de même pour les portes de multiplication et de soustraction. Une porte de test calcule 1 si le résultat du calcul qui lui est envoyé est 0, et 0 sinon. Nous effectuons les calculs en commençant par les entrées et en terminant par la sortie. Plus précisément, les flèches du circuit induisent un ordre partiel sur les portes : les entrées sont les plus petites, et la sortie est la plus grande. Les calculs peuvent se faire par niveau : le premier niveau est l'ensemble des portes qui reçoivent une flèche d'une entrée, le deuxième niveau est l'ensemble des portes qui reçoivent au moins une flèche d'une porte du premier niveau, et ainsi de suite jusqu'au dernier niveau qui est constitué uniquement de la porte de sortie. Les

calculs des portes sont réalisés niveau après niveau, en commençant par le premier et dans n'importe quel ordre à l'intérieur d'un niveau. Une autre façon de faire est de compléter l'ordre partiel existant sur les portes en un ordre total, et de faire les calculs dans cet ordre. Par la suite, nous ne nous préoccupons plus de l'ordre dans lequel les calculs sont effectués.

Comme la dernière porte est un test, le circuit calcule 0 ou 1. Il accepte l'entrée s'il calcule 1, et il la refuse dans le cas contraire. A un circuit $C(\bar{x}, \bar{a})$ sur un corps nous associons une formule $\phi(\bar{x}, \bar{a})$ du premier ordre sans quantificateur du langage des corps à paramètres dans K telle que pour tout n-uple $\bar{b}$ d'éléments de K, $C(\bar{a}, \bar{b})$ calcule 1 si et seulement si $K \models \phi(\bar{a}, \bar{b})$. Cette formule peut se construire de la manière suivante : à un n-uple $\bar{b}$ accepté par le circuit nous pouvons associer les réponses des tests effectués par le circuit. Il existe des polynômes $P_1(\bar{x}, \bar{a}), \ldots, P_r(\bar{x}, \bar{a})$ et des éléments $\varepsilon_1, \ldots, \varepsilon_r$ de $\{=, \neq\}$ tels que $P_1(\bar{b}, \bar{a})\varepsilon_1 0, \ldots, P_r(\bar{b}, \bar{a})\varepsilon_r 0$. En posant $\phi_{\bar{b}}(\bar{x}, \bar{a}) = (P_1(\bar{x}, \bar{a})\varepsilon_1 0 \wedge \cdots \wedge P_r(\bar{x}, \bar{a})\varepsilon_r 0)$, nous avons $K \models \phi_{\bar{b}}(\bar{b}, \bar{a})$. Si le circuit a τ portes de tests, il y a 2^τ réponses possibles, et donc un nombre fini de formules $\phi_{\bar{b}}(\bar{x}, \bar{a})$. Leur disjonction est la formule cherchée. Réciproquement, à toute formule sans quantificateur nous pouvons associer un circuit. Les termes sont calculés à partir des entrées avec des opérations arithmétiques, les formules atomiques sont des termes suivi d'un test. Les opérations booléennes peuvent être réalisées par des opérations du corps : si x et y sont des booléens, alors $\neg x = 1 - x$ et $x \wedge y = xy$. En général, les circuits sont plus concis que les formules : un terme qui intervient plusieurs fois dans une formule n'a besoin d'être calculé qu'une seule fois dans un circuit. Par exemple, tester si $x^{2^n} = 1$ demande un circuit avec $n + 2$ portes alors que la formule atomique $x^{2^n} = 1$ est de taille $2^n + 2$.

Dans un circuit, les portes de calculs qui sont étiquetées par une opération arithmétique calculent des polynômes à coefficients entiers des entrées conditionnés par des tests polynomiaux à coefficients entiers des entrées. Appelons *taille* τ d'un circuit son nombre de portes. Une récurrence immédiate montre alors que tous les polynômes considérés sont de degré au plus 2^τ, et que les coefficients sont des entiers de valeur absolue inférieure à 2^{2^τ}. Nous en déduisons un lemme sur la forme des sous-ensembles de K acceptés par un circuit :

LEMME 1. *Si C est un circuit de taille τ sur le corps K avec une seule variable d'entrée x, alors l'ensemble des éléments acceptés par C ou son complémentaire est fini de cardinal au plus $\tau 2^\tau$.*

DÉMONSTRATION DU LEMME. Le circuit C utilise des paramètres $\bar{a}$ de K. Soit α un élément transcendant sur K situé dans une extension de K. Supposons que α appartienne au sous-ensemble S de $K(\alpha)$ accepté par C. Sur l'entrée α, le circuit C effectue des tests de la forme "$P(\alpha) = 0$?", et répond non, sauf si P est le polynôme nul. Le circuit effectue au plus τ tests, et les polynômes sont de degrés inférieurs à 2^τ. Si tous les polynômes calculés sont identiquement nuls, alors pour toute entrée x les calculs sont les mêmes, et l'ensemble S est $K(\alpha)$ tout entier. Dans le cas contraire, si un élément x de $K(\alpha)$ n'appartient pas à S, c'est que les réponses aux tests de C ne sont pas les mêmes pour x et pour α, qui annule au moins un de ces polynômes non nuls. Le complémentaire de S est donc de cardinal au plus $\tau 2^\tau$. Le raisonnement est le même si nous supposons que C refuse α. ⊣

Considérons maintenant un ensemble X de suites de longueur n d'éléments de K. Étant donnée une suite $\bar{x} = (x_1, \ldots, x_n)$, peut-on décider si $\bar{x}$ appartient à X à l'aide d'un circuit sur le corps K ? Cela revient à demander si X est définissable par une formule sans quantificateurs à paramètres dans K.

DÉFINITIONS 2. Soit X un ensemble de suites finies de longueurs quelconques d'éléments de K. L'ensemble X est appelé *problème*. Il est $D_K(A)$, c'est-à-dire définissable, au sens des corps, à paramètres dans un sous-ensemble A de K, s'il existe une suite de formule $(\phi_n(x_1, \ldots, x_n, \bar{a}_n))_{n\geq 1}$ du premier ordre du langage des corps à paramètres $(\bar{a}_n)$ dans A, telle qu'un n-uple $\bar{b}$ d'éléments de K appartient à X si et seulement si $K \models \phi_n(\bar{b}, \bar{a}_n)$.

Pour étudier la complexité des problèmes, nous devons utiliser des formules sans quantificateurs et limiter leur taille. Pour cela, nous utilisons les circuits.

DÉFINITIONS 3. Un problème X est $P_K/poly$ s'il existe un polynôme p et une suite de circuits au sens des corps $(C_n(x_1, \ldots, x_n, \bar{a}_n))_{n\geq 1}$ à paramètres $(\bar{a}_n)$ dans K, tels que pour tout n la taille de C_n soit bornée par $p(n)$ et pour tout n-uple $\bar{b}$ de K, $\bar{b}$ appartienne à X si et seulement si $C_n(\bar{b}, \bar{a}_n)$ calcule 1. En particulier, $\bar{a}_n$ peut contenir la description d'un circuit. Le problème X est $\mathbb{P}_K$ si de plus, les paramètres $\bar{a}$ sont les mêmes pour toute la suite : pour tout n entier, $\bar{a}_n = \bar{a}$. Cette classe est appelée non-uniforme car on n'indique pas comment les circuits sont obtenus : ils sont donnés a priori. Un circuit $C_n(\bar{x}, \bar{y})$ sans paramètre est un graphe et peut être codé par une suite de booléens. Il peut donc être produit par un algorithme standard, c'est à dire qui travaille sur les booléens, par exemple par une machine de Turing. Un problème est P_K s'il est $\mathbb{P}_K$ et s'il existe un polynôme q et une machine de Turing qui sur l'entrée n produit la sortie $C_n(\bar{x}, \bar{y})$ en temps au plus $q(n)$.

L. Blum, F. Cucker, M. Shub et S. Smale ont montré ([1]) la stabilité polynomiale, ou P-stabilité, de la théorie des corps de caractéristique nulle :

PROPOSITION 1 (P-stabilité de la théorie des corps).

Soit k un sous-corps de caractéristique nulle de K. Alors, la restriction à k d'un problème P_K est P_k.

Le théorème est encore valable dans le cas non-uniforme. Cela signifie en particulier qu'on peut tester l'appartenance d'un uple de k à un problème P_K en utilisant uniquement des paramètres de k. La démonstration s'appuie sur le lemme des témoins, qui utilise la notion de hauteur d'un nombre algébrique et d'un polynôme, et que nous allons utiliser dans la démonstration de la proposition 5.

Nous pouvons enrichir notre structure de corps d'une dérivée : c'est une fonction d de K dans K qui vérifie pour tout couple (x, y) d'éléments de K : $d(x + y) = dx + dy$ et $d(xy) = xdy + ydx$. Nous obtenons un corps différentiel K. Les circuits au sens des corps différentiels sont définis comme les circuits au sens des corps, mais certaines portes peuvent être étiquetées par d : elles ne reçoivent qu'une flèche et calculent la dérivée. Nous pouvons définir de la même façon que pour les corps les classes $P_K^d/poly$, $\mathbb{P}_K^d$ et P_K^d. La théorie des corps différentiels de caractéristique nulle est P-stable, au niveau uniforme comme au niveau non-uniforme ([6]). La démonstration de cette propriété s'appuie sur le lemme de réduction, qui permet de ramener dans certaines circonstances un circuit sur un corps différentiel à un circuit sur un corps, et qui nous sera utile par la suite.

DÉFINITION 4. Un circuit sur un corps différentiel est *réduit* si toutes les portes de dérivation reçoivent leur flèche d'une autre porte de dérivation ou d'une entrée, ou autrement dit si le calcul dans le circuit peut commencer par les dérivations et continuer par les opérations arithmétiques et les tests.

LEMME 2 (Lemme de réduction, [6]). *Tout circuit $A(\bar{x})$ de taille τ sur le corps différentiel K est équivalent à un circuit réduit $B(\bar{x})$ sur le corps différentiel K, de taille au plus $4\tau^3$ (pour τ suffisamment grand). De plus, $B(\bar{x})$ peut être obtenu à partir de $A(\bar{x})$ par un algorithme standard en temps polynômial en τ.*

La dérivée permet-elle d'augmenter le pouvoir algorithmique et de résoudre plus vite un problème ? Y-a-t'il des problèmes qui soient P_K^d mais pas P_K ? Il est clair qu'en général, il existe des problèmes P_K^d qui ne sont même pas définissables sans la dérivée. En effet si la dérivée n'est pas identiquement nulle sur K l'ensemble des constantes, i.e. des éléments de dérivée nulle, est un sous-corps de K et n'est donc pas définissable au sens des corps. Limitons nous donc aux problèmes qui sont définissables au sens des corps ; pour ceux-ci, la question est ouverte. Si les seuls paramètres utilisés sont des paramètres constants, c'est à dire de dérivée nulle, alors la dérivée ne permet pas d'accélérer les problèmes.

PROPOSITION 2. *Si K est un corps différentiel algébriquement clos, si k est un sous-corps algébriquement clos de son corps des constantes, alors*

$$P_K^d \cap D_K(k) = P_K \cap D_K(k)$$

DÉMONSTRATION DE LA PROPOSITION. Soit Π un problème P_K^d, défini par la suite de circuits $(A_n(\bar{x}, \bar{a}))_{n\geq 1}$. Supposons que Π soit défini par la suite de formules du premier ordre du langage des corps $(\phi_n(x_1, \ldots, x_n, \bar{c}_n))_{n\geq 1}$ où les $\bar{c}_n$ sont des paramètres de k. La restriction Π_k de Π à k est P_k grâce à la P-stabilité de la théorie des corps de caractéristique nulle. Il existe une suite de circuits $(B_n(\bar{x}, \bar{y}))_{n\geq 1}$ qui peut être obtenue par un algorithme standard travaillant en temps polynômial et un uple $\bar{b}$ de constantes tels que $(B_n(\bar{x}, \bar{b}))_{n\geq 1}$ décide de Π_k. Le corps k vérifie pour tout entier n la formule du langage des corps : $\forall \bar{x}(\phi_n(\bar{x}, \bar{c}_n) \leftrightarrow B_n(\bar{x}, \bar{b}))$. Comme k et K sont des corps algébriquement clos, K satisfait aussi ces formules, et donc Π est P_K grâce aux circuits $(B_n(\bar{x}, \bar{b}))_{n\geq 1}$. ⊣

Si nous ne connaissons pas de problème accéléré par la dérivée, nous en connaissons par contre qui ne le sont pas : ils ne sont pas décidables en temps polynomial avec la dérivée, même si nous autorisons un nombre polynomial de paramètres. Commençons par définir les problèmes.

Une fonction croît doucement si elle vérifie les conditions du lemme suivant :

LEMME 3. *Soit f une fonction de l'ensemble des entiers dans lui-même. Il existe un polynôme q tel que la fonction f soit majorée en $+\infty$ par 2^q si et seulement s'il existe un polynôme p et une suite de circuits $(A_n(x))_{n\geq 1}$ au sens des corps sans paramètre tels que $A_n(x)$ soit de taille au plus $p(n)$ et calcule $x^{f(n)}$.*

DÉMONSTRATION DU LEMME. Si une telle suite $(A_n(x))$ existe, alors pour tout n nous avons $f(n) \leq 2^{p(n)}$. Réciproquement, s'il existe un polynôme q tel que 2^q majore f en $+\infty$, alors pour n fixé suffisamment grand nous pouvons décomposer

$f(n)$ en base deux de cette manière :

$$f(n) = \sum_{i=0}^{q(n)-1} f_i 2^i,$$

où les f_i sont des booléens. Avec un circuit de taille $q(n)$, nous pouvons calculer les x^{2^i} pour i compris entre 0 et $q(n) - 1$. Et avec au plus $q(n) - 1$ portes de multiplication, nous calculons

$$x^{f(n)} = \prod_{i=0}^{q(n)-1} x^{f_i 2^i}.$$

⊣

Supposons que f soit une fonction de l'ensemble des entiers dans lui-même ne vérifiant pas les hypothèses du lemme. Nous pourrions par exemple choisir $f(n) = 2^{2^n}$, ce qui est beaucoup plus fort car alors f majore en $+\infty$ toutes les fonctions 2^q, où q est un polynôme. Soit a un élément d'un corps K.

DÉFINITION 5. Le problème des grandes racines de l'élément a est l'ensemble $GR_{f,a}$ des uples de la forme $(x_1, \ldots, x_n)$, où n est un entier strictement positif, ${x_1}^{f(n)} = a$ et $x_2, \ldots, x_n$ sont des éléments de K. Le problème des grandes puissances de l'élément a est l'ensemble $GP_{f,a}$ des uples de la forme $(a^{f(n)}, x_2, \ldots, x_n)$. où n est un entier strictement positif et $x_2, \ldots, x_n$ des éléments de K .

THÉORÈME 3. *Si K est un corps différentiel algébriquement clos, $GR_{f,a}$ n'est pas P_K^d ni même $P_K^d/poly$.*

DÉMONSTRATION DU THÉORÈME. Soit

$$X = \left\{ x \in K : dx = \frac{1}{f(n)} \frac{da}{a} x \right\}.$$

Pour tout entier n, il existe un paramètre b_n de K tel que pour tout x de X : $x^{(n)} = b_n x$. L'ensemble X n'est pas vide car il contient les solutions de $x^{f(n)} = a$. D'autre part, le corps des constantes est infini, et X est stable par multiplication par une constante. Il est donc infini.

Supposons que $GR_{f,a}$ soit P_K^d/poly. Il existe un polynôme p et une suite de circuits de décision au sens des corps différentiels $(C_n(x_1, \ldots, x_n, \bar{c}_n))_{n \geq 1}$, où les $\bar{c}_n$ sont des éléments de K, tel que C_n soit de taille au plus $p(n)$ et $(x_1, \ldots, x_n)$ appartienne à $GR_{f,a}$ si et seulement si $C_n(x_1, \ldots, x_n, \bar{c}_n)$ calcule 1. En fixant $(x_2, \ldots, x_n)$, par exemple à $(0, \ldots, 0)$, nous obtenons une suite de circuits à une seule variable x_1. Nous pouvons appliquer le lemme de réduction à ces circuits. Nous obtenons un polynôme q et une suite de circuits réduits au sens des corps différentiels $(A_n(x_1, \bar{c}_n))_{n \geq 1}$, avec A_n de taille au plus $q(n)$. Nous ajoutons aux paramètres $\bar{c}_n$ toutes leurs dérivées jusqu'à l'ordre $q(n)$, ainsi que les paramètres $\bar{b}_n = (b_1, \ldots, b_{q(n)})$, et nous remplaçons dans le circuit A_n l'éventuelle porte qui calcule $x_1^{(n)}$ par une porte qui calcule $b_n x_1$. Nous obtenons un polynôme r et une suite de circuits au sens des corps $(E_n(x_1, \bar{e}_n))_{n \geq 1}$ avec E_n de taille au plus $r(n)$, et telle que pour tout élément x_1 de X, $x_1^{f(n)} = a$ si et seulement si $E_n(x_1, \bar{e}_n)$ calcule 1. Pour tout entier n, l'ensemble des x_1 de X qui vérifient $x_1^{f(n)} = a$ est de cardinal $f(n)$. Or d'après le lemme 1, l'ensemble des x_1 qui satisfont E_n est soit cofini, ce

qui implique ici infini, soit de cardinal au plus $r(n)2^{r(n)}$. Pour n assez grand, $f(n)$ est strictement supérieur à $r(n)2^{r(n)}$. Donc Π n'est pas P_K^d/poly. ⊣

La démonstration est encore valable si le corps n'est pas algébriquement clos, mais contient un bon nombre de racines de a : si $g(n)$ est le nombre de solutions de l'équation $x^{f(n)} = a$ dans K, il faut que g ne soit majorée par aucun polynôme. Dans le cas contraire, le problème est P_K/poly et donc P_K^d/poly : il suffit d'ajouter les racines $f(n)$-ième de a comme paramètres du n-ième circuit.

Étudions maintenant le problème des grandes puissances. C'est un problème P_K/poly : il est immédiat de tester si $x = a^{f(n)}$ si la constante $a^{f(n)}$ est fournie au circuit. Si a est nul ou égal à 1, $GP_{f,a}$ est trivialement P_K.

LEMME 4. *Si a est une racine de l'unité d'ordre ρ strictement supérieur à 1, soit $r(n)$ le reste de la division euclidienne de $f(n)$ par ρ, et R l'ensemble des n-uples $(r(n), 0, \ldots, 0)$ pour tout entier strictement positif n. Alors $GP_{f,a}$ est P_K si et seulement si R l'est. Ceci est encore valable pour les classes P_K^d, $\mathbb{P}_K$ et $\mathbb{P}_K^d$.*

DÉMONSTRATION DU LEMME. Supposons que $GP_{f,a}$ soit P_K. Il existe une suite de circuits $(A_n(\bar{x}, \bar{y}))$ produite par un algorithme standard travaillant en temps polynomial et des paramètres $\bar{\alpha}$ tels que $x_1 = a^{f(n)}$ si et seulement si $A_n(\bar{x}, \bar{\alpha})$ calcule 1. Pour un tel $\bar{x}$, nous avons $x_1 = a^{r(n)}$. Pour décider si $y_1 = r(n)$, nous procédons de la manière suivante : nous commençons par tester si y_1 est un entier compris entre 0 et $\rho - 1$. Sinon, il ne peut être égal à $r(n)$. Puis, nous calculons a^{y_1}, et nous le comparons à $a^{f(n)}$ grâce au circuit A_n. S'ils sont égaux, alors $y_1 = r(n)$.

Réciproquement, si R est P_K, il existe une suite de circuits $(A_n(\bar{x}, \bar{y}))$ produite par un algorithme standard travaillant en temps polynomial et des paramètres $\bar{\alpha}$ tels que $x_1 = r(n)$ si et seulement si $A_n(\bar{x}, \bar{\alpha})$ calcule 1. En calculant $A_n(0, \ldots, 0, \bar{\alpha})$, $\ldots$, $A_n(\rho - 1, 0, \ldots, 0, \bar{\alpha})$, nous testons si $r(n) = 0, \ldots, r(n) = \rho - 1$, et nous en déduisons $r(n)$. Il est ensuite facile de calculer $a^{r(n)}$ puis de tester si $x_1 = a^{r(n)}$. Ceci nous prouve que $GP_{f,a}$ est P_K.

La démonstration est identique pour les autres classes de complexité. ⊣

REMARQUE. S'il existe une suite de circuits au sens des corps de taille polynomiale, dont les sorties ne sont plus nécessairement des portes de test, et calculent f, nous pouvons en déduire une suite qui calcule $r(n)$, et donc $GP_{f,a}$ est $\mathbb{P}_K$. Si de plus la suite qui calcule f est produite par un algorithme standard en temps polynomial, alors $GP_{f,a}$ est P_K.

PROPOSITION 4. *Si a n'est ni 0 ni une racine de l'unité, $GP_{f,a}$ n'est pas $\mathbb{P}_K$, ni même $\mathbb{P}_K^d$.*

Étudions le cas où a est algébrique sur $\mathbf{Q}$ sans être ni 0 ni une racine de l'unité :

LEMME 5. *Si K est l'ensemble des nombres algébriques $\bar{\mathbf{Q}}$ et si a n'est ni 0 ni une racine de l'unité, alors $GP_{f,a}$ n'est pas P_K, ni même $\mathbb{P}_K$.*

Pour le montrer, nous avons besoin d'une fonction de K dans $\mathbf{R}$, appelée hauteur, utilisée dans [1] pour montrer le lemme des témoins, et qui vérifie les propriétés (P) suivantes :

- $H(1) = H(0) = 1$, $H(2) = 2$, et pour tout w, $H(w) \geq 1$ et $H(-w) = H(w) = H(1/w)$

- pour tous v et w, $H(v+w) \leq 2H(v)H(w)$, et par récurrence pour tout uple $(v_0, \ldots, v_n)$, $H(\sum_{i=0}^{n} v_i) \leq 2^n \prod_{i=0}^{n} H(v_i)$
- pour tout w et tout entier n, $H(w^n) = H(w)^n$, et pour tous v et w, $H(vw) \leq H(v)H(w)$
- pour tous v et w, $H(v+w) \geq \frac{1}{2}\frac{H(v)}{H(w)}$
- pour tout v et pour tout w non nul, $H(vw) \geq \frac{H(v)}{H(w)}$

Nous noterons par H la hauteur classique sur $\bar{\mathbf{Q}}$, définie par exemple dans le livre de S. Lang ([3]). Sur $\mathbf{N}$, H est confondue avec la valeur absolue classique. Si $\frac{a}{b}$ est un élément de $\mathbf{Q}$ sous forme irréductible, alors $H(\frac{a}{b}) = \max(|a|, |b|)$. Si α est un élément de $\bar{\mathbf{Q}}$, il est racine d'un polynôme M à coefficients entiers premiers entre eux et irréductible dans $\boldsymbol{Z}[X]$. Si a_d est son coefficient dominant et A l'ensemble de ses racines, alors $H(\alpha) = |a_d| \prod_{\alpha_i \in A} \max(1, |\alpha_i|)$ c'est la mesure de Mahler de M (cf. [2]).

Pour montrer le lemme 5, nous utilisons les définitions et le lemme suivant, qui se montre facilement à partir des propriétés (P) ([1]) :

DÉFINITIONS 6 ([1]). Si $\bar{u} = (u_1, \ldots, u_n)$ est un uple d'éléments de $\bar{\mathbf{Q}}$, alors sa hauteur $H(\bar{u})$ est le maximum des hauteurs $H(u_i)$, pour i compris entre 1 et n. Si P est un polynôme sur $\bar{\mathbf{Q}}$, en une ou plusieurs variables, alors sa hauteur $H(P)$ est le produit des hauteurs de ses coefficients.

LEMME 6. *Soit P un polynôme à une variable et à coefficients dans $\bar{\boldsymbol{Q}}$, de degré d. Soit x un élément de $\bar{\mathbf{Q}}$ qui vérifie : $H(x) > 2^d H(P)$. Alors x est racine de P si et seulement si P est le polynôme nul.*

Nous pouvons maintenant énoncer un résultat de majoration de la hauteur d'un polynôme :

LEMME 7. *Soit P un polynôme en une variable x produit par un circuit au sens des corps de taille τ ayant pour entrée x ainsi que les paramètres $\bar{b} = (b_1, \ldots, b_r)$ de $\bar{\mathbf{Q}}$. Alors :*

$$H(P) \leq 2^{(2^\tau+1)^{2r+2} \log_2 H(\bar{b})}.$$

DÉMONSTRATION DU LEMME 7. Le polynôme P est de degré au plus 2^τ, et les coefficients de P peuvent s'écrire sous la forme :

$$c = \sum_{0 \leq \alpha_1, \ldots, \alpha_r \leq 2^\tau} n_{\alpha_1 \ldots \alpha_r} b_1^{\alpha_1} \ldots b_r^{\alpha_r}$$

où les $n_{\alpha_1 \ldots \alpha_r}$ sont des entiers strictement inférieurs en valeur absolue à 2^{2^τ}, et $\alpha_1 + \cdots + \alpha_r \leq 2^\tau$. Nous avons alors :

$$H(c) \leq 2^{(2^\tau+1)^r - 1} \prod_{0 \leq \alpha_1, \ldots, \alpha_r \leq 2^\tau} H(n_{\alpha_1 \ldots \alpha_r}) H(b_1)^{\alpha_1} \ldots H(b_r)^{\alpha_r}$$

et donc

$$H(c) \leq 2^{(2^\tau+1)^r - 1} (2^{2^\tau} H(\bar{b})^{2^\tau})^{(2^\tau+1)^r} = 2^{(2^\tau+1)^r - 1} 2^{2^\tau (2^\tau+1)^r (1 + log_2 H(\bar{b}))}$$

en majorant grossièrement, nous obtenons

$$H(P) \leq 2^{(2^\tau+1)^{2r+2} \log_2 H(\bar{b})} \quad \dashv$$

Pour montrer que seules les racines de l'unité et 0 sont de hauteur 1, nous utilisons un théorème de Kronecker ([4]) :

THÉORÈME 5 (Kronecker, 1895). *Si toutes les racines d'un polynôme à coefficients entiers sont de module* 1, *alors ce sont des racines de l'unité.*

Nous en déduisons le

COROLLAIRE 1. *Si x est un élément de $\bar{\mathbf{Q}}$, alors $H(x) = 1$ si et seulement si x est* 0 *ou une racine de l'unité.*

DÉMONSTRATION DU COROLLAIRE. Si la hauteur de x est 1, alors le coefficient dominant de son polynôme minimal à coefficients entiers premiers entre eux M est de module 1, et toutes ses racines sont de module au plus 1. Donc le coefficient constant de M est de module au plus 1. Comme il est entier, il est égal à 0, 1 ou -1. S'il est nul, alors $M(X) = X$ et $x = 0$. Sinon, il est de module 1 et donc toutes les racines de M sont de module 1. D'après le théorème de Kronecker, ceci entraîne que x est une racine de l'unité. ⊣

Nous pouvons maintenant montrer le lemme 5 : Supposons que le problème $GP_{f.a}$ soit $\mathbb{P}_K$. Alors, il existe des paramètres $\bar{b} = (b_1, \ldots, b_r)$, un polynôme p et une suite de circuits au sens des corps $(C_n(x_1, \ldots, x_n, y_1, \ldots, y_r))_{n\geq 1}$ tels que pour tout entier strictement positif n, le circuit $C_n(\bar{x}, \bar{b})$ soit de taille au plus $p(n)$ et calcule 1 si et seulement si $x_1 = a^{f(n)}$. Si nous fixons les entrées $x_2, \ldots, x_n$ du circuit C_n à $(0, \ldots, 0)$, nous obtenons un circuit de même taille et qui reconnaît le même ensemble. Nous supposons donc que les entrées du circuit C_n sont x_1 et $\bar{b}$.

Lors du calcul sur l'entrée $a^{f(n)}$, le circuit effectue au moins un test de la forme $P_n(x_1, \bar{b}) = 0?$, où P_n est un polynôme non nul en x_1 et à coefficients entiers, et $P_n(a^{f(n)}, \bar{b}) = 0$. En effet, si ce n'était pas le cas, le circuit reconnaîtrait un ensemble infini. Le polynôme P_n est de degré total au plus $d_n = 2^{p(n)}$. Notons $Q_n(x_1)$ le polynôme P_n pour lequel les dernières variables sont fixées à $\bar{b}$. Par hypothèse, Q_n n'est pas identiquement nul. D'après la proposition 7, nous avons :

$$H(Q_n) \leq 2^{(2^{p(n)}+1)^{2r+2} \log_2 H(\bar{b})}$$

Or la hauteur de $a^{f(n)}$ est $H(a)^{f(n)}$, c'est-à-dire $2^{f(n)\log_2(H(a))}$. Et pour un entier n suffisamment grand :

$$2^{f(n)\log_2(H(a))} > 2^{2^{p(n)}} 2^{(2^{p(n)}+1)^{2r+2} \log_2 H(\bar{b})} > 2^{d_n} H(Q_n)$$

et donc, alors que $a^{f(n)}$ est racine du polynôme non nul Q_n :

$$H(a^{f(n)}) > 2^{d_n} H(Q_n)$$

ce qui contredit le lemme 6. ⊣

LEMME 8. *Si a est transcendant sur $\mathbf{Q}$, alors $GP_{f.a}$ n'est ni P_K ni $\mathbb{P}_K$.*

DÉMONSTRATION DU LEMME. Si $GP_{a.f}$ est $\mathbb{P}_K$, alors il est $\mathbb{P}_{\mathbf{Q}(a)}$ ($\mathbb{P}$-stabilité de la théorie des corps). Soit p un polynôme et $(A_n(x_1, \ldots, x_n, a))_{n\geq 1}$ une suite de circuits au sens des corps de taille bornée par p qui décide de $GP_{a.f}$. Fixons les variables $(x_2, \ldots, x_n)$ à $(0, \ldots, 0)$.

Le circuit A_n effectue des tests de la forme "$P(x_1, a) = 0?$". Le polynôme P est à coefficients dans $\mathbf{Q}$. Il est de degré total au plus $2^{p(n)}$. S'il est de degré r supérieur ou égal à 2 en x_1, alors le terme dominant de $P(a^{f(n)}, a)$ vu comme un polynôme en a

est de degré au moins $rf(n)$, et le terme suivant de degré au plus $(r-1)f(n)+2^{p(n)}$. Et pour n suffisamment grand, $f(n) > 2^{p(n)}$ et donc $rf(n) > (r-1)f(n) + 2^{p(n)}$. Comme a est transcendant sur $\mathbf{Q}$, le terme dominant ne peut être annulé par les autres termes du polynôme, et l'expression $P(a^{f(n)}, a)$ est nulle si et seulement si le polynôme $P(x_1, a)$ est identiquement nul. Dans ce cas, il s'annule pour toute entrée x_1, ce qui signifie que le test peut être remplacé par la constante 1. Si le circuit n'effectue aucun test, l'ensemble reconnu est soit vide, soit $\mathbf{Q}(a)$ tout entier.

Le circuit A_n effectue donc sur l'entrée $a^{f(n)}$ des tests polynomiaux de la forme "$P(x_1, a) = 0$?", avec $P(a^{f(n)}, a) \neq 0$ (au moins 1). Le polynôme $P(x_1, a)$ n'est pas identiquement nul en x_1. Et donc, pour la même raison que précédemment, $P(2a^{f(n)}, a) \neq 0$. Les calculs de A_n sur les entrées $a^{f(n)}$ et $2a^{f(n)}$ sont rigoureusement identiques, ce qui est impossible. ⊣

Si K est un corps différentiel, nous pouvons maintenant nous demander si $GP_{f,a}$ est $\mathbb{P}_K^d$. Pour cela, il faut nécessairement que sa restriction à son corps des constantes k soit P_k. Or la restriction de $GP_{f,a}$ à k est lui-même si a est une constante, et l'ensemble vide sinon. Donc :

COROLLAIRE 2. *Si a n'est ni 0 ni une racine de l'unité mais est une constante, alors $GP_{f,a}$ n'est ni $\mathbb{P}_K$ ni $\mathbb{P}_K^d$.*

Il nous reste à traiter le cas où a n'est pas une constante. Un élément algébrique a sur $\mathbf{Q}$ est de dérivée nulle. En effet, si $M(X)$ est son polynôme minimal, de dérivé $N(X)$ de degré strictement inférieur, alors $dM(a) = dadN(a) = 0$ et donc $da = 0$. D'autre part, un élément a est différentiellement algébrique, ou *d-algébrique*, sur un sous-corps k de K s'il annule un polynôme différentiel non nul à coefficients dans k. Dans le cas contraire, a est différentiellement transcendant, ou *d-transcendant*, sur k.

LEMME 9. *Si a est d-transcendant ou d-algébrique sur $\mathbf{Q}$ et non constant, $GP_{f,a}$ n'est pas $\mathbb{P}_K^d$.*

DÉMONSTRATION DU LEMME. Notons $\mathbf{Q}(a)_d$ le corps différentiel engendré par a. Si $GP_{f,a}$ est $\mathbb{P}_K^d$, alors il est $\mathbb{P}_{\mathbf{Q}(a)_d}^d$ car la théorie des corps différentiel de caractéristique nulle est $\mathbb{P}$-stable. Il existe donc un polynôme p et une suite de circuits au sens des corps différentiels $(C_n(x_1, \ldots, x_n, a))_{n\geq 1}$ tels que pour tout entier strictement positif n, le circuit $C_n(\bar{x}, a)$ soit de taille au plus $p(n)$ et calcule 1 si et seulement si $x_1 = a^{f(n)}$. Nous fixons $x_2, \ldots, x_n$ à $(0, \ldots, 0)$: les entrées du circuit C_n sont x_1 et a.

Si $x = a^{f(n)}$, alors $dx = f(n)\frac{da}{a}x$, et pour tout entier r, il existe un polynôme différentiel P_r à coefficients entiers tel que $d^r x = P_r(\frac{da}{a})x$. Le polynôme différentiel P_{r+1} est donné par la relation de récurrence : $P_{r+1}(X) = \frac{da}{a}P_r(X) + dP_r(X)$ et $P_1(X) = f(n)X$.

Nous commençons par ajouter le paramètre $f(n)$ au circuit C_n. Puis nous réduisons les circuits. Nous remplaçons le calcul des dérivées successives de x_1 par celui des P_r. Nous réduisons à nouveau. Nous obtenons des circuits $A_n(x_1, a, f(n))$ de tailles polynomiales et bornées par le polynôme q dans lesquels les seules dérivations sont les dérivations successives du paramètre a, et qui décide de $x_1 = a^{f(n)}$ pour les entrées x_1 de l'ensemble infini $X = \{ x \,/\, dx = f(n)\frac{da}{a}x \}$.

Supposons que a soit d-transcendant sur $\mathbf{Q}$. Le circuit A_n effectue des tests de la forme "$P(x_1, a, da, \ldots, d^{q(n)}a, f(n)) = 0$?", où P est un polynôme à coefficients dans $\mathbf{Q}$ de degré total au plus $2^{q(n)}$. Pour les mêmes raisons que dans la démonstration du lemme 8, P s'annule en $a^{f(n)}$ si et seulement s'il est identiquement nul en x_1. Nous en déduisons que le circuit A_n accepte $2a^{f(n)}$, ce qui est impossible.

Supposons maintenant que a soit d-algébrique sur $\mathbf{Q}$. Soit r l'ordre de son polynôme différentiel minimal, qui est à coefficients dans $\mathbf{Q}$. Il existe une suite de circuits au sens des corps $(B_n(x_1, a, \ldots, a^{(r)}, f(n)))$ de taille polynomiale et équivalente à la suite $(A_n(x_1, a, f(n)))$ pour les entrées x_1 appartenant à X. En effet, formons le circuit différentiel qui calcule $a^{(r+1)}$ avec comme entrées $a, \ldots, a^{(r)}$. Puis mettons $q(n)$ dérivées successives sous $a^{(r+1)}$. Réduisons le circuit obtenu. Le calcul de $a^{(r+2)}$ n'utilise que les dérivées d'ordre inférieur à $r+1$. Nous remplaçons donc celles des dérivées successives des entrées qui calculent $a^{(r+2)}$ par la porte qui le calcule en utilisant seulement les $r+1$ premières dérivées, c'est à dire que les flèches qui partaient de celles-là partent maintenant de celle-ci. Par récurrence, nous supprimons toutes les portes de dérivées. Nous obtenons un circuit E_n qui a pour entrées $(a, \ldots, a^{(r)})$ et qui calcule les dérivées de a jusqu'à l'ordre $q(n)$. Nous ajoutons le circuit E_n au circuit A_n et remplaçons les dérivées successives de a d'ordre supérieur à r dans le circuit A_n par les portes du circuit E_n qui les calculent Nous obtenons un circuit B_n qui n'a pas de porte de dérivation. Or nous avons $\boldsymbol{Q}(a)_d = \boldsymbol{Q}(a, \ldots, a^{(r)})$. En utilisant la P-stabilité des corps, nous obtenons une suite de circuits $(\Gamma_n(x_1, a, f(n)))$ équivalent à $(A_n(x_1, a, f(n)))$ pour les entrées x_1 appartenant à $Y = X \cap \mathbf{Q}(a)$, qui est un ensemble infini. Le paramètre a est transcendant sur $\mathbf{Q}$. Comme $2a^{f(n)} \in Y$, nous pouvons conclure comme au lemme 8. ⊣

REFERENCES

[1] LENORE BLUM, FELIPE CUCKER, MIKE SHUB, and STEVE SMALE, *Algebraic settings for the problem "$P \neq NP$?"*, ***Mathematics of numerical analysis*** (Renegar et al., editors), Lectures in Applied Mathematics, vol. 32, 1996, pp. 125–144.

[2] GRAHAM EVEREST, *Measuring the height of a polynomial*, ***The Mathematical Intelligencer***, vol. 20 (1998), no. 3, pp. 9–16.

[3] SERGE LANG, ***Fundamentals of diophantine geometry***, Springer-Verlag, 1983.

[4] WLADYSLAW NARKIEWICZ, ***Elementary and analytic theory of algebraic numbers***, Springer-Verlag, PWN-Polish Scientific Publishers, 1990.

[5] B. POIZAT, ***Les petits cailloux* (Aleas, editor)**, 1995.

[6] NATACHA PORTIER, *Stabilité polynômiale des corps différentiels*, à paraître dans this JOURNAL.

LABORATOIRE SE L' INFORMATIQUE DU PARALLEÉLISME
ÉCOLE NORMAL SUPÉRIEURE DE LYON
64 ALLE'EE D' ITALIE
69634 LYON CEDEX 07. FRANCE
E-mail: nportier@ens-lyon.fr