Le problème des grandes puissances et celui des grandes racines : une introduction à la complexité sur les corps et les corps différentiels

Natacha Portier

Tous les corps considérés sont de caractéristique nulle.

Je vous donne un élément a d'un corps K, et un élément x, et je vous demande si $x = a^6$. Comment faire ? Vous avez le droit de multiplier, d'additionner ou de soustraire deux éléments du corps, et de tester si un élément est nul. Il suffit de multiplier a par lui-même pour obtenir a^2, puis a^2 par lui-même pour obtenir a^4, puis a^2 par a^4 pour obtenir a^6, de soustraire x et de tester si le résultat obtenu est 0.

Il vous a fallu 5 opérations pour répondre à la question, ou 7 si on prend en compte le fait de regarder x et a au départ. Si on suppose que chaque opération prend le même temps, alors il vous a fallu un temps 7 pour répondre à la question. Si je vous demande maintenant si x est égal à a^{2^n}, vous pourrez répondre à la question en $n + 4$ opérations.

On regroupe les questions en problèmes. Un problème X est un ensemble de uples $(x_1, ..., x_n)$ de K, de différentes longueurs n. Par exemple, pour a fixé, $X_a = \{(x_1, ..., x_n)/x_1 = a^{2^n}\}$. Si $\bar{x} = (x_1, ..., x_n)$ est un uple d'éléments de K, on s'intéresse à la question $\bar{x} \in X$? Etudier la complexité des problèmes, c'est vouloir les classer selon le temps qu'il faut pour répondre aux questions en fonction de la taille n de la donnée. En simplifiant, si le temps pour répondre est borné par un polynôme de la taille de la donnée, on dit que le problème est polynomial (le problème est P). C'est le cas de l'exemple X_a. On parle de complexité algébrique car les opérations qu'on peut faire sont des opérations algébriques et qu'on peut tester un certain nombre de relations sur l'ensemble considéré, ici le corps K.

Certains problèmes se résolvent en temps polynomial pour peu qu'on donne une indication : c'est le cas par exemple des systèmes d'équations polynomiales. Etant donné un tel système, il n'est pas facile de savoir s'il a une solution. Par contre, si on donne un candidat, c'est facile et polynomial de tester si c'est bien une solution. La classe des problèmes de ce type est appelée NP. La lettre N signifie non déterministe, car cela revient à tirer un uple au hasard pour voir si c'est une solution. La complexité est définie plus précisément pour les anneaux dans le livre de L. Blum, F. Cucker, M. Shub et S. Smale [**?**], et plus généralement pour un ensemble avec des opérations

quelconques dans le livre de B. Poizat ([**?**]).

Une des questions importantes en théorie de la complexité est de savoir si $P = NP$ dans l'ensemble considéré (ici le corps K). Comme en général on ne sait pas répondre, on montre des théorèmes de transfert, c'est à dire on regarde les liens entre $P = NP$ dans un ensemble et dans un autre :

Théorème ([**?**]) : la question $P = NP$? a la même réponse dans tous les corps algébriquement clos de caractéristique nulle.

Que se passe-t-il si on ajoute des opérations ? On munit par exemple K d'une structure de corps différentiel en ajoutant une dérivée. C'est une fonction d de K dans K telle que pour tout x et tout y de K, $d(x+y) = dx+dy$ et $d(xy) = xdy + ydx$. On peut alors, en autorisant cette nouvelle fonction dans les calculs, définir de nouvelles classes P et NP. D'autre part, on définit la notion de corps différentiellement clos K, qui sont aux corps différentiels ce que les corps algébriquement clos sont aux corps. Un corps est algébriqument clos si pour tout polynôme $P(X)$ non constant, il existe un élément x tel que $P(x) = 0$. L'axiomatisation des corps différentiellement clos est due à L. Blum ([**?**]) : pour tout polynôme différentiel $P(X)$, i.e. un polynôme de l'indéterminée X et de ses dérivées successives, et pour tout polynôme différentiel $Q(X)$ avec des dérivées de X plus grandes, il existe un élément x de K tel que $P(x) \neq 0$ et $Q(x) = 0$. Comment relier la complexité dans les corps et dans les corps différentiels ? On montre le théorème de transfert suivant :

Théorème ([**?**]) : La question $P = NP$? a la même réponse dans tous les corps différentiellement clos de caractéristique nulle. De plus, si $P = NP$ pour les corps différentiellement clos, alors $P = NP$ pour les corps algébriquement clos.

La réciproque est ouverte.

Ces théorèmes sont les conséquences d'une propriété des corps et des corps différentiels, la stabilité polynomiale : si k est un sous-corps de K, si X est un problème P sur K, alors sa restriction à k est encore P ([**?**]). C'est encore vrai si k est un sous-corps différentiel de K, et si on considère les classes de complexité au sens des corps différentiels ([**?**]). Cette propriété sert également à montrer le théorème des grandes puissances et des grandes racines (voir plus bas).

On peut se demander plus précisément dans quelle mesure une dérivée permet de répondre plus vite aux questions. Est-ce que tous les problèmes

deviennent polynomiaux avec une dérivée ? Ou est-ce qu'au contraire, les problèmes polynomiaux avec la dérivée sont exactement ceux qui l'étaient déjà sans ? L'étude d'exemples particuliers, le problème des grandes racines et celui des grandes puissances, permet de répondre négativement à la première question. On considère une fonction f de l'ensemble des entiers dans lui-même, qui croisse suffisamment vite, i.e. qui ne soit majorée par aucune exponentielle de polynôme. Le problème des grandes racines de l'élément a est l'ensemble des uples de la forme $(x_1, ..., x_n)$, où n est un entier strictement positif, ${x_1}^{f(n)} = a$ et $x_2, ..., x_n$ sont des éléments de K. Le problème des grandes puissances de l'élément a est l'ensemble des uples de la forme $(a^{f(n)}$, $x_2, ..., x_n)$, où n est un entier strictement positif et $x_2, ..., x_n$ des éléments de K. On peut alors donner une version simplifiée du théorème :

Théorème ([**?**]) : Si K est un corps algébriquement clos, le problème des grandes racines n'est polynomial ni sans la dérivée ni avec.

Si a n'est ni 0 ni une racine de l'unité, le problème des grandes puissances n'est polynomial ni sans la dérivée ni avec, même si on considère une définition moins forte des problèmes polynomiaux.

Pour montrer ce théorème, outre la stabilité polynomiale des corps et des corps différentiels, on utilise une notion d'arithmétique : la hauteur des nombres algébriques. La hauteur d'un rationnel x est définie (par exemple dans le livre de S. Lang [**?**]) comme le produit sur toutes les valeurs absolues classiques v (le module et les valeurs absolues p-adiques pour p premier) de $max(1, v(x))$. C'est le maximum des modules de son numérateur et de son dénominateur. Cette définition s'étend aux nombres algébriques en considérant les extensions de ces valeurs absolues sur des corps de nombres (i.e. des extensions finies du corps des rationnels). On peut donner une définition équivalente à l'aide de la mesure de Mahler (voir par exemple l'article de G. Everest [**?**]). Si α est un nombre algébrique, il est racine d'un polynôme de degré minimal à coefficients entiers premiers entre eux dans leur ensemble et de coefficient dominant a_d. Si A est l'ensemble des racines de ce polynôme, alors la hauteur de α est $H(\alpha) = |a_d| \prod_{\alpha_i \in A} max(1, |\alpha_i|)$. Quels sont les éléments algébriques de hauteur 1 ? D'après un théorème de Kronecker (1895), si toutes les racines d'un polynôme à coefficients entiers sont de module 1, alors ce sont des racines de l'unité. Ceci implique que les seuls nombres algébriques de hauteur 1 sont 0 et les racines de l'unité. C'est la raison pour laquelle on distingue ce cas dans le théorème des grandes puissances.

Nous savons maintenant que l'utilisation de la dérivée ne permet pas de répondre à toutes les questions en temps polynomial. Mais permet-elle au moins dans quelques cas de répondre plus vite ?

Références

[1] *Lenore Blum*, Generalized algebraic structures : A model theoretic approach. Thèse de Ph. D. , Massachussets Institute of Technology (1968)

[2] *Lenore Blum, Felipe Cucker, Mike Shub et Steve Smale* , Complexity and Real Computation. Springer Verlag (1998)

[3] *Graham Everest*, Measuring the Height of a Polynomial. The Mathematical Intelligencer, pp. 9–16, vol. 20, nb. 3, (1998)

[4] *Serge Lang*, Fundamentals of Diophantine Geometry. Springer Verlag (1983)

[5] *Bruno Poizat*, Les petits cailloux. ALEAS éditeur (1995)

[6] *Natacha Portier*, Stabilité polynomiale des corps différentiels. *Journal of Symbolic Logic*, Vol. 64, Number 2, June 1999, pp. 803-816

[7] *Natacha Portier*, Le problème des grandes puissances et celui des grandes racines. Á paraître dans le Journal of Symbolic Logic

Natacha Portier
Laboratoire de l'Informatique du Parallélisme
École Normale Supérieure de Lyon
46, Allée d'Italie
69364 LYON CEDEX 07
Natacha.Portier@ens-lyon.fr
http ://www.ens-lyon.fr/ nportier/