Une variante de l'algorithme de Berlekamp-Massey

Nadia Ben Atti, Gema M. Diáz–Toca, Henri Lombardi

Résumé

Nous donnons une variante, légèrement plus simple, de l'algorithme de Berlekamp-Massey. L'explication de l'algorithme est également plus facile. En outre cela autorise une approche « dynamique » de cet algorithme utile dans certaines situations

Mots clés : Algorithme de Berlekamp-Massey. Suites récurrentes linéaires.

L'algorithme de Berlekamp-Massey usuel

L'algorithme de Berlekamp-Massey prend en entrée les $2n$ premiers termes d'une suite récurrente linéaire dans un corps $\mathbb{K}$ et donne en sortie le polynome générateur minimal de la suite. Inventé par Berlekamp [2], il a été « expliqué » par Massey [6] et Dornstetter [4] qui ont montré qu'on pouvait le voir comme une variante d'un algorithme d'Euclide étendu. Voici ce que cela donne.

Algorithme 1 ***Algorithme de Berlekamp-Massey usuel***

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

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

Début

Variables locales : $R, R_0, R_1, V, V_0, V_1, Q$: polynomes 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 de la boucle

$d := \sup(\deg(V_1), 1 + \deg(R_1))$; $P := X^d V_1(1/X)$; Retourner $P = P/\mathrm{cd}(P)$.

Fin.

Bien que très simple cet algorithme a toujours semblé un peu trop difficile à justifier. Une littérature considérable a été développée à son sujet. Citons par exemple [3, 4, 5, 7, 8, 9]. Nous proposons (encore une fois !) d'expliquer cet algorithme de manière vraiment simple et convaincante, mais pour cela nous avons besoin d'introduire une légère variation, très naturelle, dont, de manière étrange, nous n'avons pas trouvé trace dans la littérature.

La variante et sa justification

La variation que nous introduisons est basée sur l'idée suivante. Puisqu'à la fin de l'algorithme, le polynome V doit être renversé selon une prodédure difficile à expliquer (pourquoi doit-on prendre le polynome réciproque en degré $d = \sup(\deg(V_1), 1 + \deg(R_1))$?), le mieux

ne serait-il pas de traiter directement la suite récurrente linéaire « dans le bon sens » (elle a elle-même été renversée au départ lorsqu'on a affecté $R_1 := \sum_{i=0}^{2n-1} a_i X^i$) ?

Naturellement l'appréciation selon laquelle la suite récurrente linéaire a été renversée au départ lorsqu'on a écrit $R_1 := \sum_{i=0}^{2n-1} a_i X^i$ est assez subjective. Elle est en fait renforcée par la remarque suivante. Si le polynome générateur minimal est de degré d nettement plus petit que n les calculs dans l'algorithme ne devraient pas être sensiblement différents lorsqu'on travaille avec les $2d$ premiers termes de la suite ou lorsqu'on travaille avec les $2n$ premiers termes. Or le renversement effectué au début de l'algorithme change complètement le calcul qui est fait. Tandis qu'en l'absence de renversement, avec notre variante, le calcul sur la suite courte peut facilement être regardé comme le calcul sur la suite longue, tronqué de manière convenable.

Une autre confirmation est le caractère plus simple, et plus facile à justifier, de l'affectation finale.

Algorithme 2 ***Algorithme de Berlekamp-Massey, variante***

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

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

Début

Variables locales : $R, R_0, R_1, V, V_0, V_1, Q$: polynomes en X ; $m = 2n-1$: entier.

initialisation

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

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 de la boucle

Retourner $P := V_1/\mathrm{cd}(V_1)$.

Fin.

Nous allons maintenant prouver la correction de cet algorithme.

Si $\underline{a} = (a_n)_{n\in\mathbb{N}}$ est une suite arbitraire et si i, r, $p \in \mathbb{N}$ nous noterons $\mathrm{H}^{\underline{a}}_{i,r,p}$ la matrice de Hankel suivante, qui possède r lignes et p colonnes :

$$\mathrm{H}^{\underline{a}}_{i,r,p} = \begin{bmatrix} a_i & a_{i+1} & a_{i+2} & \ldots & a_{i+p-1} \\ a_{i+1} & a_{i+2} & & & a_{i+p} \\ a_{i+2} & & & & \\ \vdots & & & & \vdots \\ a_{i+r-1} & a_{i+r} & \ldots & \ldots & a_{i+r+p-2} \end{bmatrix}.$$

et nous noterons $\mathrm{P}^{\underline{a}}(X)$ le polynome générateur minimal de $\underline{a}$.

La proposition suivante est classique (voir par exemple [1]).

Proposition 1 *Si $\underline{a}$ est une suite récurrente linéaire qui admet un polynome générateur de degré $\leq n$, alors le degré $d \leq n$ de son polynome générateur minimal $\mathrm{P}^{\underline{a}}$ est égal au rang de*

la matrice de Hankel

$$\mathrm{H}^{\underline{a}}_{0,n,n} = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_1 & a_2 & & \iddots & a_n \\ a_2 & & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & & \vdots \\ a_{n-1} & a_n & \cdots & \cdots & a_{2n-2} \end{bmatrix}.$$

Les coefficients de $\mathrm{P}^{\underline{a}}(X) = X^d - \sum_{i=0}^{d-1} g_i X^i \in \mathbb{K}[X]$ *sont l'unique solution de l'équation*

$$\mathrm{H}^{\underline{a}}_{0,d,d}\, G = \mathrm{H}^{\underline{a}}_{d,d,1}$$

c'est-à-dire encore l'unique solution du système linéaire

$$\begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{d-1} \\ a_1 & a_2 & & \iddots & a_d \\ a_2 & & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & & \vdots \\ a_{d-1} & a_d & \cdots & \cdots & a_{2d-2} \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ \vdots \\ g_{d-1} \end{bmatrix} = \begin{bmatrix} a_d \\ a_{d+1} \\ a_{d+2} \\ \vdots \\ a_{2d-1} \end{bmatrix}. \tag{1}$$

On en déduit facilement la précision suivante.

Proposition 2 *En outre pour qu'un vecteur* $Y = (p_0, \ldots, p_n)$ *soit solution de l'équation*

$$\mathrm{H}^{\underline{a}}_{0,n,n+1}\, Y = 0$$

c'est-à-dire

$$\begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_1 & a_2 & & \iddots & a_n & a_{n+1} \\ a_2 & & \iddots & \iddots & \vdots & \vdots \\ \vdots & \iddots & \iddots & & \vdots & \vdots \\ a_{n-1} & a_n & \cdots & \cdots & a_{2n-2} & a_{2n-1} \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ \vdots \\ p_{n-1} \\ p_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \\ 0 \end{bmatrix} \tag{2}$$

il faut et il suffit que le polynome $P(X) = \sum_{i=0}^{n} p_i X^i \in \mathbb{K}[X]$ *soit multiple de* $\mathrm{P}^{\underline{a}}(X)$.

Preuve.
Puisque la matrice est de rang d son noyau est de rang $n+1-d$. Puisque la suite est une suite récurrente linéaire ayant $\mathrm{P}^{\underline{a}}$ pour polynome générateur, les polynomes $\mathrm{P}^{\underline{a}}$, $X\mathrm{P}^{\underline{a}}$, $\ldots$,$X^{n-d}\mathrm{P}^{\underline{a}}$ correspondent à des vecteurs du noyau linéairement indépendants. Donc tout élément du noyau est une combinaison linéaire de ces vecteurs colonnes. □

Par ailleurs, nous faisons la constatation suivante.

Fait 3 *En posant* $m := 2n-1$ *et* $S := \sum_{i=0}^{m} a_{m-i} X^i$, *l'équation (2) est équivalente à l'affirmation suivante. Le polynome* P *est de degré* $\leq n$ *et on a :*

$$\exists R \in \mathbb{K}[X] \text{ tel que} \quad \deg(R) < n \quad \text{et} \quad P(X)S(X) \equiv R(X) \mod X^{2n}.$$

Autrement dit donner une solution de (2) revient à trouver P, R, U *tels que :*

$$\deg(R) < n,\ \deg(P) \leq n \quad \text{et} \quad P(X)S(X) + U(X)X^{2n} = R(X) \tag{3}$$

Le problème de trouver le polynome générateur minimal de $\underline{a}$ est donc ramené au problème de réaliser (3) avec le degré de P minimum.

Nous avons par ailleurs le fait suivant « bien connu » concernant l'algorithme d'Euclide étendu.

Fait 4 *Soient R_0 et R_1 de degrés p et $q \leq p$, et un entier $n < q$. Supposons que le degré du pgcd de R_0 et R_1 est $< n$. Notons $R_0, R_1, \ldots, R_s$ la suite des restes dans l'algorithme d'Euclide.*

1. *L'algorithme d'Euclide étendu démarrant avec R_0 et R_1 réalise des équations (du même type que (3))*
$$V_k(X)R_1(X) + U_k(X)R_0 = R_k(X)$$
Lorsque le premier reste R_k de degré $< n$ est atteint, on a $\deg(V_k) \leq p - n$ et $\deg(U_k) \leq q - n$.
2. *Il n'est pas possible d'obtenir une équation du même type*
$$V(X)R_1(X) + U(X)R_0 = R(X)$$
avec $\deg(R) < \deg(R_{k-1})$ et $\deg(V) < \deg(V_k)$.

Preuve.
Pour ℓ fixé on considère l'espace vectoriel E_ℓ formé par les polynomes $V(X)R_1(X) + U(X)R_0$ avec $\deg(U) \leq \ell$ et $\deg(V) \leq \ell + p - q$. On a $E_{\ell+1} = E_\ell + XE_\ell$, avec $1 + \dim(E_\ell) \leq \dim(E_{\ell+1}) \leq 2 + \dim(E_\ell)$. Disons que « le degré k est présent dans E_ℓ » s'il y a dans E_ℓ un polynome de degré k. Notons Δ_ℓ l'ensemble des degrés présents dans E_ℓ. Le cardinal de Δ_ℓ est égal à la dimension de E_ℓ. On a aussi $\Delta_\ell \cup (1 + \Delta_\ell) \subseteq \Delta_{\ell+1}$, avec égalité si le cardinal augmente de 2 entre Δ_ℓ et $\Delta_\ell \cup (1 + \Delta_\ell)$. Comme $\#(\Delta_{\ell+1}) \leq 2 + \#(\Delta_\ell)$, l'ensemble Δ_ℓ rangé en ordre croissant ne peut pas contenir plus qu'un trou.
Prenons un exemple. Supposons que $p = 12$, $q = 10$ et que les degrés dans la suite des restes soient 7, 6, 2, 1 (avec le pgcd de degré 1). Alors les relations précédemment établies entre $\Delta_{\ell+1}$ et Δ_ℓ impliquent que les Δ_ℓ successifs sont les suivants (on a rendu le trou éventuel visible par un blanc) : Notons δ_k le plus petit élément de Δ_k. On voit alors que tout δ_k est un degré dans

Tab. 1: Degrés présents dans les E_ℓ successifs

Δ_0	=	7, 10, 11, 12,
Δ_1	=	7, 8, 10, 11, 12, 13,
Δ_2	=	7, 8, 9, 10, 11, 12, 13, 14,
Δ_3	=	6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
Δ_4	=	2, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16,
Δ_5	=	2, 3, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17,
Δ_6	=	2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18,
Δ_7	=	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19,
Δ_8	=	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
Δ_9	=	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21

etc...

la suite des restes. En outre si le degré du pgcd est $< q - k$, on a toujours $\delta_k < q - k$. Enfin si le degré ℓ est atteint la première fois avec δ_k, on a $k \leq q - \ell$, et aucun degré $< \delta_{k-1}$ n'est atteint par un E_h où $h < k$. Ceci prouve les affirmations 1 et 2. □

En appliquant le fait 4 avec $R_0 = X^{2n}$, $m = 2n - 1$, $R_1 = S = \sum_{i=0}^{m} a_{m-i}X^i$ et $q = \deg(R_1)$ on obtient donc :

– l'algorithme d'Euclide étendu démarrant avec $R_0 = X^{2n}$ et $R_1 = S$ réalise une équation telle que (3) avec $R = R_k$ lorsque le premier reste R_k de degré $< n$ est atteint,

– quand une équation telle que (3) est réalisée par l'algorithme d'Euclide étendu, il n'est pas possible d'obtenir une équation du même type $P'(X)S(X)+U'(X)X^{2n} = R'(X)$ avec $\deg(R') < \deg(R_{k-1})$ et $\deg(P') < \deg(P)$.

Ceci prouve que l'algorithme 2 est correct.

Références

[1] J. Abdeljaoued, H. Lombardi, *Méthodes Matricielles. Introduction à la Complexité Algébrique*. Springer, collection "Mathématiques et Applications" de la SMAI. (2003)

[2] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, ch. 7 (1968).

[3] U. Cheng, *On the continued fraction and Berlekamp's algorithm*, IEEE Trans. Inform. Theory, vol. IT-30, 541–44 (1984).

[4] J.L. Dornstetter, *On the equivalence Between Berlekamp's and Euclid's Algorithm*, IEEE Trans. Inform. Theory, vol. IT-33, no 3,428–431 (1987).

[5] E. Jonckheere and C. Ma, *A simple Hankel Interpretation of the Berlekamp–Massey Algorith*, Linear Algebra and its Applications 125, 65–76 (1989).

[6] J.L. Massey, *Shift register synthesis and BCH decoding*, IEEE Trans. Inform. Theory, vol. IT-15, 122–127 (1969).

[7] W.H. Mills, *Continued Fractions and Linear Recurrences*, Math. Comput. 29, 173–180 (1975).

[8] Y. Sugiyama et al. *A method for solving key equation for decoding Goppa codes*, Infor. Contr. vol 27, 87–99 (1975).

[9] L.R. Welch and R.A. Scholtz, Continued fractions and Berlekamp's algorithm, IEEE Trans. Inform. Theory, vol. IT-25, 18–27 (1979).