MÉMOIRES DE LA S. M. F.

MAURICE MIGNOTTE

Calculs sur des suites récurrentes linéaires

Mémoires de la S. M. F., tome 49-50 (1977), p. 137-140

<http://www.numdam.org/item?id=MSMF_1977__49-50__137_0>

Calculateurs en Math. (1975 - LIMOGES)
Bull. Soc. math. France
Mémoire 49-50, 1977, p. 137-140

CALCULS SUR DES SUITES RECURRENTES LINEAIRES

par Maurice MIGNOTTE

Nous étudierons le problème de la détermination des zéros d'une suite récurrente linéaire.

1. Notations et préliminaires -

Une suite $u = (u_n)_{n\geq o}$ de nombres est dite récurrente s'il existe un entier h, et des nombres $q_1, \ldots, q_h$ $(q_h \neq o)$ tels que :

$$(1) \qquad u_{n+h} = q_1 u_{n+h-1} + \ldots + q_h u_n, \quad \text{si } n \geq 0,$$

une telle suite est dite d'ordre au plus h.

On considérera le cas où les u_n et q_j sont entiers. Si on pose

$$U_n = \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+h-1} \end{pmatrix} \text{ pour } n \geq 0 \text{ et } A = \begin{pmatrix} 0 & 1 & 0 & \ldots & \\ 0 & 0 & 1 & 0 & \ldots \\ \ldots & & & & \\ 0 & \ldots\ldots\ldots & & 0 & 1 \\ q_h & \ldots\ldots\ldots & & & q_1 \end{pmatrix}$$

la relation (1) s'écrit sous forme matricielle

$$(1') \qquad U_{n+1} = A\, U_n = A^{n+1}\, U_0 \qquad \text{pour } n \geq 0.$$

On associe à u le polynôme

$$P(X) = X^h - q_1 X^{h-1} - \ldots - q_h = (X-\alpha_1)^{k_1} \ldots (X-\alpha_r)^{k_r}$$

où les α_i sont distincts et vérifient $|\alpha_1| \geq |\alpha_2| \geq \ldots \geq |\alpha_r|$. En utilisant la décomposition de Jordan de A, on voit qu'il existe des polynômes $R_1, \ldots, R_r$, tels que l'on ait :

$$(2) \qquad u_n = R_1(n)\,\alpha_1^n + \ldots + R_r(n)\,\alpha_r^n, \quad \text{si } n \geq 0$$

le degré de R_i étant majoré par $k_i - 1$, pour $i = 1, \ldots, r$.

Inversement, une suite u, définie par (2), vérifie la relation (1). Si u vérifie (1), et si on considère la suite $v = (v_n)_{n\geq 0}$ définie par

$$v_n = u_{nT+m}, \quad n \geq 0 \ (T > 0,\ m \geq 0, \text{ entiers fixés}),$$

la relation (2) montre que l'on a :

$$(3) \qquad v_n = \sum_{j=1}^{r} \alpha_j^m\, R_j(n\,T + m)\, (\alpha_j^T)^n$$

on en déduit que v vérifie une relation de récurrence d'ordre $\leq h$ et que cette relation ne dépend que de T.

2. Le théorème de Skolem-Mahler -

Il s'agit du résultat suivant.

THEOREME 1.- Soit (u) une suite récurrente linéaire. Soit E l'ensemble des indices n tels que u_n soit nul. Alors E est égal à une union finie de progressions arithmétiques (dont certaines peuvent être de raison nulle !).

Démonstration - Voir [5], par exemple.

COROLLAIRE.- Si u admet une infinité de zéros, alors, pour tout α_i, il existe α_j, $j \neq i$, tel que α_i/α_j soit une racine de l'unité.

Démonstration - Si $v_n = u_{nT+m} = 0$ pour tout n, la relation (3) permet facilement d'obtenir le résultat annoncé.

Le théorème 1 a pu être précisé, nous nous contenterons d'énoncer le résultat suivant (voir [4] pour plus de détails et d'autres résultats).

THEOREME 2.- Il existe un algorithme permettant de décider si une suite récurrente linéaire à termes entiers possède une infinité de termes nuls.

3. Une application d'un résultat de Baker -

En utilisant la minoration de formes linéaires en logarithmes de nombres algébriques démontrée en [2], on démontre le résultat suivant.

THEOREME 3.- Soit u une suite d'entiers définie par (1) et (2). Supposons que P admette au plus trois racines de module maximal et que ces racines $\alpha_1, \ldots, \alpha_\ell$ sont simples. Alors, il existe des constantes n_o et c, effectivement calculables telles que, pour $n \geq n_o$ on ait :

$$|u_n| \geq |\alpha_1|^n \, n^{-c} \quad \text{si} \quad R_1 \alpha_1^n + \ldots + R_\ell \alpha_\ell \neq 0.$$

(Les polynômes $R_1, \ldots, R_\ell$ sont constants).

Démonstration - Voir [6] ou [7].

4. Etude d'un exemple -

Considérons la suite définie par :

$$u_o = u_1 = 0, \quad u_2 = 1, \quad u_{n+3} = 2\,u_{n+2} - 4\,u_{n+1} + 4\,u_n, \quad \text{si } n \geq 0.$$

On constate que l'on a :

$$u_o = u_1 = u_4 = u_6 = u_{13} = u_{52} = 0.$$

Cet exemple, dû à Jean Berstel, contredit une conjecture affirmant qu'une suite récurrente cubique à valeurs entières, qui n'a qu'un nombre fini de zéros, en a au plus cinq (voir [5]). La détermination de tous les zéros de (u_n) était donc intéressante. Nous allons indiquer plusieurs méthodes permettant de prouver que les zéros indiqués plus haut sont les seuls.

a) Méthode p-adique -

Elle utilise le théorème suivant, dû à Strassman.

THEOREME 4.- Soit $f(x) = \sum_0^\infty a_k x^k$, une série à coefficients dans un corps $\mathfrak{p}$-adique $K_{\mathfrak{p}}$, non identiquement nulle, convergente sur $O_{\mathfrak{p}}$, anneau des entiers de K. Alors, le nombre de zéros de f dans $O_{\mathfrak{p}}$ est majoré par :

$$N = \max \{k;\ v_{\mathfrak{p}}(a_k) \text{ est minimal}\},$$

où $v_{\mathfrak{p}}$ désigne la valuation $\mathfrak{p}$-adique de K.

On considère ici un corps $\mathfrak{p}$-adique de décomposition de P considéré comme polynôme à coefficients dans $\mathbb{Q}_p$ pour $p = 53$. Voir [6] pour plus de détails.

b) Calculs modulo m -

Grâce à un raffinement quantitatif du théorème qui figure dans l'article de Baker [1], on obtient :

$$u_n \neq 0 \quad \text{si} \quad n > 10^{190}$$

Ainsi, un nombre fini de calculs (!) permet de déterminer tous les zéros de u_n.

En réduisant u_n modulo m, il est facile de montrer que la suite des résidus est ultimement périodique (il n'y a qu'un nombre fini de triplets distincts modulo m). De plus, si m est impair, la suite est purement périodique (modulo m, u_n est déterminé par u_{n+1}, u_{n+2}, u_{n+3}). Soit Z_m l'ensemble des zéros modulo m. Si $u_n = 0$, on a $n \in \cap Z_m$, et réciproquement. En prenant des valeurs de m convenablement choisies, on arrive, de proche en proche, à déterminer des nombres K de plus en plus grands tels que :

$$u_n = 0 \Rightarrow n \in Z \bmod K \quad (\text{où } Z = \{0, 1, 4, 6, 13, 52\}).$$

Un exemple montrera la marche à suivre.

On a :

- modulo 18481 ; période $2^4 . 3 . 5 . 7 . 11$, zéros : Z
- modulo 8737 ; période $2^5 . 3 . 7 . 13$, zéros : Z
- modulo 21377 ; période $2^7 . 167$, zéros : Z + (6546)
- modulo 19457 ; période $2^{10} . 19$, zéros : Z + (11338).

Des deux premiers résultats, et du fait que les éléments de Z sont distincts modulo le p. g. c. d. des périodes (égal à $2^4 . 3 . 7$), on voit que les zéros de (u_n) appartiennent à l'ensemble $Z + (2^5 . 3 . 5 . 7 . 11 . 13) . \mathbb{N}$. Puis la réduction modulo 21377 fournit, en plus de Z, le nombre 6546; mais ce nombre n'appartient pas à l'ensemble $Z + 2^5 . \mathbb{N}$ (et il en est de même pour les nombres de la progression $6546 + 2^7 \cdot 167 . \mathbb{N}$), donc les zéros de (u_n) appartiennent à l'ensemble $Z + (2^7 . 3 . 5 . 7 . 11 . 13 . 167) . \mathbb{N}$. Finalement l'étude de ces quatre cas montre que les zéros de u_n sont situés dans les progressions $Z + (2^{10} . 3 . 5 . 7 . 11 . 13 . 19 . 167) . \mathbb{N}$. En particulier, les seuls indices $n < 2^{10} . 3 . 5 . 7 . 11 . 13 . 19 . 167$ sont les nombres de Z.

Les calculs faits sur machine ont permis de dépasser la borne 10^{190}.

c) Approximations diophantiennes -

Une autre méthode, inspirée du travail de Baker et Davenport [2], n'utilise que le calcul (avec une très grande précision) des logarithmes des quantités a, ω, b, ω', définies par la condition

$$u_n = a \omega^n + \bar{a} \bar{\omega}^n + b \omega'^n \quad \text{si} \quad n \geq 0.$$

La démonstration du théorème 3 montre en effet que la condition $u_n = 0$ implique, pour n assez grand, une inégalité du type

(4) $$|n \alpha - m + \beta| < e^{-\varepsilon n}, \text{ pour un certain } \varepsilon > 0, \quad \alpha, \beta, \text{ réels.}$$

C'est un problème non homogène, mais un argument, dû à Davenport, permet de le ramener à l'étude d'un problème d'approximation diophantienne homogène :

LEMME.- Soit $K > 6$. Pour tout entier positif M, soient p et q des entiers vérifiant :

$$1 \leq q \leq K M, \quad |\alpha p - q| < 2(K M)^{-1}$$

Alors, si

$$\|q \beta\| \geq 3 K^{-1} \quad (\text{où } \| \ \| = \text{distance à l'entier le plus proche}),$$

l'inégalité (4) n'a pas de solution dans l'intervalle

$$(5) \qquad \frac{\text{Log } K^2 M}{\varepsilon} < n < M$$

Démonstration - Posons $q \alpha = p + \phi$, avec $|\phi| < 2(K M)^{-1}$. En multipliant (4) par q, il vient

$$(6) \qquad |n(p + \phi) - m q + q \beta| < q e^{-\varepsilon n}$$

Supposons que n vérifie (4). Alors,

$$|\phi| n < 2 M(K M)^{-1} = 2 K^{-1} \ ; \ q e^{-\varepsilon n} \leq K M e^{-n} < K^{-1}$$

Puis (6) implique $\|q \beta\| < 3 K^{-1}$. Contradiction.

Il faudrait ici calculer α et β avec une précision de l'ordre de 10^{-250}. La meilleure méthode consiste à utiliser la méthode de Newton en inversant la fonction exponentielle (et non le développement en série du logarithme !).

Remarque - L'existence de p et q dans l'énoncé du lemme 3 résulte du lemme d'approximation de Dirichlet.

REFERENCES

(1) A. BAKER.- Linear forms in the logarithms of algebraic numbers.- IV. Mathematika 15, (1968) p. 204-216.

(2) A. BAKER.- A sharpening of the bounds for linear forms in logarithms.- Acta Arith. 21, (1974) p. 117-129.

(3) A. BAKER et H. DAVENPORT.- The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. Quart. J. Math. Oxford 2.- (1969) p. 129-137.

(4) J. BERSTEL et M. MIGNOTTE.- Deux propriétés décidables des suites récurrentes linéaires.- Bull. Soc. Math. France. 104 (1976) p. 175-184.

(5) D.J. LEWIS.- Diophantine equations : p-adic methods.- Studies in Number Theory.- p. 23-75.- Englewood Cliffs, Prentice Hall. (1969).

(6) M. MIGNOTTE.- Suites récurrentes linéaires.- Séminaire DELANGE-PISOT-POITOU.- (1973-74) n° G 14, 9 p.

(7) M. MIGNOTTE.- A note on linear recursive sequences.- J. Australian Math. Soc. 20, sec. A, part. 2, (1974), p. 242-244.

Maurice MIGNOTTE
Université Louis Pasteur
Centre de Calcul
STRASBOURG