PUBLICATIONS MATHÉMATIQUES ET INFORMATIQUES DE RENNES

DOMINIQUE DUVAL

Au sujet de l'algorithme « de Coates »

Publications de l'Institut de recherche mathématiques de Rennes, 1985, fascicule 4
« Séminaires de mathématiques - science, histoire et société », , p. 196-206

<http://www.numdam.org/item?id=PSMIR_1985___4_196_0>

Université de Grenoble I

Institut Fourier

Laboratoire de Mathématiques
associé au CNRS

AU SUJET DE L'ALGORITHME "DE COATES"

par Dominique DUVAL

INTRODUCTION

Considérons un corps K, algébriquement clos et de caractéristique nulle, et un polynôme $F(X,Y)$ à coefficients dans K et irréductible (toutes ces hypothèses sont faites pour simplifier l'exposé).

Notons C la courbe de $\mathbb{P}_2(K)$ complétée projective de la courbe affine d'équation $F(x,y) = 0$. Le corps des fonctions algébriques sur C sera noté $K(C)$; il peut être décrit comme $K(X)[Y]/(F(X,Y))$, c'est une extension de $K(X)$ de degré $n = \deg_Y F$ (supposé ≥ 1).

Considérons aussi un diviseur $D = \sum_{\wp} n_\wp \wp$ sur C, c'est-à-dire un élément du groupe abélien libre engendré par les places $\wp$ du corps $K(C)$. L'ensemble des fonctions algébriques f sur C vérifiant $w_\wp(f) \geq -n_\wp$ en toute place $\wp$ de C (où $w_\wp$ désigne la valuation normalisée associée à $\wp$) forme un espace vectoriel sur K de dimension finie [Fu] et généralement noté $L(D)$.

L'algorithme "de Coates" calcule une base de l'espace vectoriel $L(D)$ sur K.

Le but de cet exposé est de donner quelques indications sur l'histoire de cet algorithme, d'en indiquer quelques applications, d'en donner le schéma, et de discuter certains problèmes posés par son implantation sur ordinateur.

UN PEU D'HISTOIRE

En 1970, Coates publie la description de cet algorithme "bien connu mais dont la preuve détaillée semble ne jamais avoir été donnée" [Co] . Il donne aussi une certaine mesure de sa complexité, entre autres en bornant le degré de l'extension K_1/K_0 , où K_0 (resp. K_1) désigne l'extension de $\mathbb{Q}$ engendrée par les coefficients de F (resp. par tous les nombres algébriques qui apparaissent dans l'algorithme).

En fait, cet algorithme était déjà décrit en 1933 par Bliss [Bl] et les idées essentielles étaient énoncées en 1882 par Dedekind et Weber [D-W] . Il s'agit pour eux d'une étape dans la démonstration du théorème de Riemann-Roch.

QUELQUES APPLICATIONS

• Codage des codes de Goppa : voir les exposés de Wolfmann et Michon à ce colloque. L'algorithme exposé ici s'adapte sans problème en caractéristique p tant que p est premier à n . Dans le cas contraire, l'extension $K(C)/K(X)$ peut-être inséparable ou sauvagement ramifiée et l'algorithme doit être modifié.

• Factorisation des polynômes de $K[X,Y]$: (voir [Du]). Si le polynôme $F(X,Y)$ n'est plus supposé irréductible mais seulement sans facteur multiple et sans facteur dans $K[X]$, la dimension de $L(0)$ est égale au nombre de facteurs irréductibles de F .

Il est ensuite possible de déterminer tous les facteurs de F en étudiant la suite d'espaces vectoriels

$$L(0) \supset L(-\wp_1) \supset L(-\wp_1-\wp_2) \supset \dots \supset L(-\wp_1-\wp_0 \dots -\wp_s) = 0$$

où $\wp_1, \wp_2, \dots, \wp_s$ désignent toutes les places de $K(C)$ divisant une

place fixée de $K(X)$.

• Intégration des fonctions rationnelles [Da, Tr] : le problème de calculer une primitive "élémentaire" d'une fonction de $K(C)$, ou de prouver qu'une telle primitive n'existe pas, a été résolu en 1970 par Risch [Ri] ; grâce à un théorème de Liouville, la problème est ramené à la détermination de l'ordre de la classe d'un diviseur D sur C (c'est-à-dire le plus petit entier N , s'il existe, tel que ND soit un diviseur de fonction, et $+\infty$ sinon) ; or ceci peut être résolu grâce aux résultats de A. Weil sur les courbes sur des corps finis.

La méthode donnée par Risch n'est guère applicable, et c'est à J. Davenport en 1979 [Da] qu'on doit la première méthode pratique, implantée sur le système REDUCE. Bien que limité à l'intégration des fonctions définies à partir de racines carrées (éventuellement emboitées), et peu efficace pour les courbes de genre ≥ 2 , ce système est déjà fort utile.

Plus récemment, Trager [Tr] a présenté un algorithme d'intégration qui devrait être beaucoup plus performant mais n'est pas encore implanté.

SCHEMA DE L'ALGORITHME

Les hypothèses et notations sont celles de l'introduction auxquelles il faut ajouter :

$$M(D) = \{ f \in K(C) , \forall \wp , w_\wp(f) \geq n_\wp \} = L(-D)$$

$$M^*(D) = \{ f \in K(C) , \forall \wp \neq \infty , w_\wp(f) \geq n_\wp \} .$$

L'algorithme procède en 2 temps :

1) ETUDE DE $M^*(D)$.

THEOREME 1. - $M^*(D)$ est un réseau de $K(C)$ par rapport à $K[X]$.

Autrement dit, $M^*(D)$ est un sous $K[X]$-module libre de rang n de $K(C)$.

On peut montrer ce théorème de la manière suivante :

- vérifier que $M^*(0)$ est la clôture intégrale de $K[X]$ dans $K(C)$;
- le théorème pour $D = 0$ est alors un résultat classique d'arithmétique [Se, I.4] .
- pour D quelconque, il existe λ et μ dans $K(X)^*$ tels que $\lambda M^*(0) \subset M^*(D) \subset \mu M^*(0)$, ce qui démontre le théorème 1 puisque l'anneau $K[X]$ est principal.

THEOREME 2. - Le discriminant de $M^*(D)$ est égal à $\prod_{\alpha \in K} (X-\alpha)^{\sum_{\wp|\alpha} (2n_\wp + e_\wp - 1)}$, où $e_\wp$ désigne l'indice de ramification de $\wp$ dans l'extension $K(C)/K(X)$.

Ce discriminant sera désormais noté $d(D)$.

Là encore, le résultat pour $D = 0$ est classique [Se, III.6] . Par ailleurs, on peut montrer que (pour tout diviseur D , tout $\alpha \in K$, et toute place $\wp|\alpha$, $d(D+\wp) = (X-\alpha)^2 d(D)$, et le théorème 2 en découle facilement.

1ère PARTIE DE L'ALGORITHME.

Détermination d'une base de $M^*(D)$ sur $K[X]$. Posons $(f_1, \ldots, f_n) = (1, y, \ldots, y^{n-1})$; c'est une base de $K(C)/K(X)$ de discriminant connu (c'est "presque" le discriminant en Y de F).

Multiplions chaque f_i par un λ_i de $K(X)^*$ tel que $\lambda_i f_i$ appartienne à $M^*(D)$. Notons encore $\{f_1,\dots,f_n\}$ cette nouvelle base de $K(C)$ sur $K(X)$.

(*) Si le discriminant d de $(f_1,\dots,f_n)$ est égal à $d(D)$, c'est une base de $M^*(D)$ sur $K[X]$ et l'algorithme est terminé.

Sinon, considérons un α de K tel que $v_\alpha(d) > \sum_{\wp|\alpha} (2n_\wp+e_\wp-1)$ (il n'y a qu'un nombre fini de tels α) et effectuons un "pas de réduction en α".

Une description précise d'un pas de réduction en α se trouve dans [Bl] , [Co] ou [Du] . Cela permet, en modifiant un des f_i , d'obtenir une autre base de $K(C)$ sur $K(X)$ contenue dans $M^*(D)$, dont le discriminant est égal à $d/(X-\alpha)^2$. Notons toujours $(f_1,..,f_n)$ cette nouvelle base et d son discriminant, et retournons en (*) .
Il est clair que cet algorithme s'arrête aprés un nombre fini de pas de réduction et que la base obtenue est une base de $M^*(D)$ sur $K[X]$.

Remarques.

Pour effectuer un pas de réduction, il faut appliquer l'algorithme d'élimination de Gauss à une matrice carrée d'ordre n à coefficients dans K . Ces coefficients sont des coefficients de développements de Puiseux des f_i au-dessus de α , et leur calcul introduit des nombres algébriques qui n'appartiennent pas à K_0 . Une partie de ces développements de Puiseux peut servir à la détermination des indices de ramification.

2) ETUDE DE M(D).

Définissons une application ν_D de $K(C)$ dans $\mathbb{Z} \cup \{+\infty\}$ par $\nu_D = \min_{\wp|\infty} \left[\frac{w_\wp(f) - n_\wp}{e_\wp}\right]$. Elle vérifie :

$$\begin{cases} \nu_D(f) = +\infty \Leftrightarrow f = 0 \\ \nu_D(f+g) \geq \min(\nu_D(f), \nu_D(g)) \\ \nu_D(\lambda f) = v_\infty(\lambda) + \nu_D(f) \quad \text{si} \quad \lambda \in K(X) \end{cases}$$

(où $v_\infty(\frac{\lambda_1}{\lambda_2}) = \deg(\lambda_2) - \deg(\lambda_1)$ si λ_1 et $\lambda_2 \in K[X]$).

Donc la fonction $\partial_D(f,g) = q^{-\nu_D(f-g)}$ (où q est un réel > 1 fixé) est une distance ultramétrique sur $K(C)$. Ce point de vue est celui d'Armitage [Ar].

La boule unité B_D pour cette distance est

$$B_D = \{f \in K(C),\ \forall \wp|\infty,\ w_\wp(f) \geq 0\}$$

donc $M(D) = M^*(D) \cap B_D$. (Remarque : $M^*(D)$ ne dépend que de la partie "finie" de D, alors que ν_D, δ_D et B_D ne dépendent que de sa partie "infinie").

Une base $(f_1, \ldots, f_n)$ de $M^*(D)$ sur $K[X]$ est dite minimale (pour δ_D) si, pour tout i,

$$\nu_D(f_i) = \max \{\nu_D(f),\ f \in M^*(D) - \bigoplus_{j<i} K[X] f_j\}.$$

THEOREME 3. - Soit $(f_1, \ldots, f_n)$ une base minimale (pour δ_D) de $M^*(D)$ sur $K[X]$, et soit i_0 le plus grand indice tel que $\nu_D(f_{i_0}) \geq 0$. Alors $\{X^k f_i,\ 1 \leq i \leq i_0,\ 0 \leq k \leq \nu_D(f_i)\}$ forme une base de $M(D)$ sur K.

Il nous reste donc à déterminer une base minimale à partir d'une base quelconque de $M^*(D)$ sur $K[X]$.

THEOREME 4. - Soit $(f_1,\dots,f_n)$ une base de $M^*(D)$ sur $K[X]$. Alors $\sum_{i=1}^{n} \nu_D(f_i) \leq -\deg(D) - \frac{1}{2}\sum_{\wp}(e_\wp-1)$, avec égalité si et seulement si $(f_1,\dots,f_n)$ est minimale pour δ_D .

Remarque : la quantité $\frac{1}{2}\sum_{\wp}(e_\wp-1)$ est liée au genre g de C par la formule d'Hurwitz $\frac{1}{2}\sum_{\wp}(e_\wp-1) = g-1+n$ [Fu] .

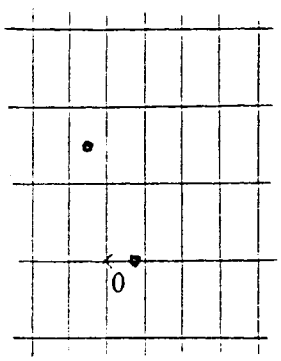
2ème PARTIE DE L'ALGORITHME.

Détermination d'une base minimale de $M^*(D)$ sur $K[X]$. Au départ, $(f_1,\dots,f_n)$ est la base de $M^*(D)$ sur $K[X]$ donnée par la 1ère partie de l'algorithme.

Tant que $\sum_{i=1}^{n} \nu_D(f_i) < -\deg(D) - \frac{1}{2}\sum_{\wp}(e_\wp-1)$, on effectue un "pas de réduction à l'∞ " ; c'est un processus légèrement différent d'un "pas de réduction en α " mais utilisant les mêmes ingrédients (voir [Bl] ou [Co] lorsque $n_\wp = 0$ et $e_\wp = 1$ pour tout $\wp|\infty$; voir [Du] pour le cas général) . A chacun de ces pas de réduction à l'∞ , l'entier $\sum_{i=1}^{n} \nu_D(f_i)$ augmente d'au moins 1 .

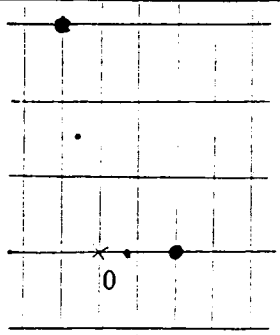
Donc l'algorithme se termine après un nombre fini de pas de réduction à l'∞ , avec une base minimale de $M^*(D)$ sur $K[X]$.

L'ensemble de l'algorithme peut se représenter (très schématiquement) ainsi :

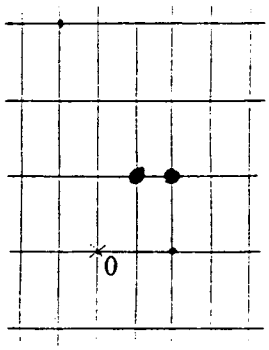
au départ : 

base de $K(C)$ sur $K(X)$

1ère partie de l'algorithme :



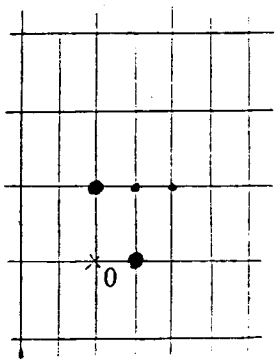
base de $K(C)$ sur $K(X)$ contenue dans $M^*(D)$.



pas de réduction aux places "finies"

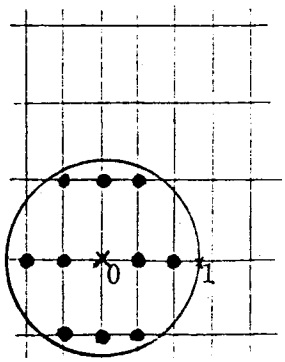
base de $M^*(D)$ sur $K[X]$.

2ème partie de l'algorithme :



pas de réduction aux places "infinies"

base minimale (pour δ_D) de $M^*(D)$ sur $K[X]$.



base de $M(D)$ sur K.

AUTRES ALGORITHMES

D'autres algorithmes permettent de calculer une base de $L(D)$ sur K .

• L'algorithme de Brill-Nœther [Fu] , de nature plus "géométrique", utilise la notion de "courbe adjointe" ; il est en général plus agréable à utiliser pour traiter des exemples de petite dimension à la main, mais sa complexité semble croître très vite avec le degré du polynôme F .

• L'algorithme de Trager [Tr] suit le même schéma que l'algorithme présenté ci-dessus : détermination d'une base, puis d'une base minimale, de $M^*(D)$. Mais il ne fait ces calculs que lorsque D est le diviseur nul (le cas d'un diviseur quelconque s'en déduisant assez facilement). Comme $M^*(0)$ est l'anneau des entiers de $K(C)$, une adaptation d'un algorithme dû à Zassenhaus pour calculer des anneaux d'entiers de corps de nombres donne le résultat. L'avantage de cet algorithme est de ne faire intervenir, dans les calculs intermédiaires, aucun nombre algébrique qui ne soit nécessaire à l'énoncé du résultat (en particulier, le calcul des développements de Puiseux est inutile).

IMPLANTATION

En dehors de l'implantation partielle de Davenport sur REDUCE déjà citée [Da] , une implantation plus complète a été réalisée par Maurer [Ma] en PASCAL et Assembleur.

Il ne travaille évidemment pas sur un corps algébriquement clos, mais seulement sur des extensions finies du corps K_0 . En utilisant les conjugaisons sur le corps K_0 il parvient à remplacer les matrices carrées d'ordre n à coefficients dans K des divers pas de réduction

par des matrices à n lignes et n' colonnes (avec $n \leq n' \leq n^2$) à coefficients dans K_0 .

Sa conclusion est que la plus grande partie du temps de calcul sert aux divers calculs d'éléments primitifs et de factorisation utilisés pour manipuler les nombres algébriques.

En considérant des développements de Puiseux modifiés, c'est-à-dire des développements en une uniformisante t en $\wp$ vérifiant $t^{e_\wp} = \lambda(X-\alpha)$ pour un $\lambda \in K$ bien choisi (et pas forcément $\lambda = 1$), il est possible de travailler avec des matrices carrées d'ordre n à coefficients dans K_0 [Du 2] .

Et surtout, en utilisant la méthode de [D 5] , les calculs avec des nombres algébriques sur K_0 ne font intervenir que de l'algèbre linéaire et des calculs de pgcd, au lieu des factorisations et calculs d'éléments primitifs habituellement utilisés.

REFERENCES

[Ar] J.V. ARMITAGE, Algebraic functions and an analogue of the geometry of numbers : the Riemann-Roch theorem. Arch. Math. (Basel), vol. 18 (1967), pp. 383-393.

[Bl] G. A. BLISS, Algebraic functions. Ann. Math. Soc. Colloquium Publ. Vol. 16 (1933).

[Co] J. COATES, Construction of rational functions on a curve. Proc. Camb. Phil. Soc. 68 (1970), pp. 105-123.

[Da] J.H.DAVENPORT, On the integration of algebraic functions. Lecture notes in computer science n°102 (1981), Springer-Verlag.

[Du] D. DUVAL, Une méthode géométrique de factorisation des polynômes en deux indéterminées. Calsyf n°3 (1983).

[Du 2] D. DUVAL, en préparation.

[D-W] R. DEDEKING, H. WEBER, Theorie der algebraischen Funktionen einer Veränderlichen.
J. für reine und angewandte Math. Bd. 92 (1882), pp. 181-290.

[D5] J. DELLA DORA, C. DICRESCENZO, D. DUVAL, About a new method for computing in algebraic number fields. Proceedings of EUROCAL'85, Lecture notes in Computer Sc., Springer Verlag (1985), à paraître.

[Fu] W. FULTON, Algebraic Curves.
Benjamin Inc. (1969).

[Ma] D. MAURER, Der Algorithmus von Coates.
Diplomarbeit, Universität des Saarlandes (1982).

[Ri] R.H. RISCH, The solution of the problem of integration in finite terms.
Bull. A.M.S. n°76 (1970), pp. 605-608.

[Se] J.-P. SERRE, Corps locaux.
Hermann (1968).

[Tr] B. TRAGER, Thesis MIT (1985).

Colloque d'Algèbre de Rennes
juin 1985