Padé-Hermite approximation - ctd

September 23rd, 2020

Overview

Linearly recurring sequences

$$a_i p_0 + a_{i+1} p_1 + \ldots + a_{i+n} p_n = 0, \ \forall i \geq 0$$

How to compute the minimal polynomial?

- There exists a generating polynomial of degree $\leq n$
- $h(x) = \sum_{i=0}^{2n-1} a_{2n-i-1} x^i$

***p* is the minimal polynomial if and only if** *p* is minimal such that

$$p(x)h(x) = r(x) \bmod x^{2n}, \;\; \deg r < \deg p$$

$$\begin{bmatrix} h(x) & -1 \end{bmatrix} \begin{bmatrix} p(x) & \cdot \\ r(x) & \cdot \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix} \bmod x^{2n}$$

Padé-Hermite approximation

Minimal approximant basis

$H(x)$ an $m \times 2m$ matrix of power series in $\mathsf{K}[[x]]$

A polynomial matrix $B \in \mathsf{K}[x]^{(2m)\times(2m)}$ is a **minimal approximant basis** of H at order σ if:

- its columns form a basis of the $\mathsf{K}[x]$-module of vectors $v \in \mathsf{K}[x]^{2m}$ such that $Hv = 0 \bmod x^\sigma$
- the basis is minimal

Minimal approximant basis

$H(x)$ an $m \times 2m$ matrix of power series in $\mathsf{K}[[x]]$

A polynomial matrix $B \in \mathsf{K}[x]^{(2m)\times(2m)}$ is a **minimal approximant basis** of H at order σ if:

- its columns form a basis of the $\mathsf{K}[x]$-module of vectors $v \in \mathsf{K}[x]^{2m}$ such that $Hv = 0 \bmod x^\sigma$
- the basis is minimal

$m = 1, \sigma = 6$

$$\begin{bmatrix} 5 + 3\,x + 2\,x^2 + x^3 + x^4 & -1 \end{bmatrix} \begin{bmatrix} x^2 - x - 1 & 2\,x^4 - 3\,x^3 \\ -8\,x - 5 & x^4 - 15\,x^3 \end{bmatrix} = \begin{bmatrix} x^6 & 2\,x^8 - x^7 + x^6 \end{bmatrix}$$

Algorithm $m = 1$

At step i:

$$\begin{bmatrix} g(x) & h(x) \end{bmatrix} \begin{bmatrix} b_{i,1}(x) & c_{i,1}(x) \\ b_{i,2}(x) & c_{i,2}(x) \end{bmatrix} = \begin{bmatrix} \rho\, x^i + x^{i+1}(\ldots) & \tau\, x^i + x^{i+1}(\ldots) \end{bmatrix}$$

- $\tau \neq 0$, $\deg b_i \geq \deg c_i$: $\quad b_{i+1} \leftarrow b_i - (\rho/\tau)\, c_i \quad c_{i+1} \leftarrow x\, c_i$
- $\tau = 0$, $\quad b_{i+1} \leftarrow x\, b_i$

Algorithm $m = 1$

At step i:

$$\begin{bmatrix} g(x) & h(x) \end{bmatrix} \begin{bmatrix} b_{i,1}(x) & c_{i,1}(x) \\ b_{i,2}(x) & c_{i,2}(x) \end{bmatrix} = \begin{bmatrix} \rho\, x^i + x^{i+1}(\ldots) & \tau\, x^i + x^{i+1}(\ldots) \end{bmatrix}$$

- $\tau \neq 0$, $\deg b_i \geq \deg c_i$: $\quad b_{i+1} \leftarrow b_i - (\rho/\tau)\, c_i \quad c_{i+1} \leftarrow x\, c_i$
- $\tau = 0$, $\quad b_{i+1} \leftarrow x\, b_i$

Cost bound: $O(\sigma^2)$

Two other algorithms “essentially equivalent” to the minimal approximant algorithm?

Berlekamp–Massey algorithm

- Shortest linear feedback shift register (LFSR) for a given binary output sequence
- Minimal polynomial of a linearly recurring sequence
- Decoding

Berlekamp–Massey algorithm

- Shortest linear feedback shift register (LFSR) for a given binary output sequence
- Minimal polynomial of a linearly recurring sequence
- Decoding

→ Given two polynomials sequence of polynomials with decreasing degrees

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-33, NO. 3, MAY 1987

On the Equivalence Between Berlekamp's and Euclid's Algorithms

JEAN LOUIS DORNSTETTER

***Abstract*—It is shown that Berlekamp's iterative algorithm can be derived from a normalized version of Euclid's extended algorithm. Simple proofs of the results given recently by Cheng are also presented.**

cost $\leq$ number of iterations $\times$ approximation order ?

$$H(x)B^{(1)}(x) = x^{\sigma}R(x)$$

$$H(x)B^{(1)}(x)Q(x) = x^{\sigma+k}S(x)$$

$$H(x)B^{(1)}(x) = x^{\sigma}R(x)$$
$$H(x)B^{(1)}(x)Q(x) = x^{\sigma+k}S(x)$$

$$\downarrow$$

$$H(x)B^{(1)}(x) = x^{\sigma}R(x)$$
$$R(x)B^{(2)}(x) = x^{k}T(x)$$

$$H(x)B^{(1)}(x) = x^{\sigma}R(x)$$
$$H(x)B^{(1)}(x)Q(x) = x^{\sigma+k}S(x)$$

$$\downarrow$$

$$H(x)B^{(1)}(x) = x^{\sigma}R(x)$$
$$R(x)B^{(2)}(x) = x^{k}T(x)$$

One has $H(x)B^{(1)}(x)B^{(2)}(x) = (x^{\sigma}R(x))B^{(2)}(x) = x^{\sigma+k}T(x)$

Is $B^{(1)}B^{(2)}$ a correct answer ?

Recursive approximant computation (simplified)

1. Approximation basis for $H(x)$ at order $\sigma/2$, input degrees $(0, 0)$

Recursive approximant computation (simplified)

1. Approximation basis for $H(x)$ at order $\sigma/2$, input degrees $(0,0)$
2. $H'(x) = x^{-\sigma/2} H(x) B^{(1)}(x)$

Recursive approximant computation (simplified)

1. Approximation basis for $H(x)$ at order $\sigma/2$, input degrees $(0,0)$
2. $H'(x) = x^{-\sigma/2} H(x) B^{(1)}(x) \mod x^{\sigma/2}$
3. Approximation basis for $H'(x)$ at order $\sigma/2$,

Recursive approximant computation (simplified)

1. Approximation basis for $H(x)$ at order $\sigma/2$, input degrees $(0,0)$
2. $H'(x) = x^{-\sigma/2} H(x) B^{(1)}(x) \mod x^{\sigma/2}$
3. Approximation basis for $H'(x)$ at order $\sigma/2$, input degrees (d_1, d_2)
4. $B(x) = B^{(1)}(x) B^{(2)}(x)$

Recursive approximant computation (simplified)

1. Approximation basis for $H(x)$ at order $\sigma/2$, input degrees $(0,0)$
2. $H'(x) = x^{-\sigma/2} H(x) B^{(1)}(x) \mod x^{\sigma/2}$
3. Approximation basis for $H'(x)$ at order $\sigma/2$, input degrees (d_1, d_2)
4. $B(x) = B^{(1)}(x) B^{(2)}(x)$

Correctness: uses only the first σ coefficients of H

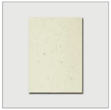
Cost: $\mathsf{T}(n) \leq 2\mathsf{T}(n/2) + O(\mathsf{M}(n))$ $\quad O(\mathsf{M}(n) \log n)$

Recursive approximant computation (simplified)

1. Approximation basis for $H(x)$ at order $\sigma/2$, input degrees $(0,0)$
2. $H'(x) = x^{-\sigma/2}H(x)B^{(1)}(x) \mod x^{\sigma/2}$
3. Approximation basis for $H'(x)$ at order $\sigma/2$, input degrees (d_1, d_2)
4. $B(x) = B^{(1)}(x)B^{(2)}(x)$

Correctness: uses only the first σ coefficients of H

Cost: $\mathsf{T}(n) \leq 2\mathsf{T}(n/2) + O(\mathsf{M}(n))$ $\quad O(\mathsf{M}(n)\log n)$



In general

$$\begin{array}{cc} & 2m \\ m & \begin{bmatrix} & H(x) & \end{bmatrix} \end{array} \begin{bmatrix} \\ B_i(x) \\ \\ \end{bmatrix} = \begin{bmatrix} & R & \end{bmatrix} + x^{i+1} T$$

$$\in K^{m \times 2m}$$

In general

$$\begin{array}{cc} & 2m \\ m & \left[\; H(x) \; \right] \end{array} \left[\; B_i(x) \; \right] = \left[\; R \; \right] + x^{i+1} T$$

$$R \in K^{m \times 2m}$$

To progress from order i to order $i+1$

→ elimination in $2m-1$ columns using a "pivot" one

→ the pivot column is multiplied by x

$$\begin{array}{cc} & 2m \\ m & \left[\; H(x) \; \right] \end{array} \left[\; \tilde{B}_i(x) \; \right] = \left[\begin{array}{cccc} 0 & 0 & \cdots & 0 \\ \hline & ////& & \end{array} \right] + x^{i+1} T$$

$H(x) \bmod x^8$, 6×3

$$\begin{bmatrix} 14x^7+13x^5+13x^4+x^3+15x^2+13x+1 & 8x^7+18x^6+3x^5+6x^4+13x^3+5x^2+12x+2 & 5x^7+14x^6+8x^5+6x^4+13x^3+9x^2+7x+16 & -1 & 0 & 0 \\ x^6+9x^4+5x^2+7 & 18x^7+17x^6+10x^5+x^4+14x^3+9x^2+12x+7 & 11x^7+9x^6+4x^5+5x^4+17x^3+7x^2+x+6 & 0 & -1 & 0 \\ 12x^7+15x^6+5x^5+12x^4+4x^3+12x^2+4x+17 & 15x^7+2x^6+3x^5+12x^4+6x^3+6x^2+x+3 & 6x^7+6x^6+8x^5+7x^4+12x^3+5x^2+14 & 0 & 0 & -1 \end{bmatrix}$$

sigma = 6 is a multiple of the dimension m = 3

```
> OB:=Obasis(F,x,[0,0,0,0,0,0],m,6) mod q;
```

$$OB := \begin{bmatrix} x+12 & 17x+7 & 17x+4 & 2x & 8x & 11x \\ 11 & x+3 & 12x+6 & 2x & 2x & 7x \\ 13 & 9 & x+4 & 8x & 17x & 11x \\ 14 & 5 & 4 & x & 18x & 11x \\ 11 & 10 & 18 & 0 & x & 2x \\ 1 & 7 & 9 & 0 & 0 & x \end{bmatrix}$$

```
> map(t->series(t,x,3) mod q, M.OB);
```

$$\begin{bmatrix} 4x^2+O(x^3) & 16x^2+O(x^3) & 4x^2+O(x^3) & 11x^2+O(x^3) & O(x^3) & O(x^3) \\ 3x^2+O(x^3) & 4x^2+O(x^3) & O(x^3) & 13x^2+O(x^3) & 3x^2+O(x^3) & O(x^3) \\ 13x^2+O(x^3) & 7x^2+O(x^3) & 13x^2+O(x^3) & 10x^2+O(x^3) & 15x^2+O(x^3) & 13x^2+O(x^3) \end{bmatrix}$$

sigma = 7, one new column of valuation 3

```
> OB:=Obasis(F,x,[0,0,0,0,0,0],m,7) mod q;
```

$$OB := \begin{bmatrix} x^2+12x & 13x+16 & 16x+11 & 4x+5 & 8x & 11x \\ 11x & x+16 & 12x+14 & 2x+3 & 2x & 7x \\ 13x & 14 & x+10 & 8x+7 & 17x & 11x \\ 14x & 6 & 9 & x+9 & 18x & 11x \\ 11x & 4 & 7 & 3 & x & 2x \\ x & 3 & 8 & 2 & 0 & x \end{bmatrix}$$

```
> map(t->series(t,x,3) mod q, M.OB);
```

$$\begin{bmatrix} O(x^3) & O(x^3) & O(x^3) & O(x^3) & O(x^3) & O(x^3) \\ O(x^3) & 11x^2+O(x^3) & 16x^2+O(x^3) & O(x^3) & 3x^2+O(x^3) & O(x^3) \\ O(x^3) & 12x^2+O(x^3) & O(x^3) & 17x^2+O(x^3) & 15x^2+O(x^3) & 13x^2+O(x^3) \end{bmatrix}$$

sigma = 8, two new columns of valuation 3

```
>
>
> OB:=Obasis(F,x,[0,0,0,0,0,0],m,8) mod q;
```

$$OB := \begin{bmatrix} x^2+12x & 13x^2+16x & 4x+5 & 4x+5 & x+6 & 11x \\ 11x & x^2+16x & 14x+8 & 2x+3 & 6 & 7x \\ 13x & 14x & x & 8x+7 & 17x+10 & 11x \\ 14x & 6x & 2 & x+9 & 18x+7 & 11x \\ 11x & 4x & 15 & 3 & x+11 & 2x \\ x & 3x & 14 & 2 & 13 & x \end{bmatrix}$$

```
> map(t->series(t,x,3) mod q, M.OB);
```

$$\begin{bmatrix} O(x^3) & O(x^3) & O(x^3) & O(x^3) & O(x^3) & O(x^3) \\ O(x^3) & O(x^3) & O(x^3) & O(x^3) & O(x^3) & O(x^3) \\ O(x^3) & O(x^3) & 5x^2+O(x^3) & 17x^2+O(x^3) & 10x^2+O(x^3) & 13x^2+O(x^3) \end{bmatrix}$$

```
>
```

sigma = 8, two new columns of valuation 3

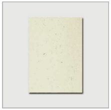
```
>
>
> OB:=Obasis(F,x,[0,0,0,0,0,0],m,8) mod q;
```

$$OB := \begin{bmatrix} x^2+12x & 13x^2+16x & 4x+5 & 4x+5 & x+6 & 11x \\ 11x & x^2+16x & 14x+8 & 2x+3 & 6 & 7x \\ 13x & 14x & x & 8x+7 & 17x+10 & 11x \\ 14x & 6x & 2 & x+9 & 18x+7 & 11x \\ 11x & 4x & 15 & 3 & x+11 & 2x \\ x & 3x & 14 & 2 & 13 & x \end{bmatrix}$$

```
> map(t->series(t,x,3) mod q, M.OB);
```

$$\begin{bmatrix} \boxed{\begin{matrix} O(x^3) & O(x^3) \\ O(x^3) & O(x^3) \\ O(x^3) & O(x^3) \end{matrix}} & \begin{matrix} O(x^3) & O(x^3) & O(x^3) & O(x^3) \\ O(x^3) & O(x^3) & O(x^3) & O(x^3) \\ \multicolumn{4}{c}{\boxed{5x^2+O(x^3) \quad 17x^2+O(x^3) \quad 10x^2+O(x^3) \quad 13x^2+O(x^3)}} \end{matrix} \end{bmatrix}$$

```
>
```



$\Rightarrow$ m steps for going to $i+1$

if σ elementary steps

$d = \frac{\sigma}{m}$ "matrix" steps

for having order d

** Ensure that the basis is minimal by carefully choosing the pivot column

** Gather together the elementary steps to use fast linear algebra

** play with input degrees for satisfying degree constraints

Slow algorithm

1. d matrix steps
2. m elementary steps
3. $O(m)$ vector operations
   degree d

3. $m^2 d$
2. $m^3 d$
1. $\underline{\underline{m^3 d^2}}$

Recursive matrix algorithm

- Divide & conquer w.r.t. the degree
- Linear algebra in $O(m^{\omega})$

$$\tilde{O}(m^{\omega} d)$$

$$\begin{array}{cc} & 2m \\ m & \begin{bmatrix} \; H(x) \; \end{bmatrix} \end{array} \begin{bmatrix} \; B(x) \; \end{bmatrix} = O(x^d)$$

Minimal approximant basis (general dimensions)

$H(x)$ an $m \times k$ matrix of power series in $\mathsf{K}[[x]]$

A polynomial matrix $B \in \mathsf{K}[x]^{k \times k}$ is a **minimal approximant basis** of H at order σ if:

- its columns form a basis of the $\mathsf{K}[x]$-module of vectors $v \in \mathsf{K}[x]^k$ such that $Hv = 0 \bmod x^\sigma$
- the basis is minimal

Fast Power Hermite Pad Solver [Beckermann & Labahn 1994, Derksen 1994]

FPHPS ALGORITHM

INPUT: $m \geq 2, s \in \mathbb{N}, \mathbf{F} = (f_1, \dots f_m)^T$, multiindex $\mathbf{n} = (n_1, \dots, n_m)$

INITIALIZATION: Let for $\sigma = 0, l = 1, \dots, m$:

$d_{l,0} = n_l, \mathbf{P}_{l,0} = (0, \dots, 0, 1, 0, \dots, 0)$($l$th unit vector)

RECURSIVE STEP: For $\sigma = 0, 1, 2, \dots$:

Let for $l = 1, \dots, m$: $c_{l,\sigma} = z^{-\sigma} \cdot \mathbf{P}_{l,\sigma}(z^s) \cdot \mathbf{F}(z)|_{z=0}$ and $\Lambda_\sigma = \{l \ : \ c_{l,\sigma} \neq 0\}$

CASE $\Lambda_\sigma = \{\}$, then for $l = 1, \dots, m$:

$\mathbf{P}_{l,\sigma+1} = \mathbf{P}_{l,\sigma}, d_{l,\sigma+1} = d_{l,\sigma}$

CASE $\Lambda_\sigma \neq \{\}$, then let $\pi = \pi_\sigma \in \Lambda_\sigma$ be defined by

$d_{\pi,\sigma} = \max \{d_{l,\sigma} \ : \ l \in \Lambda_\sigma\}$

and compute for $l = 1, \dots, m$:

$l \in \Lambda_\sigma, l \neq \pi$: $\mathbf{P}_{l,\sigma+1} = \mathbf{P}_{l,\sigma} - \frac{c_{l,\sigma}}{c_{\pi,\sigma}} \cdot \mathbf{P}_{\pi,\sigma}, d_{l,\sigma+1} = d_{l,\sigma}$

$l \notin \Lambda_\sigma$: $\mathbf{P}_{l,\sigma+1} = \mathbf{P}_{l,\sigma}, d_{l,\sigma+1} = d_{l,\sigma}$

$l = \pi$: $\mathbf{P}_{\pi,\sigma+1} = z \cdot \mathbf{P}_{\pi,\sigma}, d_{\pi,\sigma+1} = d_{\pi,\sigma} - 1$

OUTPUT: For $\sigma = 0, 1, 2, \dots$:

σ-bases $\mathbf{P}_{1,\sigma}, \dots, \mathbf{P}_{m,\sigma}$ with dct $\mathbf{P}_{l,\sigma} = d_{l,\sigma} + 1, l = 1, \dots, m$, i.e.

for all δ: $\mathcal{L}_\delta^\sigma = \{\alpha_1 \cdot \mathbf{P}_{1,\sigma} + \dots + \alpha_m \cdot \mathbf{P}_{m,\sigma} \ : \ \deg \ \alpha_l \leq d_{l,\sigma} + \delta\}$.

Note added:

Here transposed problem i.e. approximant on the left (row operations)

m x k --> k x m, actually with m=1 (1 x k) in the course

The general problem (matrix vs vector) could be reduced to the one here

Algorithm `PM-Basis`$(G,\ d,\ \delta)$
Input: $G \in \mathsf{K}[[x]]^{m\times n}$ with $m \geq n$, $d \in \mathbb{N}$ and $\delta \in \mathbb{N}^m$.
Output: a σ-basis $M \in \mathsf{K}[x]^{m\times m}$ with $\sigma = nd$, $\mu \in \mathbb{N}^m$.
Condition: $d = 0$ or $\log d \in \mathbb{N}$.

if $d = 0$ then $(M, \mu) := (I_m, \delta)$;
else if $d = 1$ then $(M, \mu) :=$ `M-Basis`(G, d, δ);
else if $d \geq 2$ then
  $(M', \mu') :=$ `PM-Basis`$(G, d/2, \delta)$;
  $G' := x^{-d/2} M' G \bmod x^{d/2}$;
  $(M'', \mu'') :=$ `PM-Basis`$(G', d/2, \mu')$;
  $(M, \mu) := (M'' M', \mu'')$;
fi;
return (M, μ);

Transposed problem also here, in the lesson : m x k
m x k --> k x m (m x n)

the order sigma is for elementary steps, hence the matrix order d is sigma here divided by n

Related problem - 1

Bézout relation

$a(x), b(x) \in \mathsf{K}[x]$, degree n

compute a relation

$$u(x)a(x) + v(x)b(x) = g(x)$$

where $g(x)$ is the gcd, say of degree k

with $\deg u < \deg b - k$ and $\deg v < \deg a - k$

Related problem - 2

Rational reconstruction

$f(x) \in \mathsf{K}[x]$, degree n

$h(x)$

Find $p(x)$ and $q(x)$ such that for k given $1 \leq k \leq n$:

$$h(x) = \frac{p(x)}{q(x)} \bmod f(x)$$

with gcd$(q,f) = 1$, $\deg p < k$, $\deg q \leq n-k$

Related problem - 3

$$a(x)u(x) = v(x) \bmod x^{2n+1}$$

Toeplitz (Hankel) linear system

$$\begin{bmatrix} a_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & a_0 & 0 \\ a_n & \ddots & a_1 & a_0 \\ a_{n+1} & a_n & \ddots & a_1 \\ \vdots & \ddots & a_n & \ddots \\ a_{2n} & a_{2n-1} & \ddots & a_n \\ 0 & a_{2n} & \ddots & \ddots \\ \vdots & \ddots & \ddots & a_{2n-1} \\ 0 & \cdots & 0 & a_{2n} \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_n \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

Related problem - 3

$$a(x)u(x) = v(x) \bmod x^{2n+1}$$

Toeplitz (Hankel) linear system

$$\begin{bmatrix} a_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & a_0 & 0 \\ a_n & \ddots & a_1 & a_0 \\ a_{n+1} & a_n & \ddots & a_1 \\ \vdots & \ddots & a_n & \ddots \\ a_{2n} & a_{2n-1} & \ddots & a_n \\ 0 & a_{2n} & \ddots & \ddots \\ \vdots & \ddots & \ddots & a_{2n-1} \\ 0 & \cdots & 0 & a_{2n} \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_n \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

Related problem - 3

Toeplitz (Hankel) linear system

[Brent, Gustavson & Yun]

THEOREM 6 (Gohberg and Semencul). *If the Toeplitz matrix T is such that each of the systems of equations $Tx = e_0$, $Ty^r = e_n$ is solvable where $y^r = (y_n, \ldots, y_0)$, and the condition $x_0 = y_0 \neq 0$ is fulfilled, then the matrix T is invertible, and its inverse S is formed according to the formula*

$$
S = \frac{1}{x_0}\left\{ \begin{bmatrix} x_0 & 0 & \cdot & 0 \\ x_1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 \\ x_n & \cdot & x_1 & x_0 \end{bmatrix} \begin{bmatrix} y_0 & y_1 & \cdot & y_n \\ 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & y_1 \\ 0 & \cdot & 0 & y_0 \end{bmatrix} \right.
$$

$$
\left. - \begin{bmatrix} 0 & \cdot & \cdot & 0 \\ y_n & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ y_1 & \cdot & y_n & 0 \end{bmatrix} \begin{bmatrix} 0 & x_n & \cdot & x_1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & x_n \\ 0 & \cdot & \cdot & 0 \end{bmatrix} \right\}
$$

Theorem of polynomials

In $O(\mathsf{M}(n)\log n) = \tilde{O}(n)$ arithmetic operations one can solve:

- Multipoint evaluation and interpolation
- Minimal polynomial of a linearly recurring sequence
- Gcd and Bézout relation
- Rational reconstruction and Padé approximation
- Hankel and Toeplitz linear system

Theorem of polynomials

In $O(\mathsf{M}(n)\log n) = \tilde{O}(n)$ arithmetic operations one can solve:

- Multipoint evaluation and interpolation
- Minimal polynomial of a linearly recurring sequence
- Gcd and Bézout relation
- Rational reconstruction and Padé approximation
- Hankel and Toeplitz linear system
- **Univariate polynomial resultant**

Digression: displacement rank

Padé-Hermite approximant

$H(x)$ a row vector of dimension m of power series in $\mathsf{K}[[x]]$

A polynomial vector $B \in \mathsf{K}[x]^m$ is a Padé-Hermite of order σ and type $(d_1, \ldots, d_m)$ if

- $H(x) \cdot B(x) = 0 \bmod x^\sigma$
- $\sigma = \sum_i (d_i + 1) - 1$
- $\deg B_i \leq d_i$, $1 \leq i \leq m$

[Zhou & Labahn 2012]

Theorem

$k \geq m$, an approximant basis of order d can be computed in $\tilde{O}(k^{\omega} \lceil md/k \rceil)$ arithmetic operations

Theorem

- $m \times 2m$, an approximant basis of order d can be computed in $\tilde{O}(m^\omega d)$ arithmetic operations
- A Padé-Hermite approximant can be computed in $\tilde{O}(m^\omega \sigma)$ arithmetic operations

Theorem

- $m \times 2m$, an approximant basis of order d can be computed in $\tilde{O}(m^\omega d)$ arithmetic operations
- A Padé-Hermite approximant can be computed in $\tilde{O}(m^\omega \sigma)$ arithmetic operations
- To go further:
  with technical difficulties (shifts $+$ overlapping linearization $+$ output linearization)
  $\tilde{O}(m^\omega d)$ with d the average degree in the output

Exercise

Let $\alpha(x) \in \mathsf{K}[[x]]$ be a root of $f(x, y)$ irreducible in $\mathsf{K}[x, y]$, $\deg_x f \leq d$, $\deg_y f \leq n$

Exercise

Let $\alpha(x) \in \mathsf{K}[[x]]$ be a root of $f(x,y)$ irreducible in $\mathsf{K}[x,y]$, $\deg_x f \leq d$, $\deg_y f \leq n$

Let $[g_0\ g_1\ \ \ldots g_n]^\mathsf{T}$ be a Padé-Hermite approximant of type $(d,d,\ldots,d)$:

$$\begin{bmatrix} 1 & \alpha(x) & \alpha^2(x) & \ldots\alpha^n(x) \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_n \end{bmatrix} = 0 \bmod x^\sigma$$

Exercise

Let $\alpha(x) \in \mathsf{K}[[x]]$ be a root of $f(x,y)$ irreducible in $\mathsf{K}[x,y]$, $\deg_x f \leq d$, $\deg_y f \leq n$

Let $[g_0 \; g_1 \; \ldots g_n]^\mathsf{T}$ be a Padé-Hermite approximant of type $(d, d, \ldots, d)$:

$$\begin{bmatrix} 1 & \alpha(x) & \alpha^2(x) & \ldots \alpha^n(x) \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_n \end{bmatrix} = 0 \bmod x^\sigma$$

If $\sigma > 2dn$ then α is a root of $g(x,y) = g_0(x) + y g_1(x) + \ldots + g_n(x) y^n$

Exercise

Let $\alpha(x) \in \mathsf{K}[[x]]$ be a root of $f(x,y)$ irreducible in $\mathsf{K}[x,y]$, $\deg_x f \leq d$, $\deg_y f \leq n$

Let $[g_0\ g_1\ \ldots g_n]^{\mathsf{T}}$ be a Padé-Hermite approximant of type $(d, d, \ldots, d)$:

$$\begin{bmatrix} 1 & \alpha(x) & \alpha^2(x) & \ldots \alpha^n(x) \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_n \end{bmatrix} = 0 \bmod x^\sigma$$

If $\sigma > 2dn$ then α is a root of $g(x,y) = g_0(x) + y g_1(x) + \ldots + g_n(x) y^n$