Beating binary powering for polynomial matrices

ISSAC'23 (Tromsø, Norway)

Sergey Yurkevich

Inria Saclay and University of Vienna

27th July, 2023

Joint work with Alin Bostan and Vincent Neiger.

An open problem

- Consider Fibonacci numbers: $F_0, F_1, \dots \in \mathbb{Z}$.
- The bit-size of F_N is in $\Theta(N)$.
- Can compute $F_N = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^N \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ in $O(\mathsf{M}_{\mathbb{Z}}(N))$ binary operations.

An open problem

- Consider Fibonacci numbers: $F_0, F_1, \dots \in \mathbb{Z}$.
- The bit-size of F_N is in $\Theta(N)$.
- Can compute $F_N = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^N \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ in $O(\mathsf{M}_{\mathbb{Z}}(N))$ binary operations.

Open problem

Can we compute $F_N \in \mathbb{Z}$ in $O(N)$ binary operations?

Polynomial case

- Fibonacci polynomials:

$$F_0(x) = 0, F_1(x) = 1 \text{ and } F_{n+2}(x) = xF_{n+1}(x) + F_n(x), \text{ for } n \geq 0$$

- Euclidean division for bivariate polynomials:

$$R_n(x, y) = y^n \bmod y^2 - xy - 1$$

- Powers of a polynomial matrix:

$$M_n(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^n$$

Polynomial case

- Fibonacci polynomials:

$$F_0(x) = 0, F_1(x) = 1 \text{ and } F_{n+2}(x) = xF_{n+1}(x) + F_n(x), \text{ for } n \geq 0$$

$$F_9(x) = 1 + 10x^2 + 15x^4 + 7x^6 + x^8 \text{ and } F_{10}(x) = 5x + 20x^3 + 21x^5 + 8x^7 + x^9.$$

- Euclidean division for bivariate polynomials:

$$R_n(x, y) = y^n \bmod y^2 - xy - 1$$

$$R_{10}(x, y) = 1 + 10x^2 + 15x^4 + 7x^6 + x^8 + (5x + 20x^3 + 21x^5 + 8x^7 + x^9)y.$$

- Powers of a polynomial matrix:

$$M_n(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^n$$

$$M_{10}(x) = \begin{pmatrix} 1 + 15x^2 + 35x^4 + 28x^6 + 9x^8 + x^{10} & 5x + 20x^3 + 21x^5 + 8x^7 + x^9 \\ 5x + 20x^3 + 21x^5 + 8x^7 + x^9 & 1 + 10x^2 + 15x^4 + 7x^6 + x^8 \end{pmatrix}.$$

Polynomial case

- Fibonacci polynomials:

$$F_0(x) = 0, F_1(x) = 1 \text{ and } F_{n+2}(x) = xF_{n+1}(x) + F_n(x), \text{ for } n \geq 0$$

$$F_9(x) = 1 + 10x^2 + 15x^4 + 7x^6 + x^8 \text{ and } F_{10}(x) = 5x + 20x^3 + 21x^5 + 8x^7 + x^9.$$

- Euclidean division for bivariate polynomials:

$$R_n(x, y) = y^n \bmod y^2 - xy - 1$$

$$R_{10}(x, y) = 1 + 10x^2 + 15x^4 + 7x^6 + x^8 + (5x + 20x^3 + 21x^5 + 8x^7 + x^9)y.$$

- Powers of a polynomial matrix: $$M_n(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^n$$

$$M_{10}(x) = \begin{pmatrix} 1 + 15x^2 + 35x^4 + 28x^6 + 9x^8 + x^{10} & 5x + 20x^3 + 21x^5 + 8x^7 + x^9 \\ 5x + 20x^3 + 21x^5 + 8x^7 + x^9 & 1 + 10x^2 + 15x^4 + 7x^6 + x^8 \end{pmatrix}.$$

Question

Can we compute $F_N, R_N, M_N \in \mathbb{K}[x]$ in $O(N)$ arithmetic operations?

How to compute $F_N(x)$ or $R_N(x, y)$ or $M_N(x)$?

- From the definition: $F_{n+2}(x) = xF_{n+1}(x) + F_n(x)$.

How to compute $F_N(x)$ or $R_N(x, y)$ or $M_N(x)$?

- From the definition: $F_{n+2}(x) = xF_{n+1}(x) + F_n(x)$. $O(N^2)$

How to compute $F_N(x)$ or $R_N(x,y)$ or $M_N(x)$?

- From the definition: $F_{n+2}(x) = xF_{n+1}(x) + F_n(x)$. $O(N^2)$
- Use binary powering to compute M_N, where $M_n(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^n$:

$$M_n(x) = \begin{cases} M_{\frac{n}{2}}(x)^2 & \text{if } n \text{ even,} \\ M(x) \cdot M_{\frac{n-1}{2}}(x)^2 & \text{if } n \text{ odd.} \end{cases}$$

How to compute $F_N(x)$ or $R_N(x, y)$ or $M_N(x)$?

- From the definition: $F_{n+2}(x) = xF_{n+1}(x) + F_n(x)$. $O(N^2)$
- Use binary powering to compute M_N, where $M_n(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^n$:

$$M_n(x) = \begin{cases} M_{\frac{n}{2}}(x)^2 & \text{if } n \text{ even,} \\ M(x) \cdot M_{\frac{n-1}{2}}(x)^2 & \text{if } n \text{ odd.} \end{cases} \quad O(\mathsf{M}(N)) = O(N \log(N))$$

How to compute $F_N(x)$ or $R_N(x,y)$ or $M_N(x)$?

- From the definition: $F_{n+2}(x) = xF_{n+1}(x) + F_n(x)$. $O(N^2)$
- Use binary powering to compute M_N, where $M_n(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^n$:

$$M_n(x) = \begin{cases} M_{\frac{n}{2}}(x)^2 & \text{if } n \text{ even,} \\ M(x) \cdot M_{\frac{n-1}{2}}(x)^2 & \text{if } n \text{ odd.} \end{cases} \quad O(\mathsf{M}(N)) = O(N \log(N))$$

- Write $F_N(x) = f_0 + f_1 x + \cdots + f_N x^N$. Then $(f_k)_{k \geq 0}$ satisfy:

$$f_{k+2} = \frac{(N+k+1)(N-k-1)}{4(k+1)(k+2)} f_k \quad \text{for } k \geq 0,$$

with $(f_0, f_1) = (1, 0)$ for odd N and $(f_0, f_1) = (0, N/2)$ for even N.

How to compute $F_N(x)$ or $R_N(x,y)$ or $M_N(x)$?

- From the definition: $F_{n+2}(x) = xF_{n+1}(x) + F_n(x)$. $O(N^2)$
- Use binary powering to compute M_N, where $M_n(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}^n$:

$$M_n(x) = \begin{cases} M_{\frac{n}{2}}(x)^2 & \text{if } n \text{ even,} \\ M(x) \cdot M_{\frac{n-1}{2}}(x)^2 & \text{if } n \text{ odd.} \end{cases} \qquad O(\mathsf{M}(N)) = O(N \log(N))$$

- Write $F_N(x) = f_0 + f_1 x + \cdots + f_N x^N$. Then $(f_k)_{k \geq 0}$ satisfy:

$$f_{k+2} = \frac{(N+k+1)(N-k-1)}{4(k+1)(k+2)} f_k \quad \text{for } k \geq 0, \qquad O(N)$$

with $(f_0, f_1) = (1, 0)$ for odd N and $(f_0, f_1) = (0, N/2)$ for even N.

Polynomial C-finite sequences

- A **polynomial C-finite sequence** $(u_n(x))_{n\geq 0} \in \mathbb{K}[x]^{\mathbb{N}}$ satisfies a recurrence

$$u_{n+r}(x) = c_{r-1}(x)u_{n+r-1}(x) + \cdots + c_0(x)u_n(x),$$

of some order $r \in \mathbb{N}$ and polynomial coefficients $c_0(x), \ldots, c_{r-1}(x) \in \mathbb{K}[x]$.

Polynomial C-finite sequences

- A **polynomial C-finite sequence** $(u_n(x))_{n\geq 0} \in \mathbb{K}[x]^{\mathbb{N}}$ satisfies a recurrence

$$u_{n+r}(x) = c_{r-1}(x)u_{n+r-1}(x) + \cdots + c_0(x)u_n(x),$$

  of some order $r \in \mathbb{N}$ and polynomial coefficients $c_0(x), \ldots, c_{r-1}(x) \in \mathbb{K}[x]$.
- The generating function is rational:

$$\sum_{k\geq 0} u_k(x)y^k = \frac{P(x,y)}{y^r Q(x,1/y)} \in \mathbb{K}(x,y)$$

Polynomial C-finite sequences

- A **polynomial C-finite sequence** $(u_n(x))_{n\geq 0} \in \mathbb{K}[x]^{\mathbb{N}}$ satisfies a recurrence

$$u_{n+r}(x) = c_{r-1}(x)u_{n+r-1}(x) + \cdots + c_0(x)u_n(x),$$

  of some order $r \in \mathbb{N}$ and polynomial coefficients $c_0(x), \ldots, c_{r-1}(x) \in \mathbb{K}[x]$.
- The generating function is rational:

$$\sum_{k\geq 0} u_k(x)y^k = \frac{P(x,y)}{y^r Q(x, 1/y)} \in \mathbb{K}(x,y)$$

- For some $a_1(x), \ldots, a_k(x) \in \overline{\mathbb{K}(x)}$ and $q_i(n,x) \in \mathbb{K}(a_1(x), \ldots, a_n(x))[n]$:

$$u_n(x) = q_1(n,x)a_1(x)^n + \cdots + q_k(n,x)a_k(x)^n$$

Polynomial C-finite sequences

- A **polynomial C-finite sequence** $(u_n(x))_{n\geq 0} \in \mathbb{K}[x]^{\mathbb{N}}$ satisfies a recurrence

$$u_{n+r}(x) = c_{r-1}(x)u_{n+r-1}(x) + \cdots + c_0(x)u_n(x),$$

  of some order $r \in \mathbb{N}$ and polynomial coefficients $c_0(x), \ldots, c_{r-1}(x) \in \mathbb{K}[x]$.
- The generating function is rational:

$$\sum_{k\geq 0} u_k(x)y^k = \frac{P(x,y)}{y^r Q(x,1/y)} \in \mathbb{K}(x,y)$$

- For some $a_1(x), \ldots, a_k(x) \in \overline{\mathbb{K}(x)}$ and $q_i(n,x) \in \mathbb{K}(a_1(x), \ldots, a_n(x))[n]$:

$$u_n(x) = q_1(n,x)a_1(x)^n + \cdots + q_k(n,x)a_k(x)^n$$

- $$u_n(x) = \begin{pmatrix} 0 & \ldots & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_{r-1}(x) & c_{r-2}(x) & \cdots & c_1(x) & c_0(x) \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}^n \cdot \begin{pmatrix} u_{r-1}(x) \\ \vdots \\ u_0(x) \end{pmatrix}$$

Theorem (Bostan, Neiger, Y., 2023)

Let $d, r \in \mathbb{N}$. There exists an algorithm solving in $O(N)$ operations $(\pm, \times, \div)$ in $\mathbb{K}$:

- SeqTerm: *Given a* **polynomial C-finite** *sequence $(u_n(x))_{n\geq 0}$ of order and degree at most r and d, compute the Nth term $u_N(x)$.*
- BivModPow: *Given polynomials $Q(x,y)$ and $P(x,y)$ in $\mathbb{K}[x,y]$ of degrees in y and x at most r and d, with $P(x,y)$ monic in y, compute $Q(x,y)^N \bmod P(x,y)$.*
- PolMatPow: *Given a square polynomial matrix $M(x)$ over $\mathbb{K}[x]$ of size and degree at most r and d, compute $M(x)^N$.*

Theorem (Bostan, Neiger, Y., 2023)

Let $d, r \in \mathbb{N}$. There exists an algorithm solving in $O(N)$ *operations* $(\pm, \times, \div)$ *in* $\mathbb{K}$:

- SeqTerm: *Given a* **polynomial C-finite** *sequence* $(u_n(x))_{n\geq 0}$ *of order and degree at most* r *and* d, *compute the* N*th term* $u_N(x)$.
- BivModPow: *Given polynomials* $Q(x,y)$ *and* $P(x,y)$ *in* $\mathbb{K}[x,y]$ *of degrees in* y *and* x *at most* r *and* d, *with* $P(x,y)$ *monic in* y, *compute* $Q(x,y)^N \bmod P(x,y)$.
- PolMatPow: *Given a square polynomial matrix* $M(x)$ *over* $\mathbb{K}[x]$ *of size and degree at most* r *and* d, *compute* $M(x)^N$.

$$
\begin{tikzcd}
& \boxed{\textsc{SeqTerm}} \arrow[dl, Rightarrow, "\text{rational g.f.}"'] & \\
\boxed{\textsc{BivModPow}} \arrow[rr, Rightarrow, "\text{Cayley-Hamilton Thm.}"'] & & \boxed{\textsc{PolMatPow}} \arrow[ul, Rightarrow, "\text{Companion matrix}"']
\end{tikzcd}
$$

The case $r = 1$

- $u_{n+1}(x) = c_0(x) u_n(x) \Rightarrow u_n(x) = c_0(x)^n u_0(x)$.

The case $r = 1$

- $u_{n+1}(x) = c_0(x) u_n(x) \Rightarrow u_n(x) = c_0(x)^n u_0(x)$.
- [Flajolet, Salvy, 1997]: Problem 4 in “The SIGSAM challenges”:

PROBLEM 4

What is the coefficient of x^{3000} in the expansion of the polynomial

$$(x+1)^{2000}(x^2+x+1)^{1000}(x^4+x^3+x^2+x+1)^{500}$$

to 13 significant digits?

The case $r = 1$

- $u_{n+1}(x) = c_0(x)u_n(x) \Rightarrow u_n(x) = c_0(x)^n u_0(x)$.
- [Flajolet, Salvy, 1997]: Problem 4 in "The SIGSAM challenges":

PROBLEM 4

What is the coefficient of x^{3000} in the expansion of the polynomial

$$(x+1)^{2000}(x^2+x+1)^{1000}(x^4+x^3+x^2+x+1)^{500}$$

to 13 significant digits?

- $f(x) = p(x)^N$ satisfies the ODE $p(x)f'(x) - Np'(x)f(x) = 0$.

The case $r = 1$

- $u_{n+1}(x) = c_0(x)u_n(x) \Rightarrow u_n(x) = c_0(x)^n u_0(x)$.
- [Flajolet, Salvy, 1997]: Problem 4 in "The SIGSAM challenges":

PROBLEM 4

What is the coefficient of x^{3000} in the expansion of the polynomial

$$(x+1)^{2000}(x^2+x+1)^{1000}(x^4+x^3+x^2+x+1)^{500}$$

to 13 significant digits?

- $f(x) = p(x)^N$ satisfies the ODE $p(x)f'(x) - Np'(x)f(x) = 0$.
- The coefficients satisfy

$$\begin{aligned}
r123 := \{&u(1) = 3500, u(2) = 6124750, u(3) = 7144958500, u(4) = 6251073531125,\\
&u(5) = 4375037588062700, u(6) = 2551584931812376500, u(0) = 1,\\
&(n-6000)u(n) + (3n-14497)u(n+1) + (5n-19990)u(n+2)\\
&+ (6n-19482)u(n+3) + (6n-16476)u(n+4) + (5n-9975)u(n+5)\\
&+ (3n-3482)u(n+6) + (n+7)u(n+7)\}
\end{aligned}$$

The case $r = 1$

- $u_{n+1}(x) = c_0(x)u_n(x) \Rightarrow u_n(x) = c_0(x)^n u_0(x)$.
- [Flajolet, Salvy, 1997]: Problem 4 in "The SIGSAM challenges":

PROBLEM 4

What is the coefficient of x^{3000} in the expansion of the polynomial

$$(x+1)^{2000}(x^2+x+1)^{1000}(x^4+x^3+x^2+x+1)^{500}$$

to 13 significant digits?

- $f(x) = p(x)^N$ satisfies the ODE $p(x)f'(x) - Np'(x)f(x) = 0$.
- The coefficients satisfy

$$\begin{aligned}
r123 := \{&u(1) = 3500, u(2) = 6124750, u(3) = 7144958500, u(4) = 6251073531125,\\
&u(5) = 4375037588062700, u(6) = 2551584931812376500, u(0) = 1,\\
&(n-6000)u(n) + (3n-14497)u(n+1) + (5n-19990)u(n+2)\\
&+ (6n-19482)u(n+3) + (6n-16476)u(n+4) + (5n-9975)u(n+5)\\
&+ (3n-3482)u(n+6) + (n+7)u(n+7)\}
\end{aligned}$$

- The full coefficient of x^{3000} could be computed by [Flajolet, Salvy, 1997] in 15sec!

SeqTerm in $O(N)$

Lemma

Let $a(x) \in \overline{\mathbb{K}(x)}$ and let $g(x)$ be **D-finite**. *Then $f(x) = g(a(x))$ is* **D-finite**.

SeqTerm in $O(N)$

Lemma

Let $a(x) \in \overline{\mathbb{K}(x)}$ and let $g(x)$ be **D-finite**. *Then $f(x) = g(a(x))$ is* **D-finite**.

Sketch of proof.

The vector space spanned over $\mathbb{K}(x)$ by $(f^{(i)}(x))_{i \geq 0}$ is finite-dimensional over $\mathbb{K}(x, a(x))$ which is itself finite-dimensional over $\mathbb{K}(x)$. $\square$

SeqTerm in $O(N)$

Lemma

Let $a(x) \in \overline{\mathbb{K}(x)}$ and let $g(x)$ be **D-finite**. *Then $f(x) = g(a(x))$ is* **D-finite**.
In particular, $a(x)^n$ satisfies a **linear ODE** *of* **order and degree independent of** n.

Sketch of proof.

The vector space spanned over $\mathbb{K}(x)$ by $(f^{(i)}(x))_{i \geq 0}$ is finite-dimensional over $\mathbb{K}(x, a(x))$ which is itself finite-dimensional over $\mathbb{K}(x)$.
Set $g(x) = x^n$ which satisfies $xg'(x) = ng(x)$. $\square$

For example: if $\varphi(x) = (x + \sqrt{x^2 + 4})/2$ then $y(x) = \varphi(x)^n$ satisfies

$$(x^2 + 4)y''(x) + xy'(x) - n^2 y(x) = 0.$$

SeqTerm in $O(N)$

Lemma

Let $a(x) \in \overline{\mathbb{K}(x)}$ and let $g(x)$ be **D-finite**. *Then $f(x) = g(a(x))$ is* **D-finite**.
In particular, $a(x)^n$ satisfies a **linear ODE** *of* **order and degree independent of** n.

- Recall: If $(u_n(x))_{n\geq 0}$ is **polynomial C-finite** then:

$$u_n(x) = q_1(n,x)a_1(x)^n + \cdots + q_k(n,x)a_k(x)^n.$$

SeqTerm in $O(N)$

Lemma

Let $a(x) \in \overline{\mathbb{K}(x)}$ and let $g(x)$ be **D-finite**. *Then $f(x) = g(a(x))$ is* **D-finite**.
In particular, $a(x)^n$ satisfies a **linear ODE** *of* **order and degree independent of** n.

- Recall: If $(u_n(x))_{n\geq 0}$ is **polynomial C-finite** then:

$$u_n(x) = q_1(n,x)a_1(x)^n + \cdots + q_k(n,x)a_k(x)^n.$$

- Hence $u_n(x)$ satisfies a "**small**" **ODE** (degree and order independent of n).

SeqTerm in $O(N)$

Lemma

Let $a(x) \in \overline{\mathbb{K}(x)}$ and let $g(x)$ be **D-finite***. Then $f(x) = g(a(x))$ is* **D-finite***.*
In particular, $a(x)^n$ satisfies a **linear ODE** *of* **order and degree independent of n***.*

- Recall: If $(u_n(x))_{n \geq 0}$ is **polynomial C-finite** then:

$$u_n(x) = q_1(n, x)a_1(x)^n + \cdots + q_k(n, x)a_k(x)^n.$$

- Hence $u_n(x)$ satisfies a "**small**" **ODE** (degree and order independent of n).
- Write $u_N(x) = c_0 + c_1 x + c_2 x^2 + \cdots$. Then: $(c_k)_{k \geq 0}$ satisfies "**small**" **recursion**.

SeqTerm in $O(N)$

Lemma

Let $a(x) \in \overline{\mathbb{K}(x)}$ and let $g(x)$ be **D-finite**. *Then $f(x) = g(a(x))$ is* **D-finite**.
In particular, $a(x)^n$ satisfies a **linear ODE** *of* **order and degree independent of** *n.*

- Recall: If $(u_n(x))_{n\geq 0}$ is **polynomial C-finite** then:

$$u_n(x) = q_1(n,x)a_1(x)^n + \cdots + q_k(n,x)a_k(x)^n.$$

- Hence $u_n(x)$ satisfies a "**small**" **ODE** (degree and order independent of n).
- Write $u_N(x) = c_0 + c_1 x + c_2 x^2 + \cdots$. Then: $(c_k)_{k\geq 0}$ satisfies "**small**" **recursion**.
- Compute initial terms and unroll $\Rightarrow$ all c_i in $O(N)$ arithmetic operations
  $\Rightarrow u_N(x)$ in $O(N)$ arithmetic complexity.

What if unrolling is impossible?

- Consider $u_n = 2^n + x^n + x^{2n}$.

What if unrolling is impossible?

- Consider $u_n = 2^n + x^n + x^{2n}$.
- **Small ODE**: $x^2 u_n'''(x) - 3x(n-1)u_n''(x) + (2n-1)(n-1)u_n'(x) = 0$,
- For $u_n(x) = \sum_{k\geq 0} c_{n,k} x^k$ obtain the recursion: $(2n-k)(n-k)kc_{n,k} = 0$.

What if unrolling is impossible?

- Consider $u_n = 2^n + x^n + x^{2n}$.
- **Small ODE**: $x^2 u_n'''(x) - 3x(n-1)u_n''(x) + (2n-1)(n-1)u_n'(x) = 0$,
- For $u_n(x) = \sum_{k \geq 0} c_{n,k} x^k$ obtain the recursion: $(2n-k)(n-k)kc_{n,k} = 0$.
- **Problem:** Cannot unroll (for $k = 0$ and $k = N$ and $k = 2N$)!

What if unrolling is impossible?

- Consider $u_n = 2^n + x^n + x^{2n}$.
- **Small ODE**: $x^2 u_n'''(x) - 3x(n-1)u_n''(x) + (2n-1)(n-1)u_n'(x) = 0$,
- For $u_n(x) = \sum_{k\geq 0} c_{n,k}x^k$ obtain the recursion: $(2n-k)(n-k)kc_{n,k} = 0$.
- **Problem:** Cannot unroll (for $k = 0$ and $k = N$ and $k = 2N$)!
- **Solution:** Define $v_n(x) = u_n(x+1)$. Then for $v_n(x) = \sum_{k\geq 0} d_{n,k}x^k$:

  $$(k+1)(k+2)d_{n,k+2} - (k+1)(3n-2k-1)d_{n,k+1} + (2n-k)(n-k)d_{n,k} = 0.$$

  Compute $v_n(x)$, then compute u_N and u_{2N} via $c_{M,i} = \sum_{k\geq 0} d_{M,k}\binom{k}{i}(-1)^{k-i}$.
- This strategy works in general because the **ODE** has finitely many singularities.

SeqTerm in $O(N)$ in practice

- Goal: Find **small** **ODE** for $u_N(x)$ efficiently.

SeqTerm in $O(N)$ in practice

- Goal: Find **small ODE** for $u_N(x)$ efficiently.
- Using Cauchy's integral formula write:

$$u_n(x) = \frac{1}{2\pi i}\oint_{|y|=\epsilon} \frac{U(x,y)}{y^{n+1}}\mathrm{d}y.$$

SeqTerm in $O(N)$ in practice

- Goal: Find **small ODE** for $u_N(x)$ efficiently.
- Using Cauchy's integral formula write:

$$u_n(x) = \frac{1}{2\pi i}\oint_{|y|=\epsilon} \frac{U(x,y)}{y^{n+1}}\mathrm{d}y.$$

- Creative Telescoping finds:

$$\Big(\underbrace{p_k(n,x)\partial_x^k + \cdots + p_0(n,x)}_{\text{"Telescoper"}}\Big)\frac{U(x,y)}{y^{n+1}} = \partial_y\Big(\underbrace{C(n,x,y)}_{\text{"Certificate"}}\Big).$$

- By Cauchy's integral theorem: $\big((p_k(n,x)\partial_x^k + \cdots + p_0(n,x)\big)\, u_n = 0.$

SeqTerm in $O(N)$ in practice

- Goal: Find **small ODE** for $u_N(x)$ efficiently.
- Using Cauchy's integral formula write:

$$u_n(x) = \frac{1}{2\pi i} \oint_{|y|=\epsilon} \frac{U(x,y)}{y^{n+1}} \mathrm{d}y.$$

- Creative Telescoping finds:

$$\Big(\underbrace{p_k(n,x)\partial_x^k + \cdots + p_0(n,x)}_{\text{“Telescoper”}}\Big)\frac{U(x,y)}{y^{n+1}} = \partial_y\Big(\underbrace{C(n,x,y)}_{\text{“Certificate”}}\Big).$$

- By Cauchy's integral theorem: $\big((p_k(n,x)\partial_x^k + \cdots + p_0(n,x)\big)u_n = 0.$
- Can prove for reduction based Creative Telescoping:

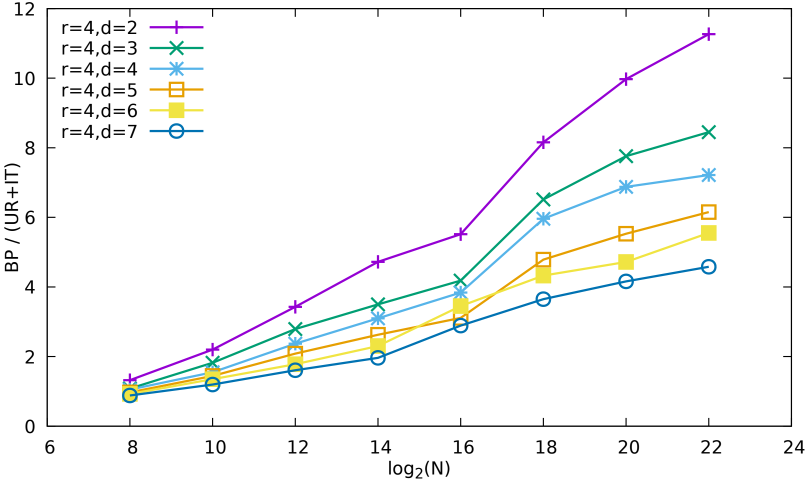
Order and degree of the Telescoper are independent of n.

Algorithm by example: Fibonacci polynomials

- $F_{n+2}(x) = xF_{n+1}(x) + F_n(x)$ with $F_0(x) = 0, F_1(x) = 1$.
- Generating function: $$\sum_{k\geq 0} F_k y^k = \frac{1}{1-xy-y^2}.$$
- Hence: $$F_n = \frac{1}{2\pi i}\oint_{|y|=\epsilon} \frac{1}{(1-xy-y^2)y^{n+1}}\mathrm{d}y.$$

Precomputation:

- `DEtools[Zeilberger](1/(1-x*y-y^2)/y^n, x, y, Dx);` $O(1)$
  $$(x^2+4)F_n''(x)^2 + 3xF_n'(x) + (1-n^2)F_n(x) = 0.$$
- `gfun[diffeqtorec](deq, F(x), u(k));` $O(1)$
  $$4(k+1)(k+2)f_{k+2} - (n+k+1)(n-k-1)f_k = 0.$$
- Compute f_0, f_1 by binary powering mod x^2. $O(\log(N))$
- Unroll. $O(N)$



- $M(x) \in \mathbb{K}[x]^{4\times 4}$.
- Want: $M(x)^N$.
- $\deg M(x) = 2, \ldots, 7$.
- $N = 2^8, 2^{10}, \ldots, 2^{22}$.

BP: Time for binary powering.
UR+IT: Time for unrolling + computing initial terms.

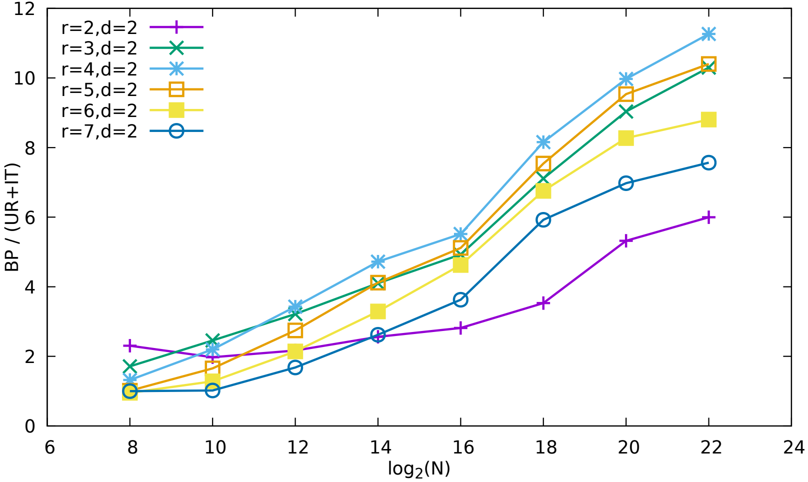
Summary and future work

- SeqTerm, BivModPow and PolMatPow can be solved in complexity $O(N)$.

- $M(x)^N$ can be computed faster than with binary powering, in practice and theory.

- Many future works:
  - More detailed complexity (w.r.t. r, d).
  - The Kth coefficient of the Nth term.
  - More general sequences.
  - Connection to the Jordan–Chevalley decomposition.

Bonus: More timings



- $M(x) \in \mathbb{K}[x]^{r \times r}$.
- Want: $M(x)^N$.
- $\deg M(x) = 2$.
- $r = 2, \ldots, 7$.
- $N = 2^8, 2^{10}, \ldots, 2^{22}$.

BP: Time for binary powering.

UR+IT: Time for unrolling + computing initial terms.

Bonus: Some precomputation timings

		Maple				Sage	Mathematica					
r	d	redct	HT	ZB	c_t	ct	FCT	CT	HCT	ℓ	d_n	d_x
2	2	0.0	0.1	0.0	0.1	0.5	0.2	0.2	0.2	2	2	16
	4	0.0	0.0	0.0	0.1	0.6	0.4	0.4	0.3	2	2	34
	6	0.0	0.0	0.0	0.1	0.6	0.7	0.5	0.5	2	2	52
	8	0.0	0.0	0.0	0.1	0.8	1.0	0.7	0.7	2	2	70
3	1	0.0	0.2	0.0	0.5	2.0	2.0	1.3	1.3	3	5	24
	2	0.0	0.1	0.8	3.4	3.1	4.0	2.6	2.5	3	5	54
	3	0.1	0.2	0.8	9.3	5.6	10	5.7	5.4	3	5	84
	4	0.1	0.5	18	19	8.2	17	9.4	8.9	3	5	114
	5	0.2	1.1	5.1	32	12	25	14	14	3	5	144
	6	0.5	1.7	9.8	49	17	35	19	20	3	5	174
4	1	0.4	2.9	23	117	20	31	25	25	4	9	58
	2	1.7	17	410	749	45	101	96	95	4	9	128
	3	4.4	43			89	295	376	373	4	9	198
	4	12	82			172	388	752	693	4	9	268
	5	18	128			280	635			4	9	338
5	1	11	34	538		163	847	780		5	14	115
	2	64	183			515				5	14	250
	3	159	526							5	14	385
	4	345								5	14	520

- Want $M(x)^N$, with $M(x) \in \mathbb{K}[x]^{r\times r}$, degree d.
- Seconds for Telescoper of

$$\frac{P(x,y)}{y^{n+1}Q(x,y)},$$

$Q(x,y)$ is the char. poly.

- redct: [Bostan, Chyzak, Lairez, Salvy,'18].
  HermiteTelescoping (HT): [Bostan, Lairez, Salvy,'13].
  Zeilberger (ZB): [DETools].
  c_t: [Chyzak, '00].
  ct: [Kauers,Mezzarobba,'19].
  CT: [Koutschan, '10].