

## Les approximants de Padé-Hermite ou la reconstruction d'équations<sup>1</sup>

### Résumé

Les approximants de Padé-Hermite sont une généralisation des approximants de Padé. Leur calcul peut s'effectuer grâce à un algorithme qui peut être vu comme une généralisation de l'algorithme d'Euclide étendu. Il permet de reconstruire une équation linéaire à coefficients polynomiaux reliant des séries formelles. Ce chapitre définit ces approximants, prouve leur existence, présente un algorithme pour les calculer et donne quelques applications.

### 1. Premières définitions et premiers résultats

Dans toute la suite,  $\mathbb{K}$  désigne un corps quelconque.

**DÉFINITION 1** (approximant de Padé-Hermite). *Soit  $n \geq 1$ ,  $\mathbf{F} = {}^t(f_1, \dots, f_n)$  un vecteur de séries formelles de  $\mathbb{K}[[X]]$  et soit  $\mathbf{d} = (d_1, \dots, d_n) \in \mathbb{N}^n$ . Un vecteur non nul  $\mathbf{P} = (P_1, \dots, P_n)$  de polynômes de  $\mathbb{K}[X]$  est appelé un « approximant de Padé-Hermite de type  $\mathbf{d}$  de  $\mathbf{F}$  » si :*

1. *La valuation  $\text{val}(\mathbf{P} \cdot \mathbf{F})$  de la série  $\mathbf{P} \cdot \mathbf{F} = \sum_{i=1}^n P_i f_i$  est au moins égale à  $\sigma := \sum (d_i + 1) - 1$  ;*
2.  *$\deg(P_i) \leq d_i$  pour tout  $1 \leq i \leq n$ .*

*L'entier  $\sigma$  est alors appelé l'ordre de l'approximant.*

Par exemple, dans la terminologie du cours précédent, si  $r/t \in \mathbb{K}(X)$  est un approximant de Padé de type  $(k, n-k)$  de  $g \in \mathbb{K}[[X]]$ , alors  $(r, t)$  est un approximant de Padé-Hermite pour  $(-1, g)$ , de type  $(k, n-k)$ . Plus généralement, il n'est pas difficile de se convaincre que le problème de reconstruction rationnelle RRS introduit au cours précédent

(RRS) : Calculer  $r, t \in \mathbb{K}[X]$  tels que :  $\deg(r) < k$ ,  $\deg(t) \leq n - k$  et  $r \equiv tg \pmod{f}$ , revient à un calcul d'approximant de Padé-Hermite  $(r, t, s)$  de  $(-1, g, f)$  de type  $(k-1, n-k, n-k+1)$ .

Le premier résultat de ce cours montre l'existence des approximants de Padé-Hermite et fournit également un premier algorithme pour leur calcul.

**THÉORÈME 4.** *Tout vecteur de séries formelles  $\mathbf{F} = (f_1, \dots, f_n) \in \mathbb{K}[[X]]^n$  admet un approximant de Padé-Hermite de type  $\mathbf{d} = (d_1, \dots, d_n) \in \mathbb{N}^n$  donné.*

---

<sup>1</sup>La première rédaction de ce chapitre est due à Pierre Lairez.

DÉMONSTRATION. On procède par coefficients indéterminés. En écrivant  $P_i = \sum_{j=0}^{d_i} p_{ij} X^j$ , on obtient un système linéaire homogène à  $\sigma = \sum_i (d_i + 1) - 1$  équations en les  $\sigma + 1$  inconnues  $p_{ij}$ . Puisqu'il a moins d'équations que d'inconnues, ce système admet forcément une solution non-triviale.  $\square$

L'algorithme qui découle de la preuve du Th. 4 repose sur la recherche d'un élément non-trivial dans le noyau d'une matrice à coefficients dans  $\mathbb{K}$ , de taille  $\sigma \times (\sigma + 1)$ . En utilisant de l'élimination gaussienne, cet algorithme est donc de complexité cubique en  $\sigma$ . Le but de la suite de ce cours est de présenter un algorithme plus efficace, dû à Harm Derksen, de complexité seulement quadratique en  $\sigma$ . En anticipant un peu, cet algorithme revient à effectuer une sorte de pivot de Gauss sur une matrice à coefficients dans  $\mathbb{K}[X]$ , mais de taille bien plus petite que  $\sigma$  (seulement linéaire en  $\max(\mathbf{d})$ ). Dans le cas particulier  $n = 2$ , l'algorithme de Derksen a essentiellement la même complexité que le calcul d'approximants de Padé via l'algorithme d'Euclide étendu.

Le problème d'approximation de Padé-Hermite a été introduit par Hermite en 1873 dans sa preuve de la transcendance de  $e$ , qui utilise le choix très particulier  $\mathbf{F} = (1, e^X, e^{2X}, \dots)$ . Deux autres cas particuliers importants sont : les « approximants algébriques » avec  $\mathbf{F} = (1, f, f^2, \dots)$  et les « approximants différentiels » avec  $\mathbf{F} = (f, f', f'', \dots)$ , où  $f$  est une série de  $\mathbb{K}[[X]]$  donnée. En Maple, le calcul d'approximants algébriques et différentiels se fait grâce aux fonctions `seriestoalgeq` et `seriestodiffeq` du package `gfun`. Le problème général d'approximation peut se traiter en utilisant la fonction `hermite_pade` du package `numapprox`. Ces trois fonctions utilisent toutes (des variantes de) l'algorithme de Derksen.

Il existe diverses généralisations utiles du problème d'approximation de Padé-Hermite, par exemple les « approximants de Padé-Hermite simultanés et matriciels », ou encore des approximants modulo un polynôme arbitraire de degré  $\sigma = \sum_i (d_i + 1) - 1$  au lieu de  $X^\sigma$ . Des algorithmes de complexité quadratique existent pour toutes ces généralisations.

Il existe des algorithmes encore plus rapides, de complexité *essentiellement linéaire* en  $\sigma$ . Ces algorithmes, de type *diviser pour régner* et reposant sur la multiplication rapide de polynômes via la *transformée de Fourier rapide* (FFT), dépassent le cadre de ce cours.

## 2. Algorithme de Derksen : idées et résultats préliminaires

Pour simplifier la présentation, on se restreint dans la suite au cas où le type de l'approximant cherché est de la forme  $\mathbf{d} = (d, \dots, d) \in \mathbb{N}^n$ , pour un certain  $d \in \mathbb{N}$ .

L'idée de l'algorithme de Derksen est de construire non pas un seul approximant de Padé-Hermite, mais toute une famille de tels approximants, et cela de manière incrémentale. Plus exactement, pour  $s = 0, 1, \dots$ , il construit une base d'une forme spéciale, appelée « base minimale », du  $\mathbb{K}[X]$ -module

$$V_s := \{\mathbf{P} \in \mathbb{K}[X]^n \mid \text{val}(\mathbf{P} \cdot \mathbf{F}) \geq s\}.$$

Comme nous le verrons plus loin, une telle base de  $V_\sigma$  pour  $\sigma = nd + n - 1$  contiendra alors nécessairement un approximant de Padé-Hermite de type  $\mathbf{d} = (d, \dots, d)$  de  $\mathbf{F}$ .

Observons que, grâce aux inclusions  $X^s \mathbb{K}[X]^n \subseteq V_s \subseteq \mathbb{K}[X]^n$ , le module  $V_s$  est libre de rang  $n$ . Précisons ce que l'on entend par « base minimale ». Pour ce

faire, nous introduisons d'abord une notion de *degré* et de *type* d'un vecteur de polynômes.

**DÉFINITION 2** (degré et type d'un vecteur de polynômes). *Pour tout vecteur de polynômes  $\mathbf{P} = (P_1, \dots, P_n) \in \mathbb{K}[X]^n$ , on définit*

$$\deg(\mathbf{P}) = \max\{\deg(P_1), \dots, \deg(P_n)\} \quad \text{et} \quad \text{type}(\mathbf{P}) = \max\{i \mid \deg(\mathbf{P}) = \deg(P_i)\}.$$

**DÉFINITION 3** (base minimale). *Soit  $V \subseteq \mathbb{K}[X]^n$  un sous-module libre de rang  $n$ . Une suite  $\mathbf{Q}_1, \dots, \mathbf{Q}_n$  est appelée « base minimale » de  $V$  si pour tout  $i$ , le vecteur  $\mathbf{Q}_i$  est non-nul, de type  $i$ , et de degré minimal parmi les éléments de  $V \setminus \{0\}$  de type  $i$ .*

Le résultat suivant précise le lien entre une base minimale et l'approximation de Padé-Hermite.

**LEMME 1.** *Soit  $d \geq 1$ . Supposons que  $\mathbf{Q}_1, \dots, \mathbf{Q}_n$  est une base minimale de  $V_{nd+n-1}$ . Soit  $\ell$  tel que  $\deg(\mathbf{Q}_\ell)$  est minimal. Alors  $\mathbf{Q}_\ell$  est un approximant de Padé-Hermite de type  $(d, \dots, d)$  pour  $\mathbf{F}$ .*

**DÉMONSTRATION.** Par Th. 4, il existe un vecteur non-nul  $\mathbf{P} \in V_{nd+n-1}$  tel que  $\deg(\mathbf{P}) \leq d$ . Soit  $i$  le type de  $\mathbf{P}$ . On a alors la suite d'inégalités :

$$\deg(\mathbf{Q}_\ell) \leq \deg(\mathbf{Q}_i) \leq \deg(\mathbf{P}) \leq d,$$

qui prouve que  $\mathbf{Q}_\ell$  est un approximant de Padé-Hermite de type  $(d, \dots, d)$  de  $\mathbf{F}$ .  $\square$

Le résultat suivant montre qu'une base minimale est nécessairement une base du  $\mathbb{K}[X]$ -module  $V$  au sens usuel.

**THÉORÈME 5.** *Soit  $V \subseteq \mathbb{K}[X]^n$  un sous-module libre de rang  $n$ . Toute base minimale de  $V$  est une base du  $\mathbb{K}[X]$ -module  $V$ .*

**DÉMONSTRATION.** Montrons d'abord qu'il s'agit d'un système de générateurs. Soit  $W := \mathbb{K}[X]\mathbf{Q}_1 + \dots + \mathbb{K}[X]\mathbf{Q}_n \subseteq V$ . On suppose par l'absurde que  $V \neq W$ . Soit  $\mathbf{P} \in V \setminus W$  un élément minimal dans  $V \setminus W$  pour l'ordre  $\mathbf{P} < \mathbf{Q}$  défini par

$$(1) \quad \begin{aligned} &\deg(\mathbf{P}) < \deg(\mathbf{Q}), \quad \text{ou} \\ &\deg(\mathbf{P}) = \deg(\mathbf{Q}) \quad \text{et} \quad \text{type}(\mathbf{P}) < \text{type}(\mathbf{Q}). \end{aligned}$$

Autrement dit,  $\mathbf{P}$  est de type minimal parmi les éléments de degré minimal de  $V \setminus W$ .

Soit  $i$  le type de  $\mathbf{P}$ . Puisque  $\text{type}(\mathbf{P}) = \text{type}(\mathbf{Q}_i)$  et  $\deg(\mathbf{P}) \geq \deg(\mathbf{Q}_i)$ , il existe un monôme  $q \in \mathbb{K}[X]$  de degré  $\deg(q) = \deg(\mathbf{P}) - \deg(\mathbf{Q}_i)$ , tel que  $\text{type}(\mathbf{P} - q\mathbf{Q}_i) < \text{type}(\mathbf{P})$ . Du coup, comme  $\deg(\mathbf{P} - q\mathbf{Q}_i) \leq \deg(\mathbf{P})$ , on obtient que

$$\mathbf{P} - q\mathbf{Q}_i < \mathbf{P}.$$

Par la minimalité de  $\mathbf{P}$ , il s'ensuit que  $\mathbf{P} - q\mathbf{Q}_i$  appartient à  $W$ , donc  $\mathbf{P} \in W$ , ce qui contredit le choix de  $\mathbf{P}$ .

Pour conclure la preuve, montrons que les  $\mathbf{Q}_i$  forment une famille libre. Si  $\sum_i a_i \mathbf{Q}_i = 0$  est une combinaison polynomiale nulle des  $\mathbf{Q}_i$ , on a que pour tout  $i$ , le vecteur  $a_i \mathbf{Q}_i$  est de type  $i$ . L'assertion découle du lemme suivant.  $\square$

**LEMME 2.** *Si  $\mathbf{P}$  et  $\mathbf{Q}$  sont de type différent, alors  $\text{type}(\mathbf{P} + \mathbf{Q}) \in \{\text{type}(\mathbf{P}), \text{type}(\mathbf{Q})\}$ .*

**DÉMONSTRATION.** Supposons  $j = \text{type}(\mathbf{P}) > i = \text{type}(\mathbf{Q})$ . Si  $\deg(\mathbf{P}) \geq \deg(\mathbf{Q})$ , alors  $\text{type}(\mathbf{P} + \mathbf{Q}) = j$  et si  $\deg(\mathbf{P}) < \deg(\mathbf{Q})$ , alors  $\text{type}(\mathbf{P} + \mathbf{Q}) = i$ .  $\square$

### 3. Algorithme de Derksen : fonctionnement

L'idée de l'algorithme est de construire de proche en proche une base minimale de  $V_s$ , partant de la base minimale des  $\mathbf{Q}_k = (0, 0, \dots, 0, 1, 0, \dots, 0)$  (avec 1 en position  $k$ ) de  $V_0$ . Cf. Lemme 1, l'élément de degré minimal dans une base minimale de  $V_{nd+n-1}$  fournit un approximant de Padé-Hermite de type  $(d, \dots, d)$  de  $\mathbf{F}$ .

Le résultat suivant montre comment construire une base minimale de  $V_{s+1}$  à partir d'une base minimale de  $V_s$ .

THÉORÈME 6. Soit  $\mathbf{Q}_1, \dots, \mathbf{Q}_n$  une base minimale de

$$V_s = \{\mathbf{P} \in \mathbb{K}[X]^n \mid \text{val}(\mathbf{P} \cdot \mathbf{F}) \geq s\}.$$

1. Si  $\text{val}(\mathbf{Q}_i \cdot \mathbf{F}) \geq s + 1$  quel que soit  $i$ , alors  $V_{s+1} = V_s$  et  $\{\mathbf{Q}_1, \dots, \mathbf{Q}_n\}$  est une base minimale de  $V_{s+1}$ .
2. Supposons que  $1 \leq i \leq n$  est tel que les deux conditions suivantes soient réunies :
  - $\text{val}(\mathbf{Q}_i \cdot \mathbf{F}) = s$  ;
  - Si  $\text{val}(\mathbf{Q}_\ell \cdot \mathbf{F}) = s$  pour un  $\ell \neq i$ , alors  $\mathbf{Q}_i < \mathbf{Q}_\ell$ , où  $<$  est l'ordre (1).

Alors :

- (a) Pour  $\ell \neq i$ , il existe un scalaire  $\lambda_\ell \in \mathbb{K}$  tel que  $\tilde{\mathbf{Q}}_\ell := \mathbf{Q}_\ell - \lambda_\ell \mathbf{Q}_i$  vérifie  $\text{val}(\tilde{\mathbf{Q}}_\ell \cdot \mathbf{F}) > s$ .
- (b) En posant  $\tilde{\mathbf{Q}}_i = X\mathbf{Q}_i$ , la suite  $\tilde{\mathbf{Q}}_1, \dots, \tilde{\mathbf{Q}}_n$  forme une base minimale de  $V_{s+1}$ .

DÉMONSTRATION. (1) L'inclusion  $V_{s+1} \subseteq V_s$  est évidente et inversement, cf. Th. 5, tout  $\mathbf{P} \in V_s$  s'écrit comme combinaison linéaire  $\sum_i a_i \mathbf{Q}_i$ , ainsi  $\mathbf{P} \cdot \mathbf{F} = \sum_i a_i (\mathbf{Q}_i \cdot \mathbf{F})$  est de valuation  $\geq s + 1$ , donc  $\mathbf{P} \in V_{s+1}$ .

(2a) Si  $\text{val}(\mathbf{Q}_\ell \cdot \mathbf{F}) > s$ , on pose  $\lambda_\ell = 0$  ; si  $\text{val}(\mathbf{Q}_\ell \cdot \mathbf{F}) = s$ , alors  $\mathbf{Q}_\ell \cdot \mathbf{F} = c_\ell X^s + \dots$  et  $\mathbf{Q}_i \cdot \mathbf{F} = c_i X^s + \dots$ , avec  $c_i \neq 0$ , et alors  $\lambda_\ell := c_\ell / c_i$  convient.

Pour (2b), commençons par montrer que la suite  $\tilde{\mathbf{Q}}_1, \dots, \tilde{\mathbf{Q}}_{i-1}, \mathbf{Q}_i, \tilde{\mathbf{Q}}_{i+1}, \dots, \tilde{\mathbf{Q}}_n$  reste une base minimale de  $V_s$ . Il suffit pour cela de montrer que pour  $\ell \neq i$ , le vecteur  $\tilde{\mathbf{Q}}_\ell$  a même type et même degré que  $\mathbf{Q}_\ell$ . Si  $\text{val}(\mathbf{Q}_\ell \cdot \mathbf{F}) > s$ , c'est évident car  $\lambda_\ell = 0$  et donc  $\tilde{\mathbf{Q}}_\ell = \mathbf{Q}_\ell$ . Sinon, le choix de  $i$  assure que  $\mathbf{Q}_\ell > \mathbf{Q}_i$ , et donc  $\mathbf{Q}_\ell$  et  $\mathbf{Q}_\ell - \lambda_\ell \mathbf{Q}_i$  ont le même degré et type.

Montrons maintenant que  $(\tilde{\mathbf{Q}}_j)_j$  est une base minimale de  $V_{s+1}$ . Comme la multiplication par un polynôme ne change pas le type, celui de  $\tilde{\mathbf{Q}}_i = X\mathbf{Q}_i$  est bien  $i$ . Il suffit donc de montrer que si  $\mathbf{P} \in V_{s+1}$  est de type  $\ell \in \{1, 2, \dots, n\}$ , alors  $\text{deg}(\mathbf{P}) \geq \text{deg}(\mathbf{Q}_\ell)$ . Si  $\ell \neq i$ , ceci est une évidence : comme  $\mathbf{P}$  appartient à  $V_{s+1} \subseteq V_s$ , et comme la suite  $\tilde{\mathbf{Q}}_1, \dots, \tilde{\mathbf{Q}}_{i-1}, \mathbf{Q}_i, \tilde{\mathbf{Q}}_{i+1}, \dots, \tilde{\mathbf{Q}}_n$  forme une base minimale de  $V_s$ , le degré de  $\mathbf{P}$  est nécessairement au moins égal à  $\text{deg}(\tilde{\mathbf{Q}}_\ell) = \text{deg}(\mathbf{Q}_\ell)$ .

Dans la suite de la preuve, on peut donc supposer que  $\mathbf{P} \in V_{s+1}$  est de type  $i$ , le but étant de montrer que  $\text{deg}(\mathbf{P}) \geq \text{deg}(X\mathbf{Q}_i)$ . Par Th. 5,  $\mathbf{P}$  s'écrit  $\mathbf{P} = \sum_{j \neq i} a_j \tilde{\mathbf{Q}}_j + a_i \mathbf{Q}_i$ . Comme  $\text{type}(\mathbf{P}) = i$ , on a  $a_i \neq 0$ , par le Lemme 2. De plus, le degré de  $\mathbf{P}$  est égal à celui de  $a_i \mathbf{Q}_i$ , cf. Lemme 3 ci-dessous.

Comme  $\text{val}(\mathbf{P} \cdot \mathbf{F}) > s$  et comme pour  $k \neq i$ ,  $\text{val}(\mathbf{Q}_k \cdot \mathbf{F}) > s$ , on a nécessairement que  $\text{val}(a_i) > 0$ . En particulier  $\text{deg}(a_i) > 0$  et donc  $\text{deg}(\mathbf{P}) \geq 1 + \text{deg}(\mathbf{Q}_i)$ .  $\square$

LEMME 3. Si  $\text{type}(\mathbf{P}) = \text{type}(\mathbf{Q}) = i$  et  $\text{type}(\mathbf{P} + \mathbf{Q}) < i$ , alors  $\text{deg}(\mathbf{P}) = \text{deg}(\mathbf{Q})$ .

**Derksen**

**Entrée :**  $\mathbf{F} = (f_1, \dots, f_n) \in \mathbb{K}[[X]]^n$  et  $d \geq 1$ .  
**Sortie :** Un approximant de Padé-Hermite de  $\mathbf{F}$ , de type  $(d, \dots, d)$ .

pour  $k$  de 1 à  $n$  définir  
 $\mathbf{Q}_k := (0, 0, \dots, 0, 1, 0, \dots, 0)$ , avec 1 en position  $k$ .  
pour  $j$  de 0 à  $nd + n - 2$  faire  
 $i := 0$   
pour  $k$  de 1 à  $n$  faire  
 $c_k := \text{coeff}(\mathbf{Q}_k \cdot \mathbf{F}, j)$   
si  $c_k \neq 0$  et  $(\mathbf{Q}_k < \mathbf{Q}_i$  ou  $i = 0)$ , alors  $i := k$   
si  $i \neq 0$  alors  
 $\mathbf{Q}_i := c_i^{-1} \mathbf{Q}_i$   
pour  $k$  de 1 à  $n$  faire  
si  $k \neq i$  alors  
 $\mathbf{Q}_k := \mathbf{Q}_k - c_k \mathbf{Q}_i$   
 $\mathbf{Q}_i := X \mathbf{Q}_i$   
 $p := 1$   
pour  $k$  de 2 à  $n$  faire  
si  $\deg(\mathbf{Q}_k) < \deg(\mathbf{Q}_p)$ , alors  $p := k$   
Renvoyer  $\mathbf{Q}_p$ .

FIG. 1. L'algorithme de Derksen

DÉMONSTRATION. Soient  $\mathbf{P} = (P_1, \dots, P_n)$  et  $\mathbf{Q} = (Q_1, \dots, Q_n)$ . L'hypothèse entraîne les égalités  $\deg(P_i) = \deg(\mathbf{P})$  et  $\deg(Q_i) = \deg(\mathbf{Q})$ . Cela implique que  $P_i$  et  $Q_i$  ont le même degré; sinon, le type de  $\mathbf{P} + \mathbf{Q}$  serait égal à  $i$ .  $\square$

L'algorithme qui se déduit de la conjonction du Lemme 1 et du Théorème 6 est donné en Fig. 1. Il est de complexité bornée par  $O(n\sigma^2)$ .

Remarquons que dans le cas « générique » (dit *normal*), la sortie  $\mathbf{Q} = \mathbf{Q}_1, \dots, \mathbf{Q}_n$  est de degré

$$\begin{bmatrix} d+1 & d & \cdots & d & d \\ d+1 & d+1 & \cdots & d & d \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ d+1 & d+1 & \cdots & d+1 & d \\ d & d & \cdots & d & d \end{bmatrix}.$$

C'est la dernière ligne  $\mathbf{Q}_n$  qui fournit l'approximant désiré.

#### 4. Applications

On rappelle que si une série est connue comme rationnelle de degré au plus  $d$ , l'approximation de Padé de type  $(d, d)$  suffit pour reconstruire la fraction rationnelle. Une question naturelle est comment se généralise cette observation dans le cadre de l'approximation de Padé-Hermite. Les réponses sont partielles, mais entièrement satisfaisantes dans la pratique.

**4.1. Recherche de relations à coefficients polynomiaux entre séries formelles.** Supposons qu'il existe une combinaison linéaire  $\sum_{i=1}^n P_i f_i = 0$ , à coefficients des polynômes  $P_i(X) \in \mathbb{K}[X]$  de degrés au plus  $d$ . Par ailleurs, supposons calculé un approximant de Padé-Hermite  $\mathbf{Q} := (Q_1, \dots, Q_n)$  de  $\mathbf{F} = (f_1, \dots, f_n)$  de type  $\mathbf{d} = (d, \dots, d)$ , via l'algorithme de Derksen. La question est donc : quel lien y a-t-il entre  $\mathbf{P} = (P_1, \dots, P_n)$  et  $\mathbf{Q}$  ?

D'abord, dans le cas *générique*, la réponse est très simple :  $\mathbf{P}$  et  $\mathbf{Q}$  sont identiques, à un coefficient scalaire près. En effet,  $\mathbf{Q} = \mathbf{Q}_n$  et  $\mathbf{Q}_1, \dots, \mathbf{Q}_n$  est une base de  $V_{nd+n-1}$  dont les degrés sont décrits après l'algo Derksen. En particulier,  $\mathbf{P}$  doit être une combinaison linéaire des  $\mathbf{Q}_i$ . Des considérations sur les degrés, utilisant la forme bien particulière des degrés des  $\mathbf{Q}_i$ , mènent à la conclusion désirée.

En effet, si  $(c_1(X), \dots, c_n(X)) \cdot {}^t(\mathbf{Q}_1, \dots, \mathbf{Q}_n) = \mathbf{P}$ , alors  $c_1 Q_{11} + \dots + c_n Q_{n1} = P_1$ , et comme  $\deg(Q_{11}) = d + 1$  et  $\deg(Q_{j1}) = d$  pour  $j > 1$  et  $\deg(P_1) \leq d$ , on obtient que  $c_1 = 0$ . De même,  $c_2 = \dots = c_{n-1} = 0$  et  $c_n$  doit être une constante  $c \in \mathbb{K}$  telle que  $\mathbf{P} = c\mathbf{Q}$ .

Dans le cas général, un argument de nothérianité permet de prouver que pour  $D \gg 0$ ,  $V_{nD+n-1}$  contient la relation  $\mathbf{P}$ , qui sera trouvée par l'algorithme de Derksen. Seulement, on ne dispose pas de borne *a priori* en fonction de  $d$ , sur le  $D$  minimal avec cette propriété. En effet, si on note

$$W_j := \{\mathbf{Q} \in \mathbb{K}[[X]]^n \mid \text{val}(\mathbf{Q} \cdot \mathbf{F}) \geq j \text{ et } \deg(\mathbf{Q}) \leq \deg(\mathbf{P})\},$$

et  $W_\infty = \bigcap_{j \geq 0} W_j$ , alors  $W_\infty$  contient toutes les relations de  $F$  en degré  $d$ , et en particulier  $\mathbf{P}$ . Puisque  $W_0 \supseteq W_1 \supseteq W_2 \supseteq \dots$  est une suite décroissante d'espaces vectoriels de dimension finie, elle est stationnaire, donc il existe un  $N$  tel que  $W_\infty = W_N = W_{N+1} = \dots$ . Le cas *normal* correspond à la situation où  $\dim(W_{k+1}) = \dim(W_k) - 1$  pour chaque  $k$  (noter la ressemblance avec la normalité de la suite des restes dans l'algorithme d'Euclide).

**4.2. Reconstruction d'équations algébriques et différentielles.** Deux cas particuliers importants, pour lesquels on peut être encore plus précis, sont les approximants algébriques et différentiels.

Soit  $f \in \mathbb{K}[[X]]$  une série formelle algébrique. Le problème d'approximation algébrique consiste à retrouver, à partir des premiers termes de  $f$  un polynôme  $P(X, Y) \in \mathbb{K}[X, Y]$  tel que  $P(X, f(X)) = 0$ . Si un tel  $P$ , de degré  $d$  en  $X$  et  $n$  en  $Y$  existe, alors les coefficients des puissances de  $Y$  formeront un approximant de Padé-Hermite de type  $(d, \dots, d)$  du vecteur de séries  $(1, f, \dots, f^n)$ . La difficulté vient de ce que un calcul d'approximation de Padé-Hermite ne trouve, *a priori*, qu'un polynôme  $Q \in \mathbb{K}[X, Y]$  tel que  $Q(X, f(X)) = 0 \pmod{X^\sigma}$ , où  $\sigma = (n+1)d - 1$ . On dit alors qu'on a *deviné* un polynôme annulateur  $Q$  de  $f$ .

Il se pose donc la question de la *certification a posteriori* de  $Q$ , c'est-à-dire qu'on souhaiterait déduire que non seulement  $Q(X, f(X)) = 0 \pmod{X^\sigma}$ , mais aussi  $Q(X, f(X)) = 0$ . Pour les approximants différentiels, la problématique est la même, la seule différence étant qu'on calcule un approximant de Padé-Hermite du vecteur des dérivées successives  $(f, f', \dots, f^{(n)})$ .

Le résultat suivant apporte une réponse partielle à la question de la certification. Il sera prouvé grâce à des techniques de résultant au Chapitre 10. Son avantage est qu'il ne dépend pas de l'algorithme utilisé pour produire l'approximant de Padé-Hermite.

**THÉORÈME 7.** *Supposons que  $f \in \mathbb{K}[[X]]$  est racine d'un polynôme irréductible de  $\mathbb{K}[X, Y]$  de degré au plus  $d$  en  $X$  et au plus  $n$  en  $Y$ . Soit  $\mathbf{Q} = (Q_0, Q_1, \dots, Q_n)$  un approximant de Padé-Hermite de type  $(d, \dots, d)$  de  $\mathbf{F} = (1, f, \dots, f^n)$ .*

*Si  $\text{val}(\mathbf{Q} \cdot \mathbf{F}) \geq 2dn$ , alors  $\mathbf{Q} \cdot \mathbf{F} = 0$ , c'est-à-dire que  $f$  est racine du polynôme  $Q = \sum_{i=1}^n Q_i Y^i$ .*

**4.3. Reconstruction de récurrences.** Soit  $(a_n)_n \in \mathbb{K}^{\mathbb{N}}$  une suite vérifiant une récurrence linéaire à coefficients polynomiaux. Comment, à partir des premiers termes de la suite, retrouver les coefficients de cette récurrence ?

L'idée consiste à trouver une équation différentielle, à coefficients polynomiaux, portant sur la série génératrice de la suite. Cette équation peut être devinée grâce à la méthode proposée au paragraphe 4.2. Il suffit ensuite de passer de l'équation différentielle à l'expression de la récurrence, ce qui n'est pas trivial mais purement formel et sera vu au Chapitre 8.

### 5. Approximants de Padé-Hermite de type arbitraire

Pour calculer un approximant de Padé-Hermite de type  $\mathbf{d} = (d_1, \dots, d_n)$ , il suffit de remplacer dans l'algorithme donné en Fig. 1,  $\text{deg}$  par  $\text{deg}_{\mathbf{d}}$  et  $\text{type}$  par  $\text{type}_{\mathbf{d}}$ , où :

$$\text{deg}_{\mathbf{d}}(\mathbf{P}) = \max\{\text{deg}(P_1) - d_1, \dots, \text{deg}(P_n) - d_n\}$$

et

$$\text{type}_{\mathbf{d}}(\mathbf{P}) = \max\{i \mid \text{deg}(P_i) - d_i = \text{deg}_{\mathbf{d}}(\mathbf{P})\}.$$