Algorithmic Guessing

Alin Bostan

Inria informatics mathematics

ENS Lyon

M2, CR06

September 30, 2020

Some organizational announcements

▷ Homework assignment: Exercise in slide 53 of last course

Exercise: For $A \in \mathbb{K}[x]^{m\times 2m}$ of degree d we are given an algorithm `ApproximantBasis(A,δ)` thats returns a minimal approximant basis at order $\delta \geq d$ in time $\tilde{O}(m^\omega \delta)$. For $M \in \mathbb{K}^{n\times n}$, give an algorithm for computing $M, M^2, \ldots, M^n$ in $\tilde{O}(n^3)$ operations in $\mathbb{K}$. You will assume (property of genericity) that for any $A \in \mathbb{K}[x]^{m\times 2m}$ encountered for some m and d during the algorithm, there exists a nullspace basis of degree d; also assume that n is a power of 2.

⟶ deadline: Monday 5 October 2020, 23:59
⟶ solution to be sent by email to the 3 instructors
⟶ either (good quality) scanned handwritten notes, or typed pdf
⟶ grades (and maybe feedback?) returned before the mid-term exam

▷ Mid-term exam:
⟶ date: Wednesday 7 October 2020, 15:45-17:45
⟶ written exam, possibly in the room (except for Austrian students)
⟶ precise instructions next Monday, stay tuned

The exercises from last week

Exercise 1: Prove that L admits at most $r = \mathrm{ord}(L)$ linearly independent solutions (over C). Hint: use Wronskians.

Exercise 2: Estimate the cost of SYM in the case of constant coefficients.

Exercise 3: Assume that the LCLM of A, B in $W_{n,n}$ is computed using the algorithm from last time (closure of D-finite functions with respect to $+$).

- Estimate the size and the degree of the polynomial matrix;
- Deduce a bound on the degrees of LCLM(A, B);
- Estimate the complexity of computing LCLM(A, B) by this method.

One exercise from the last lecture

Exercise 3: Assume that the LCLM of A, B in $W_{n,n}$ is computed using the algorithm from last time (closure of D-finite functions with respect to $+$).

1. Estimate the size and the degree of the polynomial matrix;
2. Deduce a bound on the degrees of $\mathrm{LCLM}(A, B)$;
3. Estimate the complexity of computing $\mathrm{LCLM}(A, B)$ by this method.

Solution, Q1

① Estimate the size and the degree of the polynomial matrix

$A, B \in W_{n,n}, \quad L := \mathrm{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x)\partial^i, \quad B = \sum_{i=0}^{s} b_i(x)\partial^i$

Solution, Q1

1. Estimate the size and the degree of the polynomial matrix

$A, B \in W_{n,n}$, $L :=$LCLM(A, B), $A = \sum_{i=0}^{r} a_i(x)\partial^i$, $B = \sum_{i=0}^{s} b_i(x)\partial^i$

▷ If $a_r(x)f^{(r)}(x) + \cdots + a_0(x)f(x) = 0$, $b_s(x)g^{(s)}(x) + \cdots + b_0(x)g(x) = 0$,

$$f^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f, f', \ldots, f^{(r-1)}\right), \quad g^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(g, g', \ldots, g^{(s-1)}\right),$$

so that $\quad (f+g)^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f, f', \ldots, f^{(r-1)}, g, g', \ldots, g^{(s-1)}\right).$

Solution, Q1

1. Estimate the size and the degree of the polynomial matrix

$A, B \in W_{n,n}$, $L :=\mathrm{LCLM}(A, B)$, $A = \sum_{i=0}^{r} a_i(x)\partial^i$, $B = \sum_{i=0}^{s} b_i(x)\partial^i$

▷ If $a_r(x)f^{(r)}(x) + \cdots + a_0(x)f(x) = 0$, $b_s(x)g^{(s)}(x) + \cdots + b_0(x)g(x) = 0$,

$$f^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f, f', \ldots, f^{(r-1)}\right), \quad g^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(g, g', \ldots, g^{(s-1)}\right),$$

$$\text{so that} \quad (f+g)^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f, f', \ldots, f^{(r-1)}, g, g', \ldots, g^{(s-1)}\right).$$

▷ So L has order R at most $r + s \leq 2(n-1)$, and the (rational function) matrix $M(x)$ used to find it has size $R \times (R+1)$

Solution, Q1

1. Estimate the size and the degree of the polynomial matrix

$A, B \in W_{n,n}$, $L :=\mathrm{LCLM}(A, B)$, $A = \sum_{i=0}^{r} a_i(x)\partial^i$, $B = \sum_{i=0}^{s} b_i(x)\partial^i$

▷ If $a_r(x)f^{(r)}(x) + \cdots + a_0(x)f(x) = 0$, $b_s(x)g^{(s)}(x) + \cdots + b_0(x)g(x) = 0$,

$$f^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f, f', \ldots, f^{(r-1)}\right), \quad g^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(g, g', \ldots, g^{(s-1)}\right),$$

$$\text{so that} \quad (f+g)^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f, f', \ldots, f^{(r-1)}, g, g', \ldots, g^{(s-1)}\right).$$

▷ So L has order R at most $r + s \leq 2(n-1)$, and the (rational function) matrix $M(x)$ used to find it has size $R \times (R+1)$

▷ More precisely, by induction:

$$(f+g)^{(\ell)} = \frac{1}{a_r(x)^\ell} \cdot \sum_{i=0}^{r-1} u_{\ell,i}(x) f^{(i)} + \frac{1}{b_s(x)^\ell} \cdot \sum_{i=0}^{s-1} v_{\ell,i}(x) g^{(i)}, \ \deg(u_{\ell,i}), \deg(v_{\ell,i}) < \ell n$$

1. Estimate the size and the degree of the polynomial matrix

$A, B \in W_{n,n}$, $L :=$LCLM(A, B), $A = \sum_{i=0}^{r} a_i(x)\partial^i$, $B = \sum_{i=0}^{s} b_i(x)\partial^i$

▷ If $a_r(x)f^{(r)}(x) + \cdots + a_0(x)f(x) = 0$, $b_s(x)g^{(s)}(x) + \cdots + b_0(x)g(x) = 0$,

$$f^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f, f', \ldots, f^{(r-1)}\right), \quad g^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(g, g', \ldots, g^{(s-1)}\right),$$

$$\text{so that} \quad (f+g)^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f, f', \ldots, f^{(r-1)}, g, g', \ldots, g^{(s-1)}\right).$$

▷ So L has order R at most $r + s \leq 2(n-1)$, and the (rational function) matrix $M(x)$ used to find it has size $R \times (R+1)$

▷ More precisely, by induction:

$$(f+g)^{(\ell)} = \frac{1}{a_r(x)^\ell} \cdot \sum_{i=0}^{r-1} u_{\ell,i}(x) f^{(i)} + \frac{1}{b_s(x)^\ell} \cdot \sum_{i=0}^{s-1} v_{\ell,i}(x) g^{(i)}, \ \deg(u_{\ell,i}), \deg(v_{\ell,i}) < \ell n$$

▷ So $M(x) = \frac{1}{(a_r(x)b_s(x))^{2n}} \cdot \tilde{M}(x)$, with $\tilde{M}(x)$ of degree $O(n^2)$

Solution, Q2 and Q3

2. Deduce a bound on the degrees of LCLM(A, B);
3. Estimate the complexity of computing LCLM(A, B) by this method.

$A, B \in W_{n,n}, \quad L := \mathrm{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x)\partial^i, \quad B = \sum_{i=0}^{s} b_i(x)\partial^i$

Solution, Q2 and Q3

2. Deduce a bound on the degrees of LCLM(A, B);
3. Estimate the complexity of computing LCLM(A, B) by this method.

$A, B \in W_{n,n}$, $\quad L :=$LCLM(A, B), $\quad A = \sum_{i=0}^{r} a_i(x)\partial^i$, $\quad B = \sum_{i=0}^{s} b_i(x)\partial^i$

▷ L can be found by linear algebra on a matrix $M(x) = \frac{1}{(a_r(x)b_s(x))^{2n}} \cdot \tilde{M}(x)$, with $\tilde{M}(x)$ of degree $O(n^2)$ and size $R \times (R+1)$, with $R < 2n$.

Solution, Q2 and Q3

2. Deduce a bound on the degrees of LCLM(A, B);
3. Estimate the complexity of computing LCLM(A, B) by this method.

$A, B \in W_{n,n}$, $\quad L :=$LCLM(A, B), $\quad A = \sum_{i=0}^{r} a_i(x)\partial^i$, $\quad B = \sum_{i=0}^{s} b_i(x)\partial^i$

▷ L can be found by linear algebra on a matrix $M(x) = \frac{1}{(a_r(x)b_s(x))^{2n}} \cdot \tilde{M}(x)$, with $\tilde{M}(x)$ of degree $O(n^2)$ and size $R \times (R+1)$, with $R < 2n$.

▷ By Cramer's formulas, the kernel of $M(x)$ contains polynomials of degrees $O(n^3)$.

Solution, Q2 and Q3

2. Deduce a bound on the degrees of $\mathrm{LCLM}(A, B)$;
3. Estimate the complexity of computing $\mathrm{LCLM}(A, B)$ by this method.

$$A, B \in W_{n,n}, \quad L := \mathrm{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x)\partial^i, \quad B = \sum_{i=0}^{s} b_i(x)\partial^i$$

▷ L can be found by linear algebra on a matrix $M(x) = \frac{1}{(a_r(x)b_s(x))^{2n}} \cdot \tilde{M}(x)$, with $\tilde{M}(x)$ of degree $O(n^2)$ and size $R \times (R+1)$, with $R < 2n$.

▷ By Cramer's formulas, the kernel of $M(x)$ contains polynomials of degrees $O(n^3)$.

▷ Thus, $\mathrm{ord}(L) < 2n$ and $\deg_x(L) = O(n^3)$.

2. Deduce a bound on the degrees of $\mathrm{LCLM}(A, B)$;
3. Estimate the complexity of computing $\mathrm{LCLM}(A, B)$ by this method.

$$A, B \in W_{n,n}, \quad L := \mathrm{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x)\partial^i, \quad B = \sum_{i=0}^{s} b_i(x)\partial^i$$

▷ L can be found by linear algebra on a matrix $M(x) = \frac{1}{(a_r(x)b_s(x))^{2n}} \cdot \tilde{M}(x)$, with $\tilde{M}(x)$ of degree $O(n^2)$ and size $R \times (R+1)$, with $R < 2n$.

▷ By Cramer's formulas, the kernel of $M(x)$ contains polynomials of degrees $O(n^3)$.

▷ Thus, $\mathrm{ord}(L) < 2n$ and $\deg_x(L) = O(n^3)$.

▷ This kernel (and thus L) can be found using fast polynomial linear algebra in $\tilde{O}(n^{\omega+2})$ arithmetic operations in $\mathbb{K}$.

ALGORITHMIC GUESSING

Guessing: what's the next term of the sequence?

1. $1, \ 1, \ 1, \ 1, \ 1$
2. $1, \ 1, \ 2, \ 3, \ 5$
3. $1, \ 1, \ 2, \ 5, \ 14$
4. $1, \ 2, \ 9, \ 54, \ 378$
5. $1, \ 2, \ 16, \ 192, \ 2816$
6. $1, \ 3, \ 30, \ 420, \ 6930$

Guessing: what's the next term of the sequence?

1. $1, \ 1, \ 1, \ 1, \ 1$ — 1
2. $1, \ 1, \ 2, \ 3, \ 5$
3. $1, \ 1, \ 2, \ 5, \ 14$
4. $1, \ 2, \ 9, \ 54, \ 378$
5. $1, \ 2, \ 16, \ 192, \ 2816$
6. $1, \ 3, \ 30, \ 420, \ 6930$

Guessing: what's the next term of the sequence?

1. 1, 1, 1, 1, 1 — 1
2. 1, 1, 2, 3, 5 — 8
3. 1, 1, 2, 5, 14
4. 1, 2, 9, 54, 378
5. 1, 2, 16, 192, 2816
6. 1, 3, 30, 420, 6930

Guessing: what's the next term of the sequence?

1. $1, \; 1, \; 1, \; 1, \; 1$ $\quad$ 1
2. $1, \; 1, \; 2, \; 3, \; 5$ $\quad$ 8
3. $1, \; 1, \; 2, \; 5, \; 14$ $\quad$ 42
4. $1, \; 2, \; 9, \; 54, \; 378$
5. $1, \; 2, \; 16, \; 192, \; 2816$
6. $1, \; 3, \; 30, \; 420, \; 6930$

Guessing: what's the next term of the sequence?

1. $1, \quad 1, \quad 1, \quad 1, \quad 1$ — 1
2. $1, \quad 1, \quad 2, \quad 3, \quad 5$ — 8
3. $1, \quad 1, \quad 2, \quad 5, \quad 14$ — 42
4. $1, \quad 2, \quad 9, \quad 54, \quad 378$ — 2916
5. $1, \quad 2, \quad 16, \quad 192, \quad 2816$
6. $1, \quad 3, \quad 30, \quad 420, \quad 6930$

Guessing: what's the next term of the sequence?

1. 1, 1, 1, 1, 1 — 1
2. 1, 1, 2, 3, 5 — 8
3. 1, 1, 2, 5, 14 — 42
4. 1, 2, 9, 54, 378 — 2916
5. 1, 2, 16, 192, 2816 — 46592
6. 1, 3, 30, 420, 6930

Guessing: what's the next term of the sequence?

1. 1, 1, 1, 1, 1 — 1
2. 1, 1, 2, 3, 5 — 8
3. 1, 1, 2, 5, 14 — 42
4. 1, 2, 9, 54, 378 — 2916
5. 1, 2, 16, 192, 2816 — 46592
6. 1, 3, 30, 420, 6930 — 126126

Guessing: what's the next term of the sequence?

1. 1, 1, 1, 1, 1 $\qquad 1/(1-t)$
2. 1, 1, 2, 3, 5 $\qquad 1/(1-t-t^2)$
3. 1, 1, 2, 5, 14 $\qquad (1-\sqrt{1-4t})/(2t)$
4. 1, 2, 9, 54, 378 $\qquad 27\,t^2y^2+(1-18\,t)\,y+16\,t=1$
5. 1, 2, 16, 192, 2816 $\qquad 64\,t^2\,y^3+16\,t\,y^2+(1-72\,t)\,y+54\,t=1$
6. 1, 3, 30, 420, 6930 $\qquad \left(27\,t^2-t\right)y''+(54\,t-2)\,y'+6\,y=0$

Guessing: what's the next term of the sequence?

1. $1, \; 1, \; 1, \; 1, \; 1$ — $1/(1-t)$
2. $1, \; 1, \; 2, \; 3, \; 5$ — $1/(1-t-t^2)$
3. $1, \; 1, \; 2, \; 5, \; 14$ — $(1-\sqrt{1-4t})/(2t)$
4. $1, \; 2, \; 9, \; 54, \; 378$ — $27\,t^2y^2 + (1-18\,t)\,y + 16\,t = 1$
5. $1, \; 2, \; 16, \; 192, \; 2816$ — $64\,t^2\,y^3 + 16\,t\,y^2 + (1-72\,t)\,y + 54\,t = 1$
6. $1, \; 3, \; 30, \; 420, \; 6930$ — $(27\,t^2 - t)\,y'' + (54\,t-2)\,y' + 6\,y = 0$

▷ Automated guessing: algorithmic computation of these equations

Guessing: what's the next term of the sequence?

1. $1,\ 1,\ 1,\ 1,\ 1$ — $1/(1-t)$
2. $1,\ 1,\ 2,\ 3,\ 5$ — $1/(1-t-t^2)$
3. $1,\ 1,\ 2,\ 5,\ 14$ — $(1-\sqrt{1-4t})/(2t)$
4. $1,\ 2,\ 9,\ 54,\ 378$ — $27\,t^2y^2 + (1-18\,t)\,y + 16\,t = 1$
5. $1,\ 2,\ 16,\ 192,\ 2816$ — $64\,t^2\,y^3 + 16\,t\,y^2 + (1-72\,t)\,y + 54\,t = 1$
6. $1,\ 3,\ 30,\ 420,\ 6930$ — $(27\,t^2 - t)\,y'' + (54\,t-2)\,y' + 6\,y = 0$

▷ Automated guessing: via Padé, or Hermite-Padé, approximants

PADÉ APPROXIMANTS

—guessing linear recurrences with constant coefficients—

Duality lemma (link between l.r.s.c.c. and rational functions)
Let $A(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{K}[[x]]$ be the generating function of $(a_n)_{n\geq 0}$.
The following assertions are equivalent:

(i) (a_n) is a l.r.s.c.c., having P as characteristic polynomial of degree d.

(ii) $A(x)$ is rational, of the form $A = Q/\mathsf{rev}_d(P)$ for some $Q \in \mathbb{K}[x]_{<d}$, where $\mathsf{rev}_d(P) = P(\frac{1}{x})x^d$.

Recall: duality lemma

Duality lemma (link between l.r.s.c.c. and rational functions)
Let $A(x) = \sum_{n \geq 0} a_n x^n \in \mathbb{K}[[x]]$ be the generating function of $(a_n)_{n \geq 0}$.
The following assertions are equivalent:

(i) (a_n) is a l.r.s.c.c., having P as characteristic polynomial of degree d.

(ii) $A(x)$ is rational, of the form $A = Q/\mathsf{rev}_d(P)$ for some $Q \in \mathbb{K}[x]_{<d}$, where $\mathsf{rev}_d(P) = P(\frac{1}{x})x^d$.

Moreover, if P is the minimal polynomial of $(a_n)_{n \geq 0}$, then

$$d = \max\{1 + \deg(Q), \deg(\mathsf{rev}_d(P))\} \quad \text{and} \quad \gcd(Q, \mathsf{rev}_d(P)) = 1.$$

Duality lemma (link between l.r.s.c.c. and rational functions)
Let $A(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{K}[[x]]$ be the generating function of $(a_n)_{n\geq 0}$.
The following assertions are equivalent:

(i) (a_n) is a l.r.s.c.c., having P as characteristic polynomial of degree d.

(ii) $A(x)$ is rational, of the form $A = Q/\mathsf{rev}_d(P)$ for some $Q \in \mathbb{K}[x]_{<d}$, where $\mathsf{rev}_d(P) = P(\frac{1}{x})x^d$.

Moreover, if P is the minimal polynomial of $(a_n)_{n\geq 0}$, then

$$d = \max\{1 + \deg(Q), \deg(\mathsf{rev}_d(P))\} \quad \text{and} \quad \gcd(Q, \mathsf{rev}_d(P)) = 1.$$

▷ Computing $\mathsf{MinPol}(a_n)$ is equivalent to solving a Padé approximation pb:

$$\frac{R}{V} \equiv A \bmod x^{2N}, \quad x \nmid V, \ \deg(R) < N, \ \deg(V) \leq N \ \text{ and } \ \gcd(R, V) = 1,$$

where $A = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2N-1} x^{2N-1}$.

Recall: Euclidean-type algorithm for Padé approximation

Pade$(A, 2N)$

In: A in $\mathbb{K}[x]$ with $\deg A < 2N$

Out: (R, V) s.t. $R/V \equiv A \bmod x^{2N}$, $\deg R < N, \deg V \leq N$, or FAIL

1. $R_0 := x^{2N}$; $V_0 := 0$; $R_1 := A$; $V_1 := 1$; $i := 1$.
2. While $\deg R_i \geq N$ do:
   1. $(Q_i, R_{i+1}) := \text{QuotRem}(R_{i-1}, R_i)$ $\qquad$ $\#R_{i-1} = Q_i R_i + R_{i+1}$
   2. $V_{i+1} := V_{i-1} - Q_i V_i$
   3. $i := i + 1$.
3. If $V_i(0) \neq 0$ then return (R_i, V_i); else return FAIL.

▷ Quadratic complexity: $O(N^2)$ operations in $\mathbb{K}$

▷ There exist quasi-linear time algorithms $\qquad O(\mathsf{M}(N) \log N)$

In: A bound $N \in \mathbb{N}$ on the degree of the minimal polynomial of $(a_n)_{n\geq 0}$ and the first $2N$ terms $a_0, \ldots, a_{2N-1} \in \mathbb{K}$.

Out: the minimal generating polynomial $(a_n)_{n\geq 0}$.

1. $A = a_0 + a_1 x + \cdots + a_{2N-1} x^{2N-1}$.
2. Compute the solution $(R, V) \in \mathbb{K}[x]^2$ of $\mathsf{Pade}(A, 2N)$ s.t. $V(0) = 1$.
3. $d = \max\{1 + \deg(R), \deg(V)\}$. Return $\mathsf{rev}_d(V) = V(1/x)x^d$.

▷ Quadratic complexity: $O(N^2)$ operations in $\mathbb{K}$

▷ There exist quasi-linear time algorithms $O(\mathsf{M}(N) \log N)$

Berlekamp-Massey algorithm, a variant

In: A bound $N \in \mathbb{N}$ on the degree of the minimal polynomial of $(a_n)_{n\geq 0}$ and the first $2N$ terms $a_0, \dots, a_{2N-1} \in \mathbb{K}$.

Out: the minimal generating polynomial $(a_n)_{n\geq 0}$.

1. $R_0 := x^{2N}$; $V_0 := 0$; $R_1 := a_{2n-1} + \cdots + a_0 x^{2N-1}$; $V_1 := 1$; $i := 1$.
2. While $\deg R_i \geq N$, do:
    1. $(Q_i, R_{i+1}) := \mathrm{QuotRem}(R_{i-1}, R_i)$ $\qquad \# R_{i-1} = Q_i R_i + R_{i+1}$
    2. $V_{i+1} := V_{i-1} - Q_i V_i$
    3. $i := i + 1$
3. Return $V_i / \mathrm{lc}(V_i)$.

▷ Quadratic complexity: $O(N^2)$ operations in $\mathbb{K}$

▷ There exist quasi-linear time algorithms $\qquad O(\mathsf{M}(N) \log N)$

Example

Assume given the terms $1, 1, 2, 3, 7, 13, 25, 48$ and the bound $N = 4$

Example

Assume given the terms $1, 1, 2, 3, 7, 13, 25, 48$ and the bound $N = 4$

▷ The previous algorithm starts with $V_0 = 0$, $V_1 = 1$ and

$$R_0 = x^8, \quad R_1 = x^7 + x^6 + 2\,x^5 + 3\,x^4 + 7\,x^3 + 13\,x^2 + 25\,x + 48$$

Example

Assume given the terms $1, 1, 2, 3, 7, 13, 25, 48$ and the bound $N = 4$

▷ The previous algorithm starts with $V_0 = 0$, $V_1 = 1$ and

$$R_0 = x^8, \quad R_1 = x^7 + x^6 + 2\,x^5 + 3\,x^4 + 7\,x^3 + 13\,x^2 + 25\,x + 48$$

and it computes

Example

Assume given the terms $1, 1, 2, 3, 7, 13, 25, 48$ and the bound $N = 4$

▷ The previous algorithm starts with $V_0 = 0$, $V_1 = 1$ and

$$R_0 = x^8, \quad R_1 = x^7 + x^6 + 2\,x^5 + 3\,x^4 + 7\,x^3 + 13\,x^2 + 25\,x + 48$$

and it computes

$$(Q_1, R_2) := \mathrm{QuotRem}(R_0, R_1) = (x - 1,\ -x^6 - x^5 - 4\,x^4 - 6\,x^3 - 12\,x^2 - 23\,x + 48)$$

$$V_2 := V_0 - Q_1 V_1 = -x + 1 \qquad \longrightarrow \qquad a_{n+1} = a_n$$

Example

Assume given the terms $1, 1, 2, 3, 7, 13, 25, 48$ and the bound $N = 4$

▷ The previous algorithm starts with $V_0 = 0$, $V_1 = 1$ and

$$R_0 = x^8, \quad R_1 = x^7 + x^6 + 2\,x^5 + 3\,x^4 + 7\,x^3 + 13\,x^2 + 25\,x + 48$$

and it computes

$$(Q_1, R_2) := \mathrm{QuotRem}(R_0, R_1) = (x - 1,\ -x^6 - x^5 - 4\,x^4 - 6\,x^3 - 12\,x^2 - 23\,x + 48)$$

$$V_2 := V_0 - Q_1 V_1 = -x + 1 \qquad \longrightarrow \qquad a_{n+1} = a_n$$

$$(Q_2, R_3) := \mathrm{QuotRem}(R_1, R_2) = (-x,\ -2\,x^5 - 3\,x^4 - 5\,x^3 - 10\,x^2 + 73\,x + 48)$$

$$V_3 := V_1 - Q_2 V_2 = -x^2 + x + 1 \qquad \longrightarrow \qquad a_{n+2} = a_{n+1} + a_n$$

Example

Assume given the terms $1, 1, 2, 3, 7, 13, 25, 48$ and the bound $N = 4$

▷ The previous algorithm starts with $V_0 = 0$, $V_1 = 1$ and

$$R_0 = x^8, \quad R_1 = x^7 + x^6 + 2\,x^5 + 3\,x^4 + 7\,x^3 + 13\,x^2 + 25\,x + 48$$

and it computes

$$(Q_1, R_2) := \mathrm{QuotRem}(R_0, R_1) = (x - 1,\ -x^6 - x^5 - 4\,x^4 - 6\,x^3 - 12\,x^2 - 23\,x + 48)$$

$$V_2 := V_0 - Q_1 V_1 = -x + 1 \qquad \longrightarrow \qquad a_{n+1} = a_n$$

$$(Q_2, R_3) := \mathrm{QuotRem}(R_1, R_2) = (-x,\ -2\,x^5 - 3\,x^4 - 5\,x^3 - 10\,x^2 + 73\,x + 48)$$

$$V_3 := V_1 - Q_2 V_2 = -x^2 + x + 1 \qquad \longrightarrow \qquad a_{n+2} = a_{n+1} + a_n$$

$$(Q_3, R_4) := \mathrm{QuotRem}(R_2, R_3) = (\frac{x}{2} - \frac{1}{4},\ -\frac{9x^4}{4} - \frac{9x^3}{4} - 51\,x^2 - \frac{115\,x}{4} + 60)$$

$$V_4 := V_2 - Q_3 V_3 = \frac{x^3}{2} - \frac{3x^2}{4} - \frac{5\,x}{4} + \frac{5}{4} \qquad \longrightarrow \qquad a_{n+3} = \frac{3}{2} a_{n+2} + \frac{5}{2} a_{n+1} - \frac{5}{2} a_n$$

Example

Assume given the terms $1, 1, 2, 3, 7, 13, 25, 48$ and the bound $N = 4$

▷ The previous algorithm starts with $V_0 = 0$, $V_1 = 1$ and

$$R_0 = x^8, \quad R_1 = x^7 + x^6 + 2\,x^5 + 3\,x^4 + 7\,x^3 + 13\,x^2 + 25\,x + 48$$

and it computes

$$(Q_1, R_2) := \mathrm{QuotRem}(R_0, R_1) = (x - 1,\; -x^6 - x^5 - 4\,x^4 - 6\,x^3 - 12\,x^2 - 23\,x + 48)$$

$$V_2 := V_0 - Q_1 V_1 = -x + 1 \qquad \longrightarrow \qquad a_{n+1} = a_n$$

$$(Q_2, R_3) := \mathrm{QuotRem}(R_1, R_2) = (-x,\; -2\,x^5 - 3\,x^4 - 5\,x^3 - 10\,x^2 + 73\,x + 48)$$

$$V_3 := V_1 - Q_2 V_2 = -x^2 + x + 1 \qquad \longrightarrow \qquad a_{n+2} = a_{n+1} + a_n$$

$$(Q_3, R_4) := \mathrm{QuotRem}(R_2, R_3) = (\frac{x}{2} - \frac{1}{4},\; -\frac{9x^4}{4} - \frac{9x^3}{4} - 51\,x^2 - \frac{115\,x}{4} + 60)$$

$$V_4 := V_2 - Q_3 V_3 = \frac{x^3}{2} - \frac{3x^2}{4} - \frac{5\,x}{4} + \frac{5}{4} \qquad \longrightarrow \qquad a_{n+3} = \frac{3}{2} a_{n+2} + \frac{5}{2} a_{n+1} - \frac{5}{2} a_n$$

$$(Q_4, R_5) := \mathrm{QuotRem}(R_3, R_4) = (\frac{8\,x}{9} + \frac{4}{9},\; \frac{124\,x^3}{3} + \frac{344\,x^2}{9} + \frac{292\,x}{9} + \frac{64}{3})$$

$$V_5 := V_3 - Q_4 V_4 = -\frac{4x^4}{9} + \frac{4x^3}{9} + \frac{4x^2}{9} + \frac{4x}{9} + \frac{4}{9} \qquad \longrightarrow \qquad a_{n+4} = a_{n+3} + \cdots + a_n$$

HERMITE-PADÉ APPROXIMANTS

—guessing equations with polynomial coefficients—

Definition

Definition: Given a column vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and an n-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, a Hermite-Padé approximant of type $\mathbf{d}$ for $\mathbf{F}$ is a row vector $\mathbf{P} = (P_1, \ldots, P_n) \in \mathbb{K}[x]^n$, ($\mathbf{P} \neq 0$), such that:

Definition

Definition: Given a column vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and an n-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, a Hermite-Padé approximant of type $\mathbf{d}$ for $\mathbf{F}$ is a row vector $\mathbf{P} = (P_1, \ldots, P_n) \in \mathbb{K}[x]^n$, ($\mathbf{P} \neq 0$), such that:

(1) $\mathbf{P} \cdot \mathbf{F} = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma)$ with $\sigma = \sum_i (d_i + 1) - 1$,

Definition

Definition: Given a column vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and an n-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, a Hermite-Padé approximant of type $\mathbf{d}$ for $\mathbf{F}$ is a row vector $\mathbf{P} = (P_1, \ldots, P_n) \in \mathbb{K}[x]^n$, ($\mathbf{P} \neq 0$), such that:

(1) $\mathbf{P} \cdot \mathbf{F} = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma)$ with $\sigma = \sum_i (d_i + 1) - 1$,

(2) $\deg(P_i) \leq d_i$ for all i.

Definition

Definition: Given a column vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and an n-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, a Hermite-Padé approximant of type $\mathbf{d}$ for $\mathbf{F}$ is a row vector $\mathbf{P} = (P_1, \ldots, P_n) \in \mathbb{K}[x]^n$, ($\mathbf{P} \neq 0$), such that:

(1) $\mathbf{P} \cdot \mathbf{F} = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma)$ with $\sigma = \sum_i (d_i + 1) - 1$,

(2) $\deg(P_i) \leq d_i$ for all i.

σ is called the order of the approximant $\mathbf{P}$.

Definition: Given a column vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and an n-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, a Hermite-Padé approximant of type $\mathbf{d}$ for $\mathbf{F}$ is a row vector $\mathbf{P} = (P_1, \ldots, P_n) \in \mathbb{K}[x]^n$, ($\mathbf{P} \neq 0$), such that:

(1) $\mathbf{P} \cdot \mathbf{F} = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma)$ with $\sigma = \sum_i (d_i + 1) - 1$,

(2) $\deg(P_i) \leq d_i$ for all i.

σ is called the order of the approximant $\mathbf{P}$.

▷ Very useful concept in number theory (irrationality/transcendence):

- [Hermite, 1873]: e is transcendent.
- [Lindemann, 1882]: π is transcendent; so does e^α for any $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$.
- [Apéry, 1978; Beukers, 1981]: $\zeta(3) = \sum_{n \geq 1} \frac{1}{n^3}$ is irrational.
- [Rivoal, 2000]: there exist infinite values of k such that $\zeta(2k+1) \notin \mathbb{Q}$.

Sur la généralisation des fractions continues algébriques;

PAR M. H. PADÉ,

Docteur ès Sciences mathématiques,
Professeur au lycée de Lille.

INTRODUCTION.

M. Hermite s'est, dans un travail récemment paru (1), occupé de la généralisation des fractions continues algébriques. La question est de déterminer les polynomes $X_1, X_2, \ldots, X_n$, de degrés $\mu_1, \mu_2, \ldots, \mu_n$, qui satisfont à l'équation

$$S_1 X_1 + S_2 X_2 + \ldots + S_n X_n = S\, x^{\mu_1+\mu_2+\ldots+\mu_n+n-1},$$

$S_1, S_2, \ldots, S_n$ étant des séries entières données, et S une série également entière. Ou plutôt, il s'agit d'obtenir un algorithme qui permette le calcul de proche en proche de ces systèmes de n polynomes, et qui

Worked example

Let us compute a Hermite-Padé approximant of type $(1,1,1)$ for $(1, C, C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + O(x^5)$.

Worked example

Let us compute a Hermite-Padé approximant of type $(1,1,1)$ for $(1, C, C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + O(x^5)$.
This boils down to finding $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ (not all zero) such that

$$\alpha_0+\alpha_1 x+(\beta_0+\beta_1 x)(1+x+2x^2+5x^3+14x^4)+(\gamma_0+\gamma_1 x)(1+2x+5x^2+14x^3+42x^4)=O(x^5)$$

Worked example

Let us compute a Hermite-Padé approximant of type $(1,1,1)$ for $(1,C,C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + O(x^5)$.
This boils down to finding $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ (not all zero) such that

$$\alpha_0+\alpha_1 x+(\beta_0+\beta_1 x)(1+x+2x^2+5x^3+14x^4)+(\gamma_0+\gamma_1 x)(1+2x+5x^2+14x^3+42x^4)=O(x^5)$$

Identifying coefficients, this is equivalent to a homogeneous linear system:

Worked example

Let us compute a Hermite-Padé approximant of type $(1,1,1)$ for $(1, C, C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + O(x^5)$.
This boils down to finding $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ (not all zero) such that

$$\alpha_0+\alpha_1 x+(\beta_0+\beta_1 x)(1+x+2x^2+5x^3+14x^4)+(\gamma_0+\gamma_1 x)(1+2x+5x^2+14x^3+42x^4)=O(x^5)$$

Identifying coefficients, this is equivalent to a homogeneous linear system:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 5 & 2 \\ 0 & 0 & 5 & 2 & 14 & 5 \\ 0 & 0 & 14 & 5 & 42 & 14 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \\ \gamma_1 \end{bmatrix} = 0 \iff \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 2 & 1 & 5 \\ 0 & 0 & 5 & 2 & 14 \\ 0 & 0 & 14 & 5 & 42 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \end{bmatrix} = -\gamma_1 \begin{bmatrix} 0 \\ 1 \\ 2 \\ 5 \\ 14 \end{bmatrix}.$$

Worked example

Let us compute a Hermite-Padé approximant of type $(1, 1, 1)$ for $(1, C, C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + O(x^5)$.

This boils down to finding $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ (not all zero) such that

$$\alpha_0 + \alpha_1 x + (\beta_0 + \beta_1 x)(1 + x + 2x^2 + 5x^3 + 14x^4) + (\gamma_0 + \gamma_1 x)(1 + 2x + 5x^2 + 14x^3 + 42x^4) = O(x^5)$$

Identifying coefficients, this is equivalent to a homogeneous linear system:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 5 & 2 \\ 0 & 0 & 5 & 2 & 14 & 5 \\ 0 & 0 & 14 & 5 & 42 & 14 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \\ \gamma_1 \end{bmatrix} = 0 \iff \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 2 & 1 & 5 \\ 0 & 0 & 5 & 2 & 14 \\ 0 & 0 & 14 & 5 & 42 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \end{bmatrix} = -\gamma_1 \begin{bmatrix} 0 \\ 1 \\ 2 \\ 5 \\ 14 \end{bmatrix}.$$

By homogeneity, one can choose $\gamma_1 = 1$.

Let us compute a Hermite-Padé approximant of type $(1,1,1)$ for $(1, C, C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + O(x^5)$.
This boils down to finding $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ (not all zero) such that

$$\alpha_0+\alpha_1 x+(\beta_0+\beta_1 x)(1+x+2x^2+5x^3+14x^4)+(\gamma_0+\gamma_1 x)(1+2x+5x^2+14x^3+42x^4)=O(x^5)$$

Identifying coefficients, this is equivalent to a homogeneous linear system:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 5 & 2 \\ 0 & 0 & 5 & 2 & 14 & 5 \\ 0 & 0 & 14 & 5 & 42 & 14 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \\ \gamma_1 \end{bmatrix} = 0 \iff \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 2 & 1 & 5 \\ 0 & 0 & 5 & 2 & 14 \\ 0 & 0 & 14 & 5 & 42 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \end{bmatrix} = -\gamma_1 \begin{bmatrix} 0 \\ 1 \\ 2 \\ 5 \\ 14 \end{bmatrix}.$$

By homogeneity, one can choose $\gamma_1 = 1$.
Then, the violet minor shows that one can take $(\beta_0, \beta_1, \gamma_0) = (-1, 0, 0)$.

Worked example

Let us compute a Hermite-Padé approximant of type $(1,1,1)$ for $(1, C, C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + O(x^5)$.
This boils down to finding $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ (not all zero) such that

$$\alpha_0 + \alpha_1 x + (\beta_0 + \beta_1 x)(1 + x + 2x^2 + 5x^3 + 14x^4) + (\gamma_0 + \gamma_1 x)(1 + 2x + 5x^2 + 14x^3 + 42x^4) = O(x^5)$$

Identifying coefficients, this is equivalent to a homogeneous linear system:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 5 & 2 \\ 0 & 0 & 5 & 2 & 14 & 5 \\ 0 & 0 & 14 & 5 & 42 & 14 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \\ \gamma_1 \end{bmatrix} = 0 \iff \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 2 & 1 & 5 \\ 0 & 0 & 5 & 2 & 14 \\ 0 & 0 & 14 & 5 & 42 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \end{bmatrix} = -\gamma_1 \begin{bmatrix} 0 \\ 1 \\ 2 \\ 5 \\ 14 \end{bmatrix}.$$

By homogeneity, one can choose $\gamma_1 = 1$.
Then, the violet minor shows that one can take $(\beta_0, \beta_1, \gamma_0) = (-1, 0, 0)$.
The other values are $\alpha_0 = 1$, $\alpha_1 = 0$.

Let us compute a Hermite-Padé approximant of type $(1,1,1)$ for $(1,C,C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + O(x^5)$.
This boils down to finding $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ (not all zero) such that

$$\alpha_0 + \alpha_1 x + (\beta_0 + \beta_1 x)(1 + x + 2x^2 + 5x^3 + 14x^4) + (\gamma_0 + \gamma_1 x)(1 + 2x + 5x^2 + 14x^3 + 42x^4) = O(x^5)$$

Identifying coefficients, this is equivalent to a homogeneous linear system:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 5 & 2 \\ 0 & 0 & 5 & 2 & 14 & 5 \\ 0 & 0 & 14 & 5 & 42 & 14 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \\ \gamma_1 \end{bmatrix} = 0 \iff \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 2 & 1 & 5 \\ 0 & 0 & 5 & 2 & 14 \\ 0 & 0 & 14 & 5 & 42 \end{bmatrix} \times \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \gamma_0 \end{bmatrix} = -\gamma_1 \begin{bmatrix} 0 \\ 1 \\ 2 \\ 5 \\ 14 \end{bmatrix}.$$

By homogeneity, one can choose $\gamma_1 = 1$.
Then, the violet minor shows that one can take $(\beta_0, \beta_1, \gamma_0) = (-1, 0, 0)$.
The other values are $\alpha_0 = 1,\ \alpha_1 = 0$.

▷ Thus the approximant is $(1, -1, x)$, which corresponds to $P = 1 - y + xy^2$ such that $P(x, C(x)) = 0 \bmod x^5$.

Algebraic and differential approximation = guessing

- Hermite-Padé approximants of $n = 2$ power series are related to Padé approximants, i.e. to approximation of series by rational functions
- algebraic approximants = Hermite-Padé approximants for $f_\ell = A^{\ell-1}$, where $A \in \mathbb{K}[[x]]$ seriestoalgeq, listtoalgeq
- differential approximants = Hermite-Padé approximants for $f_\ell = A^{(\ell-1)}$, where $A \in \mathbb{K}[[x]]$ seriestodiffeq, listtodiffeq

```
> listtoalgeq([1,1,2,5,14,42,132,429],y(x));
```

$$1 - y(x) + xy(x)^2$$

```
> listtodiffeq([1,1,2,5,14,42,132,429],y(x))[1];
```

$$\left\{-2y(x) + (2-4x)\frac{\mathrm{d}}{\mathrm{d}x}y(x) + x\frac{\mathrm{d}^2}{\mathrm{d}x^2}y(x), y(0) = 1, \mathrm{D}(y)(0) = 1\right\}$$

Existence and naive computation

Theorem For any vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and for any n-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, there exists a Hermite-Padé approx. of type $\mathbf{d}$ for $\mathbf{F}$.

Proof: The undetermined coefficients of $P_i = \sum_{j=0}^{d_i} p_{i,j} x^j$ satisfy a linear homogeneous system with $\sigma = \sum_i (d_i + 1) - 1$ eqs and $\sigma + 1$ unknowns.

Corollary Computation in $O(\sigma^\omega)$, for $2 \leq \omega \leq 3$ (linear algebra exponent)

▷ There are better algorithms (the linear system is structured, Sylvester-like):

- Derksen's algorithm (Euclidean-like) $O(\sigma^2)$
- Beckermann-Labahn algorithm (DAC) $\tilde{O}(\sigma) = O(\sigma \log^2 \sigma)$
- structured linear algebra algorithms for Toeplitz-like matrices $\tilde{O}(\sigma)$

Quasi-optimal computation

Theorem [Beckermann, Labahn, 1994] One can compute a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (f_1, \ldots, f_n)$ in $\tilde{O}(n^\omega d)$ ops. in $\mathbb{K}$.

Ideas:

- Compute a whole matrix of approximants
- Exploit divide-and-conquer

Algorithm:

1. If $\sigma = n(d+1) - 1 \leq$ threshold, call the naive algorithm
2. Else:
    1. recursively compute $\mathbf{P}_1 \in \mathbb{K}[x]^{n \times n}$ s.t. $\mathbf{P}_1 \cdot \mathbf{F} = O(x^{\sigma/2})$, $\deg(\mathbf{P}_1) \approx \frac{d}{2}$
    2. compute "residue" $\mathbf{R}$ such that $\mathbf{P}_1 \cdot \mathbf{F} = x^{\sigma/2} \cdot \big(\mathbf{R} + O(x^{\sigma/2})\big)$
    3. recursively compute $\mathbf{P}_2 \in \mathbb{K}[x]^{n \times n}$ s.t. $\mathbf{P}_2 \cdot \mathbf{R} = O(x^{\sigma/2})$, $\deg(\mathbf{P}_2) \approx \frac{d}{2}$
    4. return $\mathbf{P} := \mathbf{P}_2 \cdot \mathbf{P}_1$

▷ The precise choices of degrees is a delicate issue

▷ Corollary: Gcd, extended gcd, Padé approximants in $\tilde{O}(d)$ ops. in $\mathbb{K}$.

Application: certified algebraic guessing

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most d in x and at most n in y. Let $\mathbf{Q} = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (1, A, \ldots, A^n)$. If $\mathbf{Q} \cdot \mathbf{F} = O(x^{2dn+1})$, then $\mathbf{Q} \cdot \mathbf{F} = 0$.

Application: certified algebraic guessing

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most d in x and at most n in y. Let $\mathbf{Q} = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (1, A, \ldots, A^n)$. If $\mathbf{Q} \cdot \mathbf{F} = O(x^{2dn+1})$, then $\mathbf{Q} \cdot \mathbf{F} = 0$.

In other words, A is a root of the polynomial $Q = \sum_{i=0}^{n} Q_i(x) y^i$.

Application: certified algebraic guessing

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most d in x and at most n in y. Let $\mathbf{Q} = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (1, A, \ldots, A^n)$. If $\mathbf{Q} \cdot \mathbf{F} = O(x^{2dn+1})$, then $\mathbf{Q} \cdot \mathbf{F} = 0$.

In other words, A is a root of the polynomial $Q = \sum_{i=0}^{n} Q_i(x) y^i$.

Remark: If $n = 1$, this simply says that if $A \in \mathbb{K}(x)_{\leq d}$ and if $Q_0(x) + Q_1(x)A = O(x^{2d+1})$ with $\deg(Q_i) \leq d$, then $Q_0(x) + Q_1(x)A = 0$.

Indeed, if $A = P_0/P_1$ with $\deg(P_i) \leq d$, then $Q_0P_1 + Q_1P_0 = O(x^{2d+1})$ and $\deg(Q_0P_1 + Q_1P_0) \leq 2d$ implies $Q_0P_1 + Q_1P_0 = 0$.

Application: certified algebraic guessing

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most d in x and at most n in y. Let $\mathbf{Q} = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (1, A, \ldots, A^n)$. If $\mathbf{Q} \cdot \mathbf{F} = O(x^{2dn+1})$, then $\mathbf{Q} \cdot \mathbf{F} = 0$.

In other words, A is a root of the polynomial $Q = \sum_{i=0}^{n} Q_i(x) y^i$.

Proof:

Application: certified algebraic guessing

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most d in x and at most n in y. Let $\mathbf{Q} = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (1, A, \ldots, A^n)$. If $\mathbf{Q} \cdot \mathbf{F} = O(x^{2dn+1})$, then $\mathbf{Q} \cdot \mathbf{F} = 0$.

In other words, A is a root of the polynomial $Q = \sum_{i=0}^{n} Q_i(x) y^i$.

Proof: Let $P \in \mathbb{K}[x,y]$ be an irreducible polynomial such that

$$P(x, A(x)) = 0, \text{ and } \deg_x(P) \leq d, \ \deg_y(P) \leq n.$$

Application: certified algebraic guessing

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x, y]$ of degree at most d in x and at most n in y. Let $\mathbf{Q} = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (1, A, \ldots, A^n)$. If $\mathbf{Q} \cdot \mathbf{F} = O(x^{2dn+1})$, then $\mathbf{Q} \cdot \mathbf{F} = 0$.

In other words, A is a root of the polynomial $Q = \sum_{i=0}^{n} Q_i(x) y^i$.

Proof: Let $P \in \mathbb{K}[x, y]$ be an irreducible polynomial such that

$$P(x, A(x)) = 0, \text{ and } \deg_x(P) \leq d, \ \deg_y(P) \leq n.$$

- $R(x) = \mathrm{Res}_y(P, Q) \in \mathbb{K}[x]$ has degree at most $2dn$.

Application: certified algebraic guessing

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most d in x and at most n in y. Let $\mathbf{Q} = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (1, A, \ldots, A^n)$. If $\mathbf{Q} \cdot \mathbf{F} = O(x^{2dn+1})$, then $\mathbf{Q} \cdot \mathbf{F} = 0$.

In other words, A is a root of the polynomial $Q = \sum_{i=0}^{n} Q_i(x) y^i$.

Proof: Let $P \in \mathbb{K}[x,y]$ be an irreducible polynomial such that

$$P(x, A(x)) = 0, \text{ and } \deg_x(P) \leq d, \ \deg_y(P) \leq n.$$

- $R(x) = \mathsf{Res}_y(P, Q) \in \mathbb{K}[x]$ has degree at most $2dn$.
- $R(x) = UP + VQ$ for $U, V \in \mathbb{K}[x,y]$ with $\deg_y(V) < n$.

Application: certified algebraic guessing

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most d in x and at most n in y. Let $\mathbf{Q} = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (1, A, \ldots, A^n)$. If $\mathbf{Q} \cdot \mathbf{F} = O(x^{2dn+1})$, then $\mathbf{Q} \cdot \mathbf{F} = 0$.

In other words, A is a root of the polynomial $Q = \sum_{i=0}^{n} Q_i(x) y^i$.

Proof: Let $P \in \mathbb{K}[x,y]$ be an irreducible polynomial such that

$$P(x, A(x)) = 0, \text{ and } \deg_x(P) \leq d, \deg_y(P) \leq n.$$

- $R(x) = \mathrm{Res}_y(P, Q) \in \mathbb{K}[x]$ has degree at most $2dn$.
- $R(x) = UP + VQ$ for $U, V \in \mathbb{K}[x,y]$ with $\deg_y(V) < n$.
- Evaluation at $y = A(x)$ yields

$$R(x) = U(x, A(x)) \underbrace{P(x, A(x))}_{0} + V(x, A(x)) \underbrace{Q(x, A(x))}_{O(x^{2dn+1})} = O(x^{2dn+1}).$$

Application: certified algebraic guessing

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most d in x and at most n in y. Let $\mathbf{Q} = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (1, A, \ldots, A^n)$. If $\mathbf{Q} \cdot \mathbf{F} = O(x^{2dn+1})$, then $\mathbf{Q} \cdot \mathbf{F} = 0$.

In other words, A is a root of the polynomial $Q = \sum_{i=0}^{n} Q_i(x) y^i$.

Proof: Let $P \in \mathbb{K}[x,y]$ be an irreducible polynomial such that

$$P(x, A(x)) = 0, \text{ and } \deg_x(P) \leq d, \ \deg_y(P) \leq n.$$

- $R(x) = \mathrm{Res}_y(P, Q) \in \mathbb{K}[x]$ has degree at most $2dn$.
- $R(x) = UP + VQ$ for $U, V \in \mathbb{K}[x,y]$ with $\deg_y(V) < n$.
- Evaluation at $y = A(x)$ yields

$$R(x) = U(x, A(x)) \underbrace{P(x, A(x))}_{0} + V(x, A(x)) \underbrace{Q(x, A(x))}_{O(x^{2dn+1})} = O(x^{2dn+1}).$$

- Thus $R = 0$, that is $\gcd(P, Q) \neq 1$, and thus $P \mid Q$, and A is a root of Q.

Application: algebraicity of a hypergeometric series

Show that the following series is algebraic:

$$f(t) = \sum_{n \geq 0} \binom{5n}{n} t^n$$

Application: algebraicity of a hypergeometric series

Show that the following series is algebraic:

$$f(t) = \sum_{n \geq 0} \binom{5n}{n} t^n$$

Strategy: First guess a polynomial $P(t, y)$ in $\mathbb{Q}[t, y]$, s.t. $P(t, f(t)) = 0 \bmod t^?$, then prove that P admits the power series $f(t)$ as a root, i.e., $P(t, f(t)) = 0$.

Application: algebraicity of a hypergeometric series

Show that the following series is algebraic:

$$f(t) = \sum_{n\geq 0} \binom{5n}{n} t^n$$

Strategy: First guess a polynomial $P(t, y)$ in $\mathbb{Q}[t, y]$, s.t. $P(t, f(t)) = 0 \bmod t^?$, then prove that P admits the power series $f(t)$ as a root, i.e., $P(t, f(t)) = 0$.

1. Find P s.t. $P(t, f(t)) = 0 \bmod t^{20}$ by Hermite-Padé approximation.

Application: algebraicity of a hypergeometric series

Show that the following series is algebraic:

$$f(t) = \sum_{n \geq 0} \binom{5n}{n} t^n$$

Strategy: First guess a polynomial $P(t, y)$ in $\mathbb{Q}[t, y]$, s.t. $P(t, f(t)) = 0 \bmod t^?$, then prove that P admits the power series $f(t)$ as a root, i.e., $P(t, f(t)) = 0$.

1. Find P s.t. $P(t, f(t)) = 0 \bmod t^{20}$ by Hermite-Padé approximation.
2. Show that there exists a unique root $r(t) \in \mathbb{Q}[[t]]$ of P such that $r(0) = 1$.

Application: algebraicity of a hypergeometric series

Show that the following series is algebraic:

$$f(t) = \sum_{n \geq 0} \binom{5n}{n} t^n$$

Strategy: First guess a polynomial $P(t, y)$ in $\mathbb{Q}[t, y]$, s.t. $P(t, f(t)) = 0 \bmod t^?$, then prove that P admits the power series $f(t)$ as a root, i.e., $P(t, f(t)) = 0$.

1. Find P s.t. $P(t, f(t)) = 0 \bmod t^{20}$ by Hermite-Padé approximation.
2. Show that there exists a unique root $r(t) \in \mathbb{Q}[[t]]$ of P such that $r(0) = 1$.
3. $r(t) = \sum_{n=0}^{\infty} r_n t^n$ being algebraic, it is D-finite, and so (r_n) is P-recursive.

Application: algebraicity of a hypergeometric series

Show that the following series is algebraic:

$$f(t) = \sum_{n \geq 0} \binom{5n}{n} t^n$$

Strategy: First guess a polynomial $P(t, y)$ in $\mathbb{Q}[t, y]$, s.t. $P(t, f(t)) = 0 \bmod t^?$, then prove that P admits the power series $f(t)$ as a root, i.e., $P(t, f(t)) = 0$.

1. Find P s.t. $P(t, f(t)) = 0 \bmod t^{20}$ by Hermite-Padé approximation.
2. Show that there exists a unique root $r(t) \in \mathbb{Q}[[t]]$ of P such that $r(0) = 1$.
3. $r(t) = \sum_{n=0}^{\infty} r_n t^n$ being algebraic, it is D-finite, and so (r_n) is P-recursive.
4. Deduce that $(r_n)_n$ and $(f_n)_n$ with $f_n = \binom{5n}{n}$ satisfy the same recurrence of order 1 and the same initial condition $r_0 = f_0 = 1$.

Application: algebraicity of a hypergeometric series

Show that the following series is algebraic:

$$f(t) = \sum_{n \geq 0} \binom{5n}{n} t^n$$

Strategy: First guess a polynomial $P(t,y)$ in $\mathbb{Q}[t,y]$, s.t. $P(t, f(t)) = 0 \bmod t^?$, then prove that P admits the power series $f(t)$ as a root, i.e., $P(t, f(t)) = 0$.

1. Find P s.t. $P(t, f(t)) = 0 \bmod t^{20}$ by Hermite-Padé approximation.
2. Show that there exists a unique root $r(t) \in \mathbb{Q}[[t]]$ of P such that $r(0) = 1$.
3. $r(t) = \sum_{n=0}^{\infty} r_n t^n$ being algebraic, it is D-finite, and so (r_n) is P-recursive.
4. Deduce that $(r_n)_n$ and $(f_n)_n$ with $f_n = \binom{5n}{n}$ satisfy the same recurrence of order 1 and the same initial condition $r_0 = f_0 = 1$.
5. Conclude that $f_n = r_n$ for all n, thus $f(t) = r(t)$ is algebraic.

Application: algebraicity of a hypergeometric series

```
> f5:=sum(binomial(5*n,n)*t^n, n=0..infinity):
> simplify(f5) assuming t>0 and t<1/100;
```

$$ {}_4F_3\left(\left[\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5}\right];\left[\frac{1}{4},\frac{1}{2},\frac{3}{4}\right];\frac{3125\,t}{256}\right) $$

Application: algebraicity of a hypergeometric series

```
> f5:=sum(binomial(5*n,n)*t^n, n=0..infinity):
> simplify(f5) assuming t>0 and t<1/100;
```

$$ {}_4F_3\left(\left[\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5}\right];\left[\frac{1}{4},\frac{1}{2},\frac{3}{4}\right];\frac{3125\,t}{256}\right) $$

```
> P5:=subs(y(t) = y, seriestoalgeq(series(f5,t,20), y(t))[1]);
```

$$ 1+15\,y+80\,y^2+160\,y^3+(3125\,t-256)\,y^5 $$

```
> f5:=sum(binomial(5*n,n)*t^n, n=0..infinity):
> simplify(f5) assuming t>0 and t<1/100;
```

$$ {}_4F_3\left(\left[\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5}\right];\left[\frac{1}{4},\frac{1}{2},\frac{3}{4}\right];\frac{3125\,t}{256}\right) $$

```
> P5:=subs(y(t) = y, seriestoalgeq(series(f5,t,20), y(t))[1]);
```

$$ 1+15\,y+80\,y^2+160\,y^3+(3125\,t-256)\,y^5 $$

```
> subs({t=0, y=1}, P5), subs({t=0, y=1}, diff(P5,y));
```

$$ 0, \quad -625 $$

Application: algebraicity of a hypergeometric series

```
> deq5:=algeqtodiffeq(P5, y(t))[1];
```

$$120\,y(t) + (15000\,t - 24)\,\frac{\mathrm{d}}{\mathrm{d}t}y(t) + \left(45000\,t^2 - 816\,t\right)\frac{\mathrm{d}^2}{\mathrm{d}t^2}y(t) + \left(25000\,t^3 - 1152\,t^2\right)\frac{\mathrm{d}^3}{\mathrm{d}t^3}y(t) + \left(3125\,t^4 - 256\,t^3\right)\frac{\mathrm{d}^4}{\mathrm{d}t^4}y(t) = 0$$

Application: algebraicity of a hypergeometric series

```
> deq5:=algeqtodiffeq(P5, y(t))[1];
```

$$120\,y(t) + (15000\,t - 24)\frac{d}{dt}y(t) + \left(45000\,t^2 - 816\,t\right)\frac{d^2}{dt^2}y(t) + \left(25000\,t^3 - 1152\,t^2\right)\frac{d^3}{dt^3}y(t) + \left(3125\,t^4 - 256\,t^3\right)\frac{d^4}{dt^4}y(t) = 0$$

```
> rec5:=map(factor, diffeqtorec(deq5, y(t), r(n)));
```

$$5\,(5\,n+1)(5\,n+2)(5\,n+3)(5\,n+4)\,r(n) - 8\,(4\,n+1)(2\,n+1)(4\,n+3)(n+1)\,r(n+1) = 0$$

Application: algebraicity of a hypergeometric series

```
> deq5:=algeqtodiffeq(P5, y(t))[1];
```

$$120\,y(t)+(15000\,t-24)\,\frac{d}{dt}y(t)+\left(45000\,t^2-816\,t\right)\frac{d^2}{dt^2}y(t)+$$
$$\left(25000\,t^3-1152\,t^2\right)\frac{d^3}{dt^3}y(t)+\left(3125\,t^4-256\,t^3\right)\frac{d^4}{dt^4}y(t)=0$$

```
> rec5:=map(factor, diffeqtorec(deq5, y(t), r(n)));
```

$$5\,(5\,n+1)\,(5\,n+2)\,(5\,n+3)\,(5\,n+4)\,r(n)-$$
$$8\,(4\,n+1)\,(2\,n+1)\,(4\,n+3)\,(n+1)\,r(n+1)=0$$

```
> f:=n -> binomial(5*n,n):
> simplify(convert(subs({r(n)=f(n), r(n+1)=f(n+1)}, rec5), GAMMA));
```

$$0$$

Let $(a_n)_{n\geq 0}$ be a sequence with $a_0 = a_1 = 1$ satisfying the recurrence

$$(n+3)a_{n+1} = (2n+3)a_n + 3na_{n-1}, \quad \text{for all } \ n > 0.$$

Show that a_n is an integer for all n.

Homework: an exercise for 7/10/2020

Let $(a_n)_{n\geq 0}$ be a sequence with $a_0 = a_1 = 1$ satisfying the recurrence

$$(n+3)a_{n+1} = (2n+3)a_n + 3na_{n-1}, \quad \text{for all } \ n > 0.$$

Show that a_n is an integer for all n.

Follow the next steps:

1. Compute the first 5 terms of the sequence, $a_0, \dots, a_4$;
2. Determine a Hermite-Padé approximant of type $(0,1,2)$ for $(1, f, f^2)$, where $f = \sum_n a_n x^n$;
3. Deduce that $P(x, f(x)) = 0 \bmod x^5$ for $P(x,y) := 1 + (x-1)y + x^2y^2$;
4. Show that the equation $P(x,y) = 0$ admits a root $y = g(x) \in \mathbb{Q}[[x]]$ whose coefficients satisfy the same linear recurrence as $(a_n)_{n\geq 0}$;
5. Deduce that $a_{n+2} = a_{n+1} + \sum_{k=0}^{n} a_k \cdot a_{n-k}$ for all n, and conclude.

FAST SKEW MULTIPLICATION

- Naive expansion by Leibniz's formula and expansion of $\partial^j x^u$:

$$BA = \sum_{i,j,u,v=0}^{n} b_{i,j} a_{u,v} x^i \underbrace{\left(\partial^j x^u\right)}_{\leq n \text{ terms}} \partial^v \quad \to O\left(n^5\right)$$

- Iterative scheme by derivations of the right-hand factor:

$$BA = \sum_{i=0}^{n} b_i(x) \underbrace{\left(\partial^i A\right)}_{\substack{\text{degree } \leq 2n \text{ in } \partial \\ \text{degree } \leq n \text{ in } x}} \quad \text{by } \partial T = T\partial + \frac{dT}{dx} \quad \to O\left(\mathsf{M}(n)\, n^2\right)$$

- Takayama's iterative scheme by derivations of both factors:

$$BA = \sum_{k=0}^{n} \frac{1}{k!} \underbrace{\left[\frac{d^k B}{d\partial^k} \frac{d^k A}{dx^k}\right]}_{\substack{\text{bivariate commutative product} \\ \text{in bidegree } (n,n)}} \quad \to O\left(\mathsf{M}(n^2)\, n\right)$$

Review of complexity results (unbalanced case)

Product of operators in $W_{r,d} = \mathbb{K}[x]\langle\partial\rangle_{d,r}$

- Naive: $O(d^2r^2 \min(d,r))$ ops
- Iterative: $O(\min(d,r)^2 \, \mathsf{M}(\max(d,r)))$ ops
- Takayama: $O(\min(d,r) \, \mathsf{M}(dr))$ ops

Upcoming:

- [van der Hoeven, 2002]: $O(\max(d,r)^2 \, \min(d,r)^{\omega-2})$ ops
- [Benoit, B., van der Hoeven, 2012]: $\tilde{O}(dr \, \min(d,r)^{\omega-2})$ ops

▷ ω is a feasible exponent for matrix multiplication ($2 \leq \omega \leq 3$)
▷ $\tilde{O}$ indicates that polylogarithmic factors are neglected.
▷ The last two algorithms use an evaluation-interpolation strategy.

$A(x,\theta)$ and $B(x,\theta)$ of bidegree (n,n) $\quad \to \quad C = BA = \sum_{i=0}^{2n} x^i C_i(\theta)$, $\deg C_i \leq 2n$.

$$\theta^j(x^k) = k^j x^k \;\to\; C(x^k) = \sum_{i=0}^{2n} C_i(k)\, x^{i+k}.$$

By Lagrange interpolation: $\big(C_i(k)\big)_{0\leq i,k\leq 2n} \to \big(C_i(\theta)\big)_{0\leq i\leq 2n}$.

$$K[x]_{\leq 2n} \xrightarrow{A\cdot} K[x]_{\leq 3n} \xrightarrow{B\cdot} K[x]_{\leq 4n}.$$

Matrix of size $(4n+1)\times(3n+1)$ for B, $(3n+1)\times(2n+1)$ for A.

Complexity: $\mathsf{SkewM}(n,n) \subset O\big(\mathsf{MM}(n)\big) = O(n^\omega)$

- Composition: product of the matrices of differential operators.
- Evaluation/interpolation: Vandermonde matrix and inverse.
- Conversion $\partial \leftrightarrow \theta$: matrix of Stirling numbers and inverse.

Improvements [B., Chyzak, Le Roux, 2008]

A1. Fast multipoint evaluation/interpolation in $O\big(n\,\mathsf{M}(n)\log n\big)$.

A2. Fast conversions between monomial and falling-factorial bases [Gerhard, 2000] in $O\big(n\,\mathsf{M}(n)\log n\big)$.

$\longrightarrow O\big(\mathsf{MM}(n)\big)$ with the better constants given in the table.

B1. Smaller matrices are sufficient: when B, A of bidegree (n,n) in (x,∂),

$$K[x]_{\leq 2n} \xrightarrow{A\cdot} K[x]_{\leq 3n} \xrightarrow{B\cdot} K[x]_{\leq 2n}.$$

Size $(2n+1)\times(3n+1)$ for B, $(3n+1)\times(2n+1)$ for A.

B2. Direct calculation with ∂.

Improvements [B., Chyzak, Le Roux, 2008]

- A new, direct algorithm for $\mathbb{K}[x]\langle\partial\rangle$, with better constant c.

Algorithm	VdH_θ	IVdH_θ	VdH_∂	IVdH_∂	$\mathsf{MulWeyl}$
All block products	37	24	96	48	12
Zeros + Strassen	20	8	47	12	8

Number c of $n \times n$ block products for multiplication of skew polynomials in (x, θ), resp. (x, ∂), of bidegree (n, n).

- Equivalence $\mathsf{SkewM}(n, n) \propto \mathsf{MM}(n)$
  [Van der Hoeven, 2002]: $\mathsf{SkewM}(n, n) \subset O(\mathsf{MM}(n))$

  [B., Chyzak, Le Roux, 2008]: $O(\mathsf{SkewM}(n, n)) \supset \mathsf{MM}(n)$

  1. $\mathsf{MM}(n) \subset \mathsf{LTMM}(O(n))$: $\begin{bmatrix} I_n & 0 & 0 \\ M & I_n & 0 \\ 0 & N & I_n \end{bmatrix}^2 = \begin{bmatrix} I_n & 0 & 0 \\ 2M & I_n & 0 \\ NM & 2N & I_n \end{bmatrix}$.
  2. $\mathsf{LTMM}(n) \subset O(\mathsf{SkewM}(n))$:

$$\begin{bmatrix} m_{0,0} & & 0 & & 0 \\ \vdots & \ddots & & \ddots & \\ m_{i,0} & & m_{i,i} & & 0 \\ \vdots & \ddots & & \ddots & \\ m_{n,0} & \cdots & m_{n,n-i} & \cdots & m_{n,n} \end{bmatrix} \xleftrightarrow[O(n\,\mathsf{M}(n)\log n)]{m_{i,j}=A_{i-j}(j)} \underbrace{\sum_{\ell=0}^{n} x^\ell A_\ell(\theta)}_{\text{bidegree } (n,n)}.$$

Using Euler's operator $\theta = x\partial$:

- $\theta x^p = x^p\theta + x\left(px^{p-1}\right) = x^p\theta$,
- $x^v f(\theta) = f(\theta - v)\, x^v$ in complexity $O\big(\mathsf{M}(\deg f)\big)$.

$$\left(\sum_{u=0}^{p-1} x^u B_u(x^p,\theta)\right)\left(\sum_{v=0}^{p-1} A_v(x^p,\theta)x^v\right) = \sum_{u,v=0}^{p-1} x^u \underbrace{\Big[(B_u A_v)(x^p,\theta)\Big]}_{\substack{\text{commutative bivariate}\\ \text{product in bidegree } (n/p,\,n)}} x^v.$$

$$\left.\begin{array}{l} \text{Products } O\big(p^2\,\mathsf{M}(n^2/p)\big) \subset O\big(p\,\mathsf{M}(n^2)\big) \\ \text{Conversions } x \leftrightarrow x^p\text{: } O\big(pn\,\mathsf{M}(n)\log n\big) \\ \text{Conversions } \partial \leftrightarrow \theta\text{: } O\big(n\,\mathsf{M}(n)\log n\big) \end{array}\right\} \to \tilde{O}(pn^2).$$

The case of unbalanced products [Benoit, B., van der Hoeven, 2012]

Theorem [Benoit, B., Hoeven, 2012] Product in $W_{r,d} = \mathbb{K}[x]\langle\partial\rangle_{d,r}$ with cost

$$\tilde{O}(dr \min(d,r)^{\omega-2}).$$

The case of unbalanced products [Benoit, B., van der Hoeven, 2012]

Theorem [Benoit, B., Hoeven, 2012] Product in $W_{r,d} = \mathbb{K}[x]\langle\partial\rangle_{d,r}$ with cost

$$\tilde{O}(dr \min(d,r)^{\omega-2}).$$

▹ In the important case $d = r^2$, this complexity reads $\tilde{O}(r^{\omega+1})$
▹ Improves: $O(r^7)$ [naive]; $\tilde{O}(r^{\omega+2})$ [Hoeven'02]; $\tilde{O}(r^4)$ [iter + Takayama]

Theorem [Benoit, B., Hoeven, 2012] Product in $W_{r,d} = \mathbb{K}[x]\langle\partial\rangle_{d,r}$ with cost

$$\tilde{O}(dr \min(d,r)^{\omega-2}).$$

▷ In the important case $d = r^2$, this complexity reads $\tilde{O}(r^{\omega+1})$
▷ Improves: $O(r^7)$ [naive]; $\tilde{O}(r^{\omega+2})$ [Hoeven'02]; $\tilde{O}(r^4)$ [iter + Takayama]

▷ Main ideas

- Use evaluation-interpolation on exponential polynomials $x^i \exp(\alpha x)$
- Replace (fast) Lagrange interpolation by (fast) Hermite interpolation
- Use $(x, \partial) \xleftrightarrow{\text{reflection}} (\partial, -x)$ to reduce to the case $r \geqslant d$

The case of unbalanced products [Benoit, B., van der Hoeven, 2012]

Theorem [Benoit, B., Hoeven, 2012] Product in $W_{r,d} = \mathbb{K}[x]\langle\partial\rangle_{d,r}$ with cost

$$\tilde{O}(dr\min(d,r)^{\omega-2}).$$

▷ In the important case $d = r^2$, this complexity reads $\tilde{O}(r^{\omega+1})$
▷ Improves: $O(r^7)$ [naive]; $\tilde{O}(r^{\omega+2})$ [Hoeven'02]; $\tilde{O}(r^4)$ [iter + Takayama]

▷ Main ideas

- Use evaluation-interpolation on exponential polynomials $x^i \exp(\alpha x)$
- Replace (fast) Lagrange interpolation by (fast) Hermite interpolation
- Use $(x, \partial) \xleftrightarrow{\text{reflection}} (\partial, -x)$ to reduce to the case $r \geqslant d$

▷ Combined with DAC in [Hoeven'16] yields alternative probabilistic (Monte Carlo) algorithms in $\tilde{O}(r^{\omega+1})$ for LCLM, GCRD in $W_{r,r}$