Algorithmic Guessing

Alin Bostan

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 $\text{ApproximantBasis}(A, \delta)$ that 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 $r = \text{ord}(L)$ 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 $\text{LCLM}(A, B)$;
- Estimate the complexity of computing $\text{LCLM}(A, B)$ by this method.
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 LCLM($A, B$);
3. Estimate the complexity of computing LCLM($A, B$) by this method.
Estimate the size and the degree of the polynomial matrix

\[ A, B \in W_{n,n}, \quad L := \text{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x) \partial^i, \quad B = \sum_{i=0}^{s} b_i(x) \partial^i \]
Estimate the size and the degree of the polynomial matrix
\[ A, B \in \mathcal{W}_{n,n}, \quad L := \text{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x) \partial^i, \quad B = \sum_{i=0}^{s} b_i(x) \partial^i \]

\[ \text{If} \quad a_r(x)f^{(r)}(x) + \cdots + a_0(x)f(x) = 0, \quad b_s(x)g^{(s)}(x) + \cdots + b_0(x)g(x) = 0, \]

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

so that \( (f + g)^{(\ell)} \in \text{Vect}_{\mathbb{K}(x)} \left( f, f', \ldots, f^{(r-1)}, g, g', \ldots, g^{(s-1)} \right). \]
1. Estimate the size and the degree of the polynomial matrix
\[ A, B \in \mathcal{W}_{n,n}, \quad L := \text{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x) \partial^i, \quad B = \sum_{i=0}^{s} b_i(x) \partial^i \]

If \( a_r(x)f^{(r)}(x) + \cdots + a_0(x)f(x) = 0, \quad b_s(x)g^{(s)}(x) + \cdots + b_0(x)g(x) = 0, \)
\[ f^{(\ell)} \in \text{Vect}_{\mathbb{K}(x)} \left( f, f', \ldots, f^{(r-1)} \right), \quad g^{(\ell)} \in \text{Vect}_{\mathbb{K}(x)} \left( g, g', \ldots, g^{(s-1)} \right), \]
so that \( (f + g)^{\ell} \in \text{Vect}_{\mathbb{K}(x)} \left( f, f', \ldots, f^{(r-1)}, g, g', \ldots, g^{(s-1)} \right) \).

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 \( R \times (R + 1) \).
Estimate the size and the degree of the polynomial matrix

\[ A, B \in \mathcal{W}_{n,n}, \quad L := \text{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x) \partial^i, \quad B = \sum_{i=0}^{s} b_i(x) \partial^i \]

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

\[ f^{(\ell)} \in \text{Vect}_K(x) \left( f, f', \ldots, f^{(r-1)} \right), \quad g^{(\ell)} \in \text{Vect}_K(x) \left( g, g', \ldots, g^{(s-1)} \right), \]

so that \( (f + g)^{(\ell)} \in \text{Vect}_K(x) \left( f, f', \ldots, f^{(r-1)}, g, g', \ldots, g^{(s-1)} \right). \)

▶ 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:

\[ (f + g)^{(\ell)} = \frac{1}{a_r(x)\ell} \cdot \sum_{i=0}^{r-1} u_{\ell,i}(x)f^{(i)} + \frac{1}{b_s(x)\ell} \cdot \sum_{i=0}^{s-1} v_{\ell,i}(x)g^{(i)}, \quad \deg(u_{\ell,i}), \deg(v_{\ell,i}) < \ell n \]
Estimate the size and the degree of the polynomial matrix

\[ A, B \in \mathcal{W}_{n,n}, \quad L := \text{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x) \partial^i, \quad B = \sum_{i=0}^{s} b_i(x) \partial^i \]

\[ \text{If } a_r(x)f^{(r)}(x) + \cdots + a_0(x)f(x) = 0, \quad b_s(x)g^{(s)}(x) + \cdots + b_0(x)g(x) = 0, \]

\[ f^{(\ell)} \in \text{Vect}_{K(x)}(f, f', \ldots, f^{(r-1)}), \quad g^{(\ell)} \in \text{Vect}_{K(x)}(g, g', \ldots, g^{(s-1)}), \]

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

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

\[ \text{More precisely, by induction:} \]

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

\[ \text{So } M(x) = \frac{1}{(a_r(x)b_s(x))^{2n}} \cdot \tilde{M}(x), \text{ with } \tilde{M}(x) \text{ of degree } O(n^2) \]
Deduce a bound on the degrees of LCLM(A, B);

Estimate the complexity of computing LCLM(A, B) by this method.

\[ A, B \in W_{n,n}, \quad L \equiv \text{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x) \partial^i, \quad B = \sum_{i=0}^{s} b_i(x) \partial^i \]
2. Deduce a bound on the degrees of $\text{LCLM}(A, B)$;
3. Estimate the complexity of computing $\text{LCLM}(A, B)$ by this method.

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

$L$ 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 $R < 2n$. 
Deduce a bound on the degrees of \( \text{LCLM}(A, B) \);

Estimate the complexity of computing \( \text{LCLM}(A, B) \) by this method.

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

\( L \) 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 \( R < 2n \).

\( L \) 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 \( O(n^3) \).
2. Deduce a bound on the degrees of $\text{LCLM}(A, B)$;

3. Estimate the complexity of computing $\text{LCLM}(A, B)$ by this method.

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

$L$ 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, $\text{ord}(L) < 2n$ and $\text{deg}_x(L) = O(n^3)$. 
Deduce a bound on the degrees of $\text{LCLM}(A, B)$;

Estimate the complexity of computing $\text{LCLM}(A, B)$ by this method.

\[ A, B \in \mathcal{W}_{n,n}, \quad L := \text{LCLM}(A, B), \quad A = \sum_{i=0}^{r} a_i(x) \partial^i, \quad B = \sum_{i=0}^{s} b_i(x) \partial^i \]

$\triangleright$ $L$ 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 $R < 2n$.

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

$\triangleright$ Thus, $\text{ord}(L) < 2n$ and $\text{deg}_x(L) = O(n^3)$.

$\triangleright$ 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

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, 3, 5

1, 1, 2, 5, 14

1, 2, 9, 54, 378

1, 2, 16, 192, 2816

1, 3, 30, 420, 6930
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

1
8
42
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
<table>
<thead>
<tr>
<th></th>
<th>Sequence</th>
<th>Next Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1, 1, 1, 1, 1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1, 1, 2, 3, 5</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>1, 1, 2, 5, 14</td>
<td>42</td>
</tr>
<tr>
<td>4</td>
<td>1, 2, 9, 54, 378</td>
<td>2916</td>
</tr>
<tr>
<td>5</td>
<td>1, 2, 16, 192, 2816</td>
<td>46592</td>
</tr>
<tr>
<td>6</td>
<td>1, 3, 30, 420, 6930</td>
<td></td>
</tr>
</tbody>
</table>
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
   \[1/(1 - t)\]

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
   \[27\, t^2 y^2 + (1 - 18\, t)\, y + 16\, t = 1\]

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
   \[(27\, t^2 - t)\, y'' + (54\, t - 2)\, y' + 6\, y = 0\]
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
   \[ 27t^2y^2 + (1 - 18t)y + 16t = 1 \]

5. 1, 2, 16, 192, 2816
   \[ 64t^2y^3 + 16ty^2 + (1 - 72t)y + 54t = 1 \]

6. 1, 3, 30, 420, 6930
   \[ (27t^2 - t)y'' + (54t - 2)y' + 6y = 0 \]

▷ 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
   \[ 27t^2y^2 + (1 - 18t)y + 16t = 1 \]

5. 1, 2, 16, 192, 2816
   \[ 64t^2y^3 + 16ty^2 + (1 - 72t)y + 54t = 1 \]

6. 1, 3, 30, 420, 6930
   \[ (27t^2 - t)y'' + (54t - 2)y' + 6y = 0 \]

▷ 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 \( A = Q / \text{rev}_d(P) \) for some \( Q \in \mathbb{K}[x]_{<d} \),
where \( \text{rev}_d(P) = P(\frac{1}{x})x^d \).
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 \( A = Q / \text{rev}_d(P) \) for some \( Q \in \mathbb{K}[x]_{<d} \),
where \( \text{rev}_d(P) = P(\frac{1}{x}) x^d \).

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

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

1. \((a_n)\) is a l.r.s.c.c., having \( P \) as characteristic polynomial of degree \( d \).
2. \( A(x) \) is rational, of the form \( A = Q/\text{rev}_d(P) \) for some \( Q \in \mathbb{K}[x]_{<d} \),
   where \( \text{rev}_d(P) = P\left(\frac{1}{x}\right)x^d \).

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

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

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

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

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

\[ \text{Pade}(A, 2N) \]

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

\textbf{Out:} \((R, V)\) s.t. \( R/V \equiv A \mod x^{2N}, \deg R < N, \deg V \leq N, \) 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. \((Q_i, R_{i+1}) := \text{QuotRem}(R_{i-1}, R_i)\) \hspace{1cm} \#R_{i-1} = Q_iR_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.

\[ \begin{align*}
\blacktriangleright \textbf{Quadratic complexity: } & O(N^2) \text{ operations in } \mathbb{K} \\
\blacktriangleright \textbf{There exist quasi-linear time algorithms: } & O(M(N) \log N)
\end{align*} \]
Berlekamp-Massey algorithm

**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 $\text{Pade}(A, 2N)$ s.t. $V(0) = 1$.
3. $d = \max\{1 + \deg(R), \deg(V)\}$. Return $\text{rev}_d(V) = V(1/x)x^d$.

▷ **Quadratic complexity:** $O(N^2)$ operations in $\mathbb{K}$
▷ There exist quasi-linear time algorithms $O(M(N) \log N)$
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 $a_0, \ldots, a_{2N-1} \in \mathbb{K}$.

**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. $(Q_i, R_{i+1}) := \text{QuotRem}(R_{i-1}, R_i)$
   2. $V_{i+1} := V_{i-1} - Q_i V_i$
   3. $i := i + 1$
3. Return $V_i / \text{lc}(V_i)$.

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

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

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

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

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

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

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

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

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

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

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

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

and it computes

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

\[
V_2 := V_0 - Q_1 V_1 = -x + 1 \quad \rightarrow \quad a_{n+1} = a_n
\]

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

\[
V_3 := V_1 - Q_2 V_2 = -x^2 + x + 1 \quad \rightarrow \quad a_{n+2} = a_{n+1} + a_n
\]

\[
(Q_3, R_4) := \text{QuotRem}(R_2, R_3) = \left(\frac{x}{2} - \frac{1}{4}, -\frac{9x^4}{4} - \frac{9x^3}{4} - 51x^2 - \frac{115x}{4} + 60\right)
\]

\[
V_4 := V_2 - Q_3 V_3 = \frac{x^3}{2} - \frac{3x^2}{4} - \frac{5x}{4} + \frac{5}{4} \quad \rightarrow \quad a_{n+3} = \frac{3}{2}a_{n+2} + \frac{5}{2}a_{n+1} - \frac{5}{2}a_n
\]
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

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

and it computes

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

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

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

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

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

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

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

$$V_5 := V_3 - Q_4 V_4 = -\frac{4x^4}{9} + \frac{4x^3}{9} + \frac{4x^2}{9} + \frac{4x}{9} + \frac{4}{9} \quad \rightarrow \quad a_{n+4} = a_{n+3} + \cdots + a_n$$
HERMITE-PADÉ APPROXIMANTS
—guessing equations with polynomial coefficients—
**Definition:** Given a column vector $F = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and an $n$-tuple $d = (d_1, \ldots, d_n) \in \mathbb{N}^n$, a Hermite-Padé approximant of type $d$ for $F$ is a row vector $P = (P_1, \ldots, P_n) \in \mathbb{K}[x]^n, (P \neq 0)$, such that:

\[
\begin{align*}
&\text{(1)} \quad P \cdot F = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma) \\
&\text{(2)} \quad \deg(P_i) \leq d_i \quad \text{for all } i.
\end{align*}
\]

$\sigma$ is called the order of the approximant $P$.

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

- [Hermite, 1873]: $e$ is transcendent.
- [Lindemann, 1882]: $\pi$ is transcendent; so does $e^\alpha$ for any $\alpha \in \mathbb{Q}\{0\}$.
- [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 $\zeta(2k+1) \in \mathbb{Q}$.
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. $\text{deg}(P_i) \leq d_i$ for all $i$.

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

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

[Hermite, 1873]: $e$ is transcendent.

[Lindemann, 1882]: $\pi$ is transcendent; so does $e^{\alpha}$ for any $\alpha \in \mathbb{Q}\{0\}$.

[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 $\zeta(2k+1)/\in \mathbb{Q}$. 

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

1. \( P \cdot F = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma) \) with \( \sigma = \sum_i (d_i + 1) - 1 \),
2. \( \deg(P_i) \leq d_i \) for all \( i \).

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

- [Hermite, 1873]: \( e \) is transcendent.
- [Lindemann, 1882]: \( \pi \) is transcendent; so does \( e^{\alpha} \) for any \( \alpha \in \mathbb{Q} \setminus \{0\} \).
- [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 \( \zeta(2k+1) \in \mathbb{Q} \).
Definition: Given a column vector \( F = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n \) and an \( n \)-tuple \( d = (d_1, \ldots, d_n) \in \mathbb{N}^n \), a Hermite-Padé approximant of type \( d \) for \( F \) is a row vector \( P = (P_1, \ldots, P_n) \in \mathbb{K}[x]^n, (P \neq 0) \), such that:

1. \( P \cdot F = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma) \) with \( \sigma = \sum_i (d_i + 1) - 1 \),
2. \( \deg(P_i) \leq d_i \) for all \( i \).

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

1. $P \cdot F = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma)$ with $\sigma = \sum_i (d_i + 1) - 1$,
2. $\deg(P_i) \leq d_i$ for all $i$.

$\sigma$ is called the order of the approximant $P$.

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

- [Hermite, 1873]: $e$ is transcendent.
- [Lindemann, 1882]: $\pi$ is transcendent; so does $e^{\alpha}$ 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 polynômes $X_1, X_2, \ldots, X_n$, 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 $n$ polynômes, et qui...
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:

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

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 $P(x, C(x)) = 0 \mod x^5$. 
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

$$\alpha_0 + \alpha_1 x + (\beta_0 + \beta_1 x)(1 + x + 2x^2 + 5x^3 + 14x^4) + (\gamma_0 + \gamma_1 x)(1 + 2x + 5x^2 + 14x^3 + 42x^4) = O(x^5)$$
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:
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:
\[
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 2 & 1 \\
0 & 0 & 2 & 1 & 5 & 2 \\
0 & 0 & 5 & 2 & 14 & 5 \\
0 & 0 & 14 & 5 & 42 & 14
\end{bmatrix}
\begin{bmatrix}
\alpha_0 \\
\alpha_1 \\
\beta_0 \\
\beta_1 \\
\gamma_0 \\
\gamma_1
\end{bmatrix}
= 0 \iff
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 2 \\
0 & 0 & 2 & 1 & 5 \\
0 & 0 & 5 & 2 & 14 \\
0 & 0 & 14 & 5 & 42
\end{bmatrix}
\begin{bmatrix}
\alpha_0 \\
\alpha_1 \\
\beta_0 \\
\beta_1 \\
\gamma_0
\end{bmatrix}
= -\gamma_1
\begin{bmatrix}
0 \\
1 \\
2 \\
5 \\
14
\end{bmatrix}.
\]
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:

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

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:

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

By homogeneity, one can choose \(\gamma_1 = 1\).

Then, the violet minor shows that one can take \((\beta_0, \beta_1, \gamma_0) = (-1, 0, 0)\).
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:

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

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 $P(x, C(x)) = 0 \mod x^5$. 

\[\triangleright\]
Hermite-Padé approximants of $n = 2$ power series are related to Padé approximants, i.e. to approximation of series by rational functions

\[ f_\ell = A^{\ell-1}, \]

where $A \in \mathbb{K}[[x]]$

algebraic approximants = Hermite-Padé approximants for $f_\ell = A^{\ell-1}$, where $A \in \mathbb{K}[[x]]$

\[ 1 - y(x) + xy(x)^2 \]

\[ \left\{ -2y(x) + (2 - 4x) \frac{d}{dx} y(x) + x \frac{d^2}{dx^2} y(x), y(0) = 1, D(y)(0) = 1 \right\} \]
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 \(F = (f_1, \ldots, f_n)\) in \(\tilde{O}(n^\omega d)\) ops. in \(\mathbb{K}\).

Ideas:

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

Algorithm:

1. If \(\sigma = n(d + 1) - 1 \leq \text{threshold}\), call the naive algorithm
2. Else:
   1. recursively compute \(P_1 \in \mathbb{K}[x]^{n \times n}\) s.t. \(P_1 \cdot F = O(x^{\sigma/2})\), \(\deg(P_1) \approx \frac{d}{2}\)
   2. compute “residue” \(R\) such that \(P_1 \cdot F = x^{\sigma/2} \cdot (R + O(x^{\sigma/2}))\)
   3. recursively compute \(P_2 \in \mathbb{K}[x]^{n \times n}\) s.t. \(P_2 \cdot R = O(x^{\sigma/2})\), \(\deg(P_2) \approx \frac{d}{2}\)
   4. return \(P := P_2 \cdot P_1\)

▷ The precise choices of degrees is a delicate issue
▷ Corollary: Gcd, extended gcd, Padé approximants in \(\tilde{O}(d)\) ops. in \(\mathbb{K}\).
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 $Q = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $F = (1, A, \ldots, A^n)$. If $Q \cdot F = O(x^{2dn+1})$, then $Q \cdot F = 0$. 

Evaluation at $y = A(x)$ yields $R(x) = U(x, A(x))P(x, A(x)) + V(x, A(x))Q(x, A(x)) = O(x^{2dn+1})$. Thus $R = 0$, that is $\gcd(P, Q) \neq 1$, and thus $P | Q$, and $A$ is a root of $Q$. 

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

In other words, $A$ is a root of the polynomial $Q = \sum_{i=0}^{n} Q_i(x)y^i$. 
**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 \( Q = (Q_0, Q_1, \ldots, Q_n) \) be a Hermite-Padé approximant of type \((d, \ldots, d)\) for \( F = (1, A, \ldots, A^n) \). If \( Q \cdot F = O(x^{2dn+1}) \), then \( Q \cdot F = 0 \).

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 \( Q_0P_1 + Q_1P_0 = 0 \).
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 \( Q = (Q_0, Q_1, \ldots, Q_n) \) be a Hermite-Padé approximant of type \((d, \ldots, d)\) for \( F = (1, A, \ldots, A^n) \). If \( Q \cdot F = O(x^{2dn+1}) \), then \( Q \cdot F = 0 \).

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

Proof:
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 $Q = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d,\ldots,d)$ for $F = (1, A, \ldots, A^n)$. If $Q \cdot F = O(x^{2dn+1})$, then $Q \cdot F = 0$.

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

$$P(x, A(x)) = 0, \ \text{and} \ \deg_x(P) \leq d, \ \deg_y(P) \leq n.$$
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 $Q = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $F = (1, A, \ldots, A^n)$. If $Q \cdot F = O(x^{2dn+1})$, then $Q \cdot F = 0$.

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

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

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

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 $Q = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $F = (1, A, \ldots, A^n)$. If $Q \cdot F = O(x^{2dn+1})$, then $Q \cdot F = 0$.

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

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

- $R(x) = \text{Res}_y(P, Q) \in \mathbb{K}[x]$ 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 \( Q = (Q_0, Q_1, \ldots, Q_n) \) be a Hermite-Padé approximant of type \((d, \ldots, d)\) for \( F = (1, A, \ldots, A^n) \). If \( Q \cdot F = O(x^{2dn+1}) \), then \( Q \cdot F = 0 \).

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

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

- \( R(x) = \text{Res}_y(P, Q) \in \mathbb{K}[x] \) 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

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

Thus \( R = 0 \), that is \( \gcd(P, Q) \neq 1 \), and thus \( P | Q \), and \( A \) is a root of \( Q \).
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 $Q = (Q_0, Q_1, \ldots, Q_n)$ be a Hermite-Padé approximant of type $(d, \ldots, d)$ for $F = (1, A, \ldots, A^n)$. If $Q \cdot F = O(x^{2dn+1})$, then $Q \cdot F = 0$.

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

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

- $R(x) = \text{Res}_y(P, Q) \in \mathbb{K}[x]$ 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

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

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

Alin Bostan
Algorithmic guessing of algebraic and differential equations
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. \( P(t, f(t)) \equiv 0 \mod t^2 \), 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. \( P(t, f(t)) = 0 \) mod \( t^2 \), 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. \( P(t, f(t)) = 0 \) mod \( t^{20} \) by Hermite-Padé approximation.
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. \( P(t, f(t)) = 0 \mod t^2 \), 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. \( P(t, f(t)) = 0 \mod t^{20} \) 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. \( P(t, f(t)) = 0 \mod t^2 \), 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. \( P(t, f(t)) = 0 \mod t^{20} \) 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.
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. \( P(t, f(t)) = 0 \mod t^2 \), 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. \( P(t, f(t)) = 0 \mod t^{20} \) 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. \( P(t, f(t)) = 0 \mod t^2 \), 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. \( P(t, f(t)) = 0 \mod t^{20} \) 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

\[ f_5 := \sum_{n=0}^{\infty} \binom{5n}{n} t^n, \quad n=0..\infty \]
\[ \text{simplify}(f_5) \text{ assuming } t>0 \text{ and } t<1/100; \]

\[ 4F3 \left( \left[ \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5} \right] ; \left[ \frac{1}{4}, \frac{1}{2}, \frac{3}{4} \right] ; \frac{3125t}{256} \right) \]
Application: algebraicity of a hypergeometric series

\[
> \text{f5:=sum(binomial(5*n,n)*t^n, n=0..infinity):}
> \text{simplify(f5) assuming t>0 and t<1/100;}
\]

\[
_{4}F_{3} \left( \begin{bmatrix} 1 & 2 & 3 & 4 \end{bmatrix} ; \begin{bmatrix} 1 & 1 & 3 \end{bmatrix} ; \frac{3125 t}{256} \right)
\]

\[
> \text{P5:=subs(y(t) = y, seriestoalgeq(series(f5,t,20), y(t))[1]);}
\]

\[
1 + 15 y + 80 y^2 + 160 y^3 + (3125 t - 256) y^5
\]
Application: algebraicity of a hypergeometric series

\[
\begin{align*}
> f5&:=\text{sum}(\text{binomial}(5\cdot n, n) \cdot t^n, n=0..\infty): \\
> \text{simplify}(f5) \text{ assuming } t>0 \text{ and } t<1/100; \\
4F3 &\left( \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5' & 5' & 5' & 5' \end{bmatrix}; \begin{bmatrix} 1 & 1 & 3 \\ 4' & 2' & 4' \end{bmatrix}; \frac{3125 t}{256} \right)
\end{align*}
\]

\[
> P5 := \text{subs}(y(t) = y, \text{seriestoalgeq}(	ext{series}(f5, t, 20), y(t))[1]);
\]

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

\[
> \text{subs}\{t=0, y=1\}, P5, \text{subs}\{t=0, y=1\}, \text{diff}(P5,y);
\]

\[
0, -625
\]
Application: algebraicity of a hypergeometric series

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

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

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

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

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

\[
5 (5 n + 1) (5 n + 2) (5 n + 3) (5 n + 4) r(n) - \\
8 (4 n + 1) (2 n + 1) (4 n + 3) (n + 1) r(n + 1) = 0
\]

```maple
> 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 
\[(n + 3)a_{n+1} = (2n + 3)a_n + 3na_{n-1}, \text{ for all } n > 0.\]

Show that \(a_n\) is an integer for all \(n\).
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, \(a_0, \ldots, a_4\);
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 \(P(x, f(x)) = 0 \mod x^5\) 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
Review of a few direct algorithms (balanced case: $A, B \in W_{n,n}$)

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

$$BA = \sum_{i,j,u,v=0}^n b_{i,j} a_{u,v} x^i (\partial^j x^u) \partial^v \rightarrow O(n^5) \leq n \text{ terms}$$

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

$$BA = \sum_{i=0}^n b_i(x) (\partial^i A) \quad \text{by} \quad \partial T = T \partial + \frac{dT}{dx} \rightarrow O(M(n) n^2)$$

  degree $\leq 2n$ in $\partial$
  degree $\leq n$ in $x$

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

$$BA = \sum_{k=0}^n \frac{1}{k!} \left[ \frac{d^k B}{d \partial^k} \frac{d^k A}{d x^k} \right] \rightarrow O(M(n^2) n)$$

  bivariate commutative product
  in bidegree $(n,n)$
Review of complexity results (unbalanced case)

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

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

$\omega$ 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.
Product in $\mathbb{K}[x] \langle \theta \rangle$, with $\theta := x\partial$  
[Van der Hoeven, 2002]

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

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

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

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

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

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

- Composition: product of the matrices of differential operators.  
- Evaluation/interpolation: Vandermonde matrix and inverse.  
- Conversion $\partial \leftrightarrow \theta$: matrix of Stirling numbers and inverse.
A1. Fast multipoint evaluation/interpolation in $O(n M(n) \log n)$.

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

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

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

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

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

B2. Direct calculation with $\partial$. 
A new, direct algorithm for $\mathbb{K}[x]\langle \partial \rangle$, with better constant $c$.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>VdH$_\theta$</th>
<th>IVdH$_\theta$</th>
<th>VdH$_\partial$</th>
<th>IVdH$_\partial$</th>
<th>MulWeyl</th>
</tr>
</thead>
<tbody>
<tr>
<td>All block products</td>
<td>37</td>
<td>24</td>
<td>96</td>
<td>48</td>
<td>12</td>
</tr>
<tr>
<td>Zeros + Strassen</td>
<td>20</td>
<td>8</td>
<td>47</td>
<td>12</td>
<td>8</td>
</tr>
</tbody>
</table>

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

Equivalence $\text{SkewM}(n,n) \propto \text{MM}(n)$

[Van der Hoeven, 2002]: $\text{SkewM}(n,n) \subset O(\text{MM}(n))$

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

1. $\text{MM}(n) \subset \text{LTMM}(O(n))$:

$$
\begin{bmatrix}
I_n & 0 & 0 \\
M & I_n & 0 \\
0 & N & I_n
\end{bmatrix}^2 =
\begin{bmatrix}
I_n & 0 & 0 \\
2M & I_n & 0 \\
NM & 2N & I_n
\end{bmatrix}.
$$

2. $\text{LTMM}(n) \subset O(\text{SkewM}(n))$:

$$
\begin{bmatrix}
m_{0,0} & 0 & 0 \\
\vdots & \ddots & \ddots \\
m_{i,0} & \ldots & m_{i,i} & 0 \\
\vdots & \ddots & \ddots & \ddots \\
m_{n,0} & \ldots & m_{n,n-i} & \ldots & m_{n,n}
\end{bmatrix} \\
\overset{m_{i,j}=A_{i-j}(j)}{\longleftrightarrow} \sum_{\ell=0}^{n} x^\ell A_\ell(\theta).
$$

bidegree $(n,n)$
Characteristic \( p > 0 \): Product in \( \tilde{O}(pn^2) \) [B., Chyzak, Le Roux, 2008]

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 \( O(M(\deg f)) \).

\[
\left( \sum_{u=0}^{p-1} x^u B_u(x^p, \theta) \right) \left( \sum_{v=0}^{p-1} A_v(x^p, \theta) x^v \right) = \sum_{u,v=0}^{p-1} x^u \left[ (B_u A_v)(x^p, \theta) \right] x^v.
\]

Commutative bivariate product in bidegree \((n/p, n)\)

Products \( O\left( p^2 M(n^2/p) \right) \subset O\left( p M(n^2) \right) \)

Conversions \( x \leftrightarrow x^p: O\left( pn M(n) \log n \right) \)

Conversions \( \partial \leftrightarrow \theta: O\left( n M(n) \log n \right) \)

\[ \rightarrow \tilde{O}(pn^2). \]
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]
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 $x^i \exp(ax)$
  - Replace (fast) Lagrange interpolation by (fast) Hermite interpolation
  - Use $(x, \partial) \leftrightarrow \text{reflection} \rightarrow (\partial, -x)$ to reduce to the case $r \geq d$
The case of unbalanced products [Benoit, B., van der Hoeven, 2012]

**Theorem** [Benoit, B., Hoeven, 2012] Product in $W_{r,d} = K[x] \langle \partial \rangle_{d,r}$ 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 $x^i \exp(ax)$
- Replace (fast) Lagrange interpolation by (fast) Hermite interpolation
- Use $(x, \partial) \xrightarrow{\text{reflection}} (\partial, -x)$ to reduce to the case $r \geq d$

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