

2.8.2 Algorithme de Berlekamp/Massey

On donne dans un corps $\mathcal{K}$ les $2n$ premiers éléments d'une suite récurrente linéaire $(a_k)_{k \in \mathbb{N}}$ pour laquelle on sait qu'il existe un polynôme générateur de degré n . Le problème est de calculer le polynôme générateur minimal g de la suite.

Une telle solution est donnée par l'algorithme de Berlekamp/Massey [27] qui donne en sortie le degré d ainsi que les coefficients d'un polynôme $f = c_d g$ associé au polynôme g . Ce polynôme g est alors obtenu en divisant par c_d .

L'algorithme de Berlekamp/Massey utilise les propriétés de la suite des triplets (R_i, U_i, V_i) formée des restes et des multiplicateurs de Bézout successifs dans l'algorithme d'Euclide étendu pour le couple de polynômes (R_{-1}, R_0) où $R_{-1} = X^{2n}$ et $R_0 = \sum_{i=0}^{2n-1} a_i X^i$.

Posant $V_{-1} = U_0 = 0$ et $U_{-1} = V_0 = 1$, ces triplets vérifient, pour tout $i \geq 0$, les relations :

$$\begin{aligned} R_{i-1} &= R_i Q_i + R_{i+1} && \text{où } d^\circ R_{i+1} < d^\circ R_i \\ U_{i+1} &= U_{i-1} - Q_i U_i, \\ V_{i+1} &= V_{i-1} - Q_i V_i, && \text{d'où :} \\ R_i &= U_i R_{-1} + V_i R_0, \\ \text{de plus : } U_i V_{i-1} - V_i U_{i-1} &= (-1)^i && \text{et } d^\circ R_i < 2n - d^\circ V_i. \end{aligned}$$

Les deux dernières relations se vérifient facilement par récurrence sur i .

On arrête le processus au premier reste, disons R_m , de degré plus bas que n , pour obtenir :

$$U_m X^{2n} + V_m R_0 = R_m \quad \text{avec } d^\circ R_m < n.$$

Posons $d = \sup(d^\circ V_m, 1 + d^\circ R_m)$ et $P = X^d V_m (1/X)$. Alors on peut montrer que P divisé par son coefficient dominant est le polynôme générateur minimal de la suite (a_k) (cf. [GG] et [27]). Par exemple dans le cas où $d^\circ V_m = n$ et $V_m(0) \neq 0$, en écrivant que les termes de degré compris entre n et $2n - 1$ du polynôme $V_m(X) R_0(X)$ sont nuls, on constate que $P(X)$ est bien un polynôme générateur de la suite (a_k) .

Ceci donne précisément l'algorithme 2.16 page suivante (dans lequel $\text{cd}(P)$ désigne le coefficient dominant de P).

Cet algorithme est dû à Berlekamp, mais sous une forme où la relation avec l'algorithme d'Euclide étendu était invisible. C'est Massey qui a fait le rapprochement. Pour plus de détails sur la relation entre cet algorithme et l'algorithme d'Euclide étendu, on pourra consulter [27].

Algorithme 2.16 *Algorithme de Berlekamp-Massey*

Entrée : Un entier $n \geq 1$. Une liste non nulle d'éléments du corps $\mathcal{K}$, $[a_0, a_1, \dots, a_{2n-1}]$: les $2n$ premiers termes d'une suite récurrente linéaire, sous l'hypothèse qu'elle admet un polynôme générateur de degré $\leq n$.

Sortie : Le polynôme générateur minimal P de la suite récurrente linéaire.

Début

Variables locales : $R, R_0, R_1, V, V_0, V_1, Q$: polynômes en X

initialisation

$R_0 := X^{2n}; R_1 := \sum_{i=0}^{2n-1} a_i X^i; V_0 := 0; V_1 := 1;$

boucle

tant que $n \leq \deg(R_1)$ **faire**

$(Q, R) :=$ quotient et reste de la division de R_0 par R_1 ;

$V := V_0 - Q * V_1$;

$V_0 := V_1; V_1 := V; R_0 := R_1; R_1 := R$;

fin tant que

sortie

$d := \sup(\deg(V_1), 1 + \deg(R_1)); P := X^d V_1(1/X);$

Retourner $P := P/\text{cd}(P)$.

Fin.

2.8.3 Méthode de Wiedemann

L'algorithme de Wiedemann [96] pour la résolution des systèmes linéaires sur un corps $\mathcal{K}$ est un algorithme probabiliste, avec divisions, qui est basé sur la théorie des suites récurrentes linéaires. Il est particulièrement efficace dans le cas des matrices creuses sur les corps finis.

Il utilise le fait que si le polynôme minimal P^A d'une matrice $A \in \mathcal{K}^{n \times n}$ est de degré n (donc égal, à un signe près, au polynôme caractéristique P_A de A), alors il existe toujours un vecteur $v \in \mathcal{K}^{n \times 1}$ pour lequel le polynôme générateur minimal de la suite récurrente linéaire $(A^k v)_{k \in \mathbb{N}}$ est égal à P^A . Il suffit en effet, comme nous l'avons vu dans la section 1.3 (corollaire 1.3.3), de prendre un vecteur de $\mathcal{K}^n$ en dehors d'une réunion finie de sous-espaces de $\mathcal{K}^n$.

L'algorithme de Wiedemann choisit au hasard une forme linéaire $\pi : \mathcal{K}^n \rightarrow \mathcal{K}$ et un vecteur $v \in \mathcal{K}^n$ puis il calcule les $2n$ premiers termes de la suite récurrente linéaire $(\pi(A^k v))_{k \in \mathbb{N}}$ dans $\mathcal{K}$. Enfin le polynôme générateur minimal de cette suite est obtenu par l'algorithme