ANNE BERTRAND

Nombres de Perron et problèmes de rationalité

Astérisque, tome 198-199-200 (1991), p. 67-76
<http://www.numdam.org/item?id=AST_1991__198-199-200__67_0>

NOMBRES DE PERRON ET PROBLEMES DE RATIONALITE

par

Anne BERTRAND

1. Le Théorème de Perron.

On dit qu'une matrice carrée B est primitive s'il existe un entier k tel que B^k ait tous ses coefficients strictement positifs. Le Théorème de PERRON, qui date du siècle dernier, affirme que :

THÉORÈME DE PERRON : *Toute matrice primitive B à coefficients positifs ou nuls admet une valeur propre λ strictement positive telle que pour toute autre valeur propre μ de B :*

$$|\mu| < \lambda.$$

Le nombre λ est dit valeur propre strictement dominante de B.

Ceci est vrai en particulier pour les matrices à coefficients strictement positifs, qui sont forcément primitives.

On dit qu'une matrice carrée d'ordre $B = (b_{ij})$ est réductible s'il existe une partition de $\{1, \ldots, n\}$ en deux ensembles non vides I et J tels que

$$\forall (i,j) \in I \times J \quad b_{ij} = 0.$$

Si cela n'est pas vrai B est dite irréductible. FROBENIUS a complété les résultats de PERRON en établissant que :

THÉORÈME DE FROBENIUS : *Soit B une matrice carrée irréductible à coefficients positifs ou nuls ; alors B admet une valeur propre réelle positive λ telle que toute autre valeur propre μ vérifie*

$$|\mu| \leq \lambda$$

et si $|\mu| = \lambda$, alors il existe une racine de l'unité $e^{2i\pi/h}$ telle que $\mu = e^{2i\pi/h}\lambda$; le spectre de B est invariant par rotation d'angle $\dfrac{2\pi}{h}$.

S.M.F.
Astérisque 198-199-200 (1991)

Exemples : la matrice $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ est primitive : son carré est $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ et ses valeurs propres sont $\dfrac{1+\sqrt{5}}{2}$ $(\sim 1,6)$ et $\dfrac{1-\sqrt{5}}{2}$ $(\sim -0,6)$.

La matrice $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ est irréductible, la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ ne l'est pas ($b_{ij} = 0$ si $(i,j) \in \{1,2\} \times \{3\}$).

Dans le cas où B est à coefficients dans $\mathbb{N}$ (c'est à ce cas précis que nous nous intéresserons), les valeurs propres de B sont des entiers algébriques racines du polynôme caractéristique de B ; si λ est valeur propre strictement dominante d'une matrice primitive B sur $\mathbb{N}$, les conjugués de λ sont aussi valeurs propres de B et donc tous les conjugués de λ distincts de λ sont en module strictement inférieur à λ. Douglas LIND a baptisé *Nombres de Perron* les entiers algébriques qui sont strictement supérieurs aux modules de leurs conjugués. On peut se poser la question suivante : quels sont exactement les nombres entiers algébriques qui sont valeur propre strictement dominante d'au moins une matrice primitive à coefficients dans $\mathbb{N}$? Et bien, ce sont exactement les nombres de PERRON comme le montre le théorème suivant :

THÉORÈME (LIND - HANDLEMAN, 1980-1984) : *Soit λ un nombre de Perron ; alors il existe une matrice primitive B à coefficients dans $\mathbb{N}$ dont λ est la valeur propre strictement dominante.*

Exemple : $\dfrac{1+\sqrt{5}}{2}$ est un Perron, mais par $\sqrt{2}$ dont le conjugué est $-\sqrt{2}$. Les démonstrations de LIND et HANDLEMAN sont de nature géométrique ; nous voulons présenter ici la trame d'une preuve algébrique basée sur des problèmes de rationalité (de langages et de séries).

2. Langages.

Soit A un alphabet fini, c'est à dire un ensemble fini de symboles ; soit A^* l'ensemble des mots sur A, c'est à dire des suites finies sur A (y compris le mot vide) ; on munit A^* du produit de concaténation (le concatené de $u_1 \cdots u_k$ et $v_1 \cdots v_h$ est $u_1 \cdots u_k \; v_1 \cdots v_h$) ; on appelle langage une partie de A^*.

Etant donné un langage L sur un alphabet A, on définit une relation d'équivalence sur les mots de A^* : $u \sim v$ si et seulement si

$$\forall a, b \in A^* \quad aub \in L \iff avb \in L$$

(u et v ont les mêmes contextes dans L).

Le langage L est dit rationnel si le nombre de classes de A^* modulo cette relation d'équivalence est fini. Par exemple, si $A = \{0,1\}$, si L_1 est l'ensemble des mots sur A dans lesquels n'apparaissent jamais deux 1 consécutifs ($L_1 = \{0,1,00,01,10,000,001,010,100,101,\ldots\}$) alors L_1 est rationnel car les classes modulo L_1 ont pour système de représentants dans A^* :

$$\begin{array}{ll}
0 & (a0b \in L_1 \text{ si } a,b \in L_1) \\
1 & (a1b \in L_1 \text{ si } a,b \in L_1, a \text{ finit et } b \text{ débute par } 0) \\
01 & (a01b \in L_1 \text{ si } a,b \in L_1, b \text{ commence par } 0) \\
10 & (a10b \in L_1 \text{ si } a,b \in L_1 \text{ et } a \text{ finit par } 0) \\
11 & (a11b \text{ n'est jamais dans } L_1).
\end{array}$$

L'ensemble des langages rationnels est aussi la plus petite classe de langages contenant les langages finis et stables pour la réunion, le "produit" $L_1L_2 = \{uv; u \in L_1, v \in L_2\}$ et par l'opération "étoile" : $L^* = L \cup L^2 \cup L^3 \cup \cdots$ (ceci constitue le Théorème de Kleene).

Exemple : si $C = \{0,10\}$, alors C^* est l'ensemble des mots de L_1 finissant par 0 ; on remarque que

$$L_1 = C^*U(C^*1).$$

3. Matrices sur $\mathbb{N}$ et systèmes dynamiques.

Un langage L est dit factoriel si, dès que uvw est dans L, v y est aussi ; il est dit prolongeable si pour tout u appartenant à L on peut trouver des mots de A^*, a et b, tels que aub soit dans L ; il est dit transitif si, dès que u et v sont dans L, on peut trouver un mot w de A^* tel que uwv soit dans L.

Le langage A^*, le langage L_1 du §.2 possèdent ces trois propriétés.

Systèmes dynamiques symboliques. Considérons l'ensemble $A^{\mathbb{N}} = \{a_1a_2a_3\cdots;\ a_i \in A\}$ des suites sur A, muni de la transformation T dite shift : $T(a_1a_2a_3\cdots) = (a_2a_3a_4\cdots)$. Etant donné un langage L factoriel et prolongeable on appelle système dynamique symbolique S associé à L l'ensemble $S = \{a_1a_2a_3\cdots; \forall n,p,\ a_{n+1}\cdots a_{n+p} \in L\}$ dont on vérifie qu'il est invariant par T. Lorsque L est rationnel on dit que L est un système sofique ; le système est dit transitif si le langage L est transitif et il est dit mélangeant s'il existe un entier k tel que pour tout $h \geq k$ et pour tout couple u,v de mots de L (apparaissant donc dans les suites de S) on peut trouver un mot w de longueur h (la longueur d'un mot est le nombre de lettres qui le composent) tel que uwv soit encore dans L.

Si, par exemple, $L = L_1$, S_1 est l'ensemble des suites de 0 et 1 dans lesquelles on n'observe jamais deux 1 consécutifs.

Les systèmes de MARKOV sont un cas particulier des systèmes sofiques : soit P un ensemble fini de mots, et L le langage formé par les mots ne contenant aucun mot de P ; il est facile de voir qu'il existe un entier k et un ensemble fini M de mots de longueur $k+1$ tel que le système dynamique associé à L soit $S = \{a_1 a_2 \cdots ; \forall n,\ a_n \cdots a_{n+k} \in M\}$: la connaissance des k lettres $a_n \cdots a_{n+k-1}$ détermine les valeurs possibles de a_{n+k} ; de tels langages sont bien sûr rationnels. Par exemple le système S_1 est un système de MARKOV mélangeant d'ordre 1 pour lequel $M = \{00, 01, 10\}$. On peut associer à ce système dynamique la matrice suivante :

$$\begin{pmatrix} b_{00} & b_{10} \\ b_{01} & b_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} : \begin{pmatrix} 1 \text{ car } 00 \in M & 1 \text{ car } 10 \in M \\ 1 \text{ car } 01 \in M & 0 \text{ car } 11 \in M \end{pmatrix}$$

Autre exemple : considérons le système d'ordre 2 dans lequel 111 n'apparaît jamais ; on peut lui associer la matrice d'ordre 4 sur $\mathbb{N}$:

$$\begin{pmatrix} b_{00,00} & b_{00,01} & b_{00,10} & b_{00,11} \\ b_{01,10} & b_{01,01} & b_{01,10} & b_{01,11} \\ b_{10,00} & b_{10,01} & b_{10,10} & b_{10,11} \\ b_{11,00} & b_{11,01} & b_{11,10} & b_{11,11} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

dans laquelle $b_{c_1c_2,d_1d_2} = 1$ s'il existe un mot $u_1u_2u_3$ de $L \cap A^3$ tel que $u_1u_2 = c_1c_2$ et $u_2u_3 = d_1d_2$; $b_{c_1c_2,d_1d_2} = 0$ sinon. De même, à tout système de MARKOV d'ordre k sur un alphabet de p lettres on associe la matrice carrée d'ordre p^k $b = (b_{c_1\cdots c_k,d_1\cdots d_k})$ où $b_{c_1\cdots c_k,d_1\cdots d_k}$ vaut 1 si $d_1 \cdots d_{k-1} = c_2 \cdots c_k$ et $d_1 \cdots d_k \in M$ et 0 sinon. Lorsque le système est mélangeant la matrice B est primitive ; d'une façon générale et par un procédé plus sophistiqué (sic), *à tout système sofique mélangeant on peut associer une matrice primitive B sur $\mathbb{N}$.*

Que représente pour le système la valeur propre λ strictement dominante de B ? Remarquons que le nombre de mots de longueur $k+1$ apparaissant dans une chaîne de MARKOV est égal à la somme des coefficients de la matrice B ; de même, le nombre de mots de longueur $k+n$ apparaissant dans une chaîne de MARKOV est égal à la somme des coefficients de la matrice B^n ; par exemple, pour le système L_1 avec la matrice $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $B^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, $B^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$ ... ; la somme des coefficients de B vaut 3, celle de B^2, 5, celle de B^3, 8 ; or il y a trois mots de longueur deux (00,01,10), cinq mots de longueur 3 (000,001,010,100,101) et huit mots de longueur 4 (0000,0001,0010,0100,0101,1000,1001,1010). Les 2-mots sont ainsi formés à partir des mots de longueur 1 :