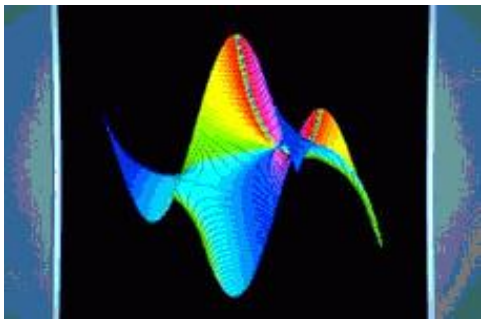
D-finiteness: Algorithms and Applications

Alin Bostan, Frédéric Chyzak, Bruno Salvy

Algorithms Project, Inria



March 21, 2007

I Intro

Aim: at the end of this talk, you should be able to

- give an algorithm to compute the first N decimal digits of $\pi = 3.14159265358979323\ldots$ in $\tilde{\mathcal{O}}(N)$ bit operations.
- compute in $\tilde{\mathcal{O}}(N)$ bit operations the ($\mathcal{O}(N)$ bits long) coefficient of x^N in the expansion of $(1+x+x^2)^N$.

- prove that $y = \tan(x)$ verifies no linear differential equation with polynomial coefficients, even though $y' = 1 + y^2$.
- show that the sequence (p_n) of prime numbers $2, 3, 5, 7, 11, \ldots$ does not satisfy any linear recurrence with coefficients in $\mathbb{Q}[n]$.

- give an algorithm using $\tilde{\mathcal{O}}(\sqrt{N})$ bit operations to decide if

  $$(2x+1)^3y''+(2x+1)(8x+3-4N(1+2x))y'+2N((4x+2)N-4x-1)y = 0$$

  has or not a polynomial solution $y(x) \in \mathbb{Q}[x]$.
- show that $y(x) = (x+1)/(x-1)$ is the only solution in $\mathbb{Q}(x)$ of

  $$(x-1)(x^2-2)y''(x) + 2x(x^2-x-1)y'(x) + 4(x-2)y(x) = 0.$$

But you will still have to attend the next talks to find out how your computer can prove/discover identities like

$$\sum_{k=0}^{2n}(-1)^k\frac{\binom{4n}{2k}}{\binom{2n}{k}} = \frac{1}{1-2n},$$

$$\sum_{k\in\mathbb{Z}}(-1)^k\binom{a+b}{a+k}\binom{a+c}{c+k}\binom{b+c}{b+k} = \frac{(a+b+c)!}{a!\,b!\,c!},$$

$$\sum_{k=0}^{n}\left(\sum_{j=0}^{k}\binom{n}{j}\right)^3 = n2^{3n-1}+2^{3n}-3n2^{n-2}\binom{2n}{n},$$

$$\frac{1}{2}J_0(x)^2+J_1(x)^2+J_2(x)^2+\cdots = \frac{1}{2},$$

$$\int_0^{+\infty} xJ_1(ax)I_1(ax)Y_0(x)K_0(x)\,dx = -\frac{\ln(1-a^4)}{2\pi a^2}.$$

Structure of the talk

1. Fast computation of the first N terms, resp. of the Nth term, of a recurrence with polynomial coefficients
2. Singularities of D-finite series
3. Polynomial and rational solutions of linear differential equations

II N terms vs. Nth term

The naive algorithm is optimal for the first N terms

$$a_r(n)u_{n+r} + \cdots + a_0(n)u_n = 0, \qquad a_i \in \mathbb{K}[n].$$

rewrites as a 1st order recurrence in $U_n = (u_n, \ldots, u_{n+r-1})^t$ with matrix coefficient over $\mathbb{K}(n)$

$$U_{n+1} = C(n)U_n \quad \text{where} \quad C(n) = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ -\frac{a_0}{a_r}(n) & & \cdots & & -\frac{a_{r-1}}{a_r}(n) \end{pmatrix}.$$

$\longrightarrow$ $\mathcal{O}(N)$ arithmetic ops to compute $u_0, u_1, \ldots, u_N$
$\longrightarrow$ series expansion of solutions of LDE: $\mathcal{O}(N)$ arithmetic ops.
$\longrightarrow$ $\tilde{\mathcal{O}}(N^2)$ bit operations to compute $u_0, u_1, \ldots, u_N$ over $\mathbb{K} = \mathbb{Q}$.

One can do much better to compute the Nth term alone!

Results

1. $u_0, u_1, \ldots u_N$ in $\mathcal{O}(N)$ arithmetic ops, $\tilde{\mathcal{O}}(N^2)$ bit ops
   OPTIMAL
2. u_N over $\mathbb{K} = \mathbb{Q}$ in $\tilde{\mathcal{O}}(N)$ bit ops (by binary splitting)
   OPTIMAL
3. u_N in $\tilde{\mathcal{O}}(\sqrt{N})$ arithmetic ops (by baby steps/giant steps)
   NOT OPTIMAL
4. Special case, constant coefficients $a_i \in \mathbb{K}$: u_N in $\mathcal{O}(\log N)$ arithmetic ops, $\mathcal{O}(N)$ bit operations OPTIMAL

$\longrightarrow$ open problem: can we compute u_N in the general case in only $\mathcal{O}(\log N)$ arithmetic ops?
$\longrightarrow$ if the answer were YES, then PRIMES IS IN P would be trivial
$(p-1)! = -1 \bmod p$ iff p is prime (Wilson)

Examples of applications

- compute high decimal expansions of constants like $e, \gamma, \pi, \zeta(3)$ [Hakmem72,Brent75,Chudnovsky^{2}88]
- more generally, evaluate a D-finite function at an algebraic number $\longrightarrow$ analytic continuation along arbitrary paths
- Sigsam Challenges'97, Problem 4. Coefficient of x^{3000} in

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

(first compute a rec. of order 7, then use binary splitting)

- From an analysis of Gröbner bases: roots of $P_n(x)$ defined by

$$\sum_{n\geq 0} P_n(x)\frac{z^n}{n!} = \left(\frac{1+z}{1+z^2}\right)^x$$

controll the complexity of solving "generic" systems with n quadratic equations in $\mathbb{F}_2[x_1,\ldots,x_n]$ [BaFaSa05]

- Rational solutions of LDEs & LREs [BoClSa05, BoChClSa06]

The easy case: constant coefficients

Fibonacci-like sequences:

$$F_0 = F_1 = 1, \qquad F_{n+2} = aF_{n+1} + bF_n, \quad (a, b \in \mathbb{Q}).$$

Matrix formulation:

$$\begin{pmatrix} F_{N-1} \\ F_N \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}}_{C} \begin{pmatrix} F_{N-2} \\ F_{N-1} \end{pmatrix} = C^{N-1} \begin{pmatrix} F_0 \\ F_1 \end{pmatrix}, \qquad N \geq 1.$$

$\longrightarrow$ F_N in $\mathcal{O}(\log N)$ arithmetic operations by binary powering:

$$C^k = \begin{cases} (C^{k/2})^2, & \text{if } k \text{ is even,} \\ (C^{\frac{k-1}{2}})^2 C, & \text{else.} \end{cases}$$

$\longrightarrow$ easy generalization to recurrences of arbitrary order with constant coefficients.

Fast Multiplication

- Balanced input: $\operatorname{size} T \times \operatorname{size} T$
  - Naïve: $\mathsf{I}(T) = \mathcal{O}(T^2)$
  - Karatsuba (1963): $\mathsf{I}(T) = \mathcal{O}(T^{1.59})$
  - Fast Fourier Transform: $\mathsf{I}(T) = \mathcal{O}(T \log T \log\log T) = \tilde{\mathcal{O}}(T)$ [Schönhage-Strassen71, Fürer07]
- Same for polynomials ($\mathsf{M}(T)$).
- Many applications via Newton iteration, including division.
- Fast polynomial gcd, resultant, multipoint evaluation, interpolation by divide-and-conquer.

Multipoint Evaluation

Problem (Evaluate P at $x_1, \ldots, x_d$, $\deg P = d$.)

Naive way: $\mathcal{O}(d^2)$ operations.

Multipoint Evaluation

Problem (Evaluate P at $x_1, \dots, x_d$, $\deg P = d$.)

Naive way: $\mathcal{O}(d^2)$ operations.

Borodin & Moenck 74: Recursive computation

$$Q_i^j := (x - x_i) \cdots (x - x_j)$$

$$P(x_i) = \begin{cases} (P \bmod Q_1^{\lfloor d/2 \rfloor})(x_i), & i \le d/2 \\ (P \bmod Q_{\lceil d/2 \rceil}^{d})(x_i), & i > d/2. \end{cases}$$

$$\text{Complexity: } C(d) = \underbrace{2C(d/2)}_{\text{recursion}} + \underbrace{2\,\mathrm{M}(d/4)}_{Q} + \underbrace{\frac{7}{2}\,\mathrm{M}(d)}_{\text{divisions}}$$

$$= \mathcal{O}(\mathrm{M}(d) \log d) = \tilde{\mathcal{O}}(d).$$

Binary Splitting & Bit Complexity

Problem (Fast computation of $N! = 1 \times \cdots \times N$)

Naive way: complexity $\tilde{\mathcal{O}}(N^2)$

$$\sum_{k=1}^{N} \mathsf{I}(k \log k, \log k) = \sum_{k=1}^{N} k\, \mathsf{I}(\log k) =$$

$$\mathcal{O}\big(N^2\, \mathsf{I}(\log N)\big) = \tilde{\mathcal{O}}(N^2)$$

Binary Splitting & Bit Complexity

Problem (Fast computation of $N! = 1 \times \cdots \times N$)

Naive way: complexity $\tilde{\mathcal{O}}(N^2)$

- Binary Splitting: balance computation sequence so as to take advantage of fast multiplication (operands of same sizes):

$$N! = \underbrace{(1 \times \cdots \times \lfloor N/2 \rfloor)}_{\text{size } \frac{1}{2} N \log N} \times \underbrace{((\lfloor N/2 \rfloor + 1) \times \cdots \times N)}_{\text{size } \frac{1}{2} N \log N}$$

  and recurse. Complexity $\tilde{\mathcal{O}}(N)$.
- Extends to matrix factorials $C(N)C(N-1)\cdots C(1)$, same complexity $\longrightarrow$ recurrences of arbitrary order.

Example: fast computation of $e = \exp(1)$

$$e_n = \sum_{k=0}^{n} \frac{1}{k!} \to \exp(1) = 2.7182818284590452\ldots$$

$e_n - e_{n-1} = 1/n! \Rightarrow n(e_n - e_{n-1}) = e_{n-1} - e_{n-2}$, thus

$$\begin{pmatrix} e_{N-1} \\ e_N \end{pmatrix} = \frac{1}{N} \underbrace{\begin{pmatrix} 0 & N \\ -1 & N+1 \end{pmatrix}}_{C(N)} \begin{pmatrix} e_{N-2} \\ e_{N-1} \end{pmatrix} = \frac{1}{N!} C(N)C(N-1)\cdots C(2) \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$\to$ e_N in $\tilde{\mathcal{O}}(N)$ bit operations [Brent76]

$\to$ generalizes to the evaluation of any D-finite function at an algebraic number [Chudnovsky^{2}87]

Example: fast computation of π

Ramanujan's marvelous hypergeometric identity (1914)

$$\frac{1}{\pi} = \frac{\sqrt{8}}{9801} \sum_{n \geq 0} \frac{(4n)!(1103 + 26390n)}{(n!)^4 \cdot (4 \cdot 99)^{4n}}.$$

Hides some deep number theory. Algebraic relations between ${}_2F_1$ and ${}_3F_2$ via Clausen's identity

$${}_2F_1\left(\left.\begin{matrix} a, b \\ a+b+1/2 \end{matrix}\right| z\right)^2 = {}_3F_2\left(\left.\begin{matrix} 2a, a+b, 2b \\ a+b+1/2, 2a+2b \end{matrix}\right| z\right)$$

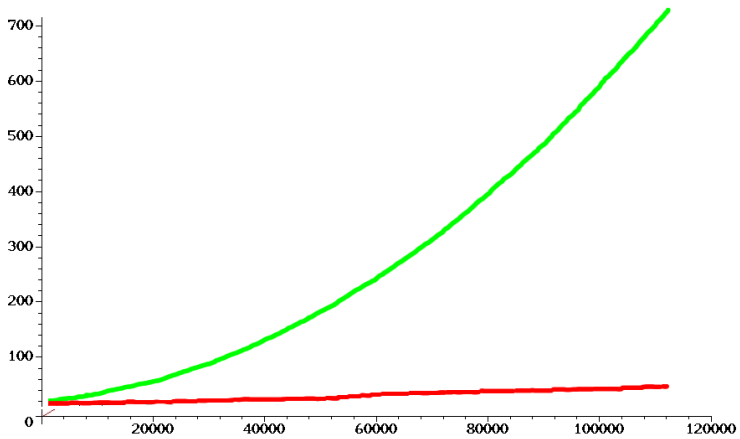
give a representation of $(K(k)/\pi)^2$ as a ${}_3F_2$ hypergeometric function, where $K(k)$ is the complete elliptic integral

$$K(k) = \int_0^{\pi/2} \frac{dt}{\sqrt{1 - k^2 \sin^2 t}} = \frac{\pi}{2} \cdot {}_2F_1\left(\left.\begin{matrix} 1/2, 1/2 \\ 1 \end{matrix}\right| k^2\right).$$

Example: fast computation of π

[Chudnovsky^{2}87] Ramanujan-type series, faster convergence

$$\frac{1}{\pi} = \frac{1}{53360\sqrt{640320}} \sum_{n\geq 0} \frac{(-1)^n (6n)!(13591409 + 545140134n)}{n!^3 (3n)!(8 \cdot 100100025 \cdot 327843840)^n}.$$



Used in Maple & Mathematica. 1st order recurrence, it yields 14 correct digits per iteration. 4 billion digits [Chudnovsky^{2}94].

Baby-Steps/Giant-Steps

Problem ($N!$ mod p in less than N operations)

Naive: N arithmetic operations

Baby-Steps/Giant-Steps

Problem ($N!$ mod p in less than N operations)

Naive: N arithmetic operations

- Strassen 76: $\tilde{\mathcal{O}}(\sqrt{N})$.
  1. Compute $Q(x) = (x+1)\cdots(x+k)$ $\quad \tilde{O}(k)$;
  2. Evaluate $Q(0), Q(k), \ldots, Q(N-k)$ $\quad \tilde{O}(N/k)$;
  3. Compute their product $\quad O(N/k)$.
- Extends to matrix factorials in $\tilde{\mathcal{O}}(\sqrt{N})$ [Chudnovsky^{2}88];

Application: dimension of kernel of $C(N)C(N-1)\cdots C(1)$ over $\mathbb{Q}$

Probabilistic algorithm in $\tilde{O}(\sqrt{N})$ bit operations [BoClSa05].

Probability at least $1 - \frac{1}{2\log^2 N}$. Primes of size a bit more than $\log N$.

Examples of applications

- Deterministic factorization of integers, [Pollard74, Strassen76]:

$$\tilde{\mathcal{O}}\left(\sqrt[4]{N}\right) \quad \text{bit operations to factor } N$$

- Point counting on hyperelliptic curves using Cartier-Manin operator $\longrightarrow$ coefficient of X^{p-1} in $f^{(p-1)/2}$, where $f \in \mathbb{F}_p[X]$ [BoGaSc03].
- Fast detection of polynomial and rational solutions of differential equations [BoChSa05].

III Singularities of D-finite functions

Location of Singularities

$$\mathcal{L}y := a_0(x)y^{(d)}(x) + \cdots + a_d(x)y(x) = 0 \Leftrightarrow$$

$$(E) \quad Y'(x) = A(x)Y(x), \qquad Y = \begin{pmatrix} y \\ \vdots \\ y^{(d-1)} \end{pmatrix}, \quad A = \begin{pmatrix} 1 & & 0 \\ 0 & 1 & \\ -\frac{a_d}{a_0} & \cdots & -\frac{a_1}{a_0} \end{pmatrix}.$$

Theorem (Cauchy)

If $A(x)$ is analytic in a simply connected domain $R \subset \mathbb{C}$, then for $a \in R$, $\alpha \in \mathbb{C}^d$, (E) has a solution analytic in R s.t. $Y(a) = \alpha$.

Corollary

If $\mathcal{L}y(x) = 0$ and if ρ is a singularity of $y(x)$, then $a_0(\rho) = 0$. In particular, a D-finite function has only finitely many *singularities.*

Definition

Singularity at ∞: $y(1/x)$ singular at 0.

Indicial Polynomial

$$\mathcal{L}y := a_0(x)y^{(d)}(x) + \cdots + a_d(x)y(x) = 0. \qquad \text{(E)}$$

Idea: to every singularity ρ of $\mathcal{L}$, attach a polynomial P_ρ whose roots σ are the possible valuations of formal series solutions $y(x) = (x-\rho)^\sigma \sum_{n\geq 0} u_n^{(\rho)}(x-\rho)^n$ of $\mathcal{L}y = 0$ at ρ.

Definition

Indicial polynomial: $\mathcal{L}(x-\rho)^\sigma \sim P_\rho(\sigma)(x-\rho)^{\sigma+m}$ [Fuchs1868]

Proposition

If $\rho = 0$ is a singularity of $\mathcal{L}$, the sequence $\left(u_n^{(0)}\right)_n$ satisfies

$$b_r(n)u_{n+r}^{(0)} + \cdots + b_0(n)u_n^{(0)} = 0,$$

where $P_\rho(\sigma) = b_r(\sigma - r)$ and $P_\infty(\sigma) = b_0(\sigma)$.

Example

$$(2x+1)^3y''+(2x+1)(8x+3-4N(1+2x))y'+2N((4x+2)N-4x-1)y=0$$

$$\mathcal{L}(x^\sigma) =$$
$$\underbrace{\sigma(\sigma-1)}_{P_0(\sigma)}x^{\sigma-2}+\cdots+\underbrace{(8\sigma(\sigma-1)+16\sigma(1-N)+2N(4N-4))}_{P_\infty(\sigma)}x^{\sigma+1}$$

$$\underbrace{(n+3)(n+2)}_{P_0(n+3)}u_{n+3}+\cdots+8\underbrace{(n-N)(n-N+1)}_{P_\infty(n)}u_n=0$$

Classification of singularities

$$\mathcal{L}y := a_0(x)y^{(d)}(x) + \cdots + a_d(x)y(x) = 0. \qquad \text{(E)}$$

Theorem (Fabry1885)

At a singular point ρ, (E) admits a basis of formal solutions

- $\deg P = d$: *regular singular point.*

$$\Psi_i(z) = (z-\rho)^{\sigma_i} \sum_{j=0}^{d_i} \log^j(z-\rho)\, \underbrace{\Phi_{i,j}(z-\rho)}_{\text{convergent p. s.}}, \qquad P(\sigma_i) = 0.$$

- $\deg P < d$: *irregular singular point*

$$y_i(t) = \exp\Big(\underbrace{P_i(1/t)}_{\text{polynomial}}\Big)\, \underbrace{\Psi_i(t)}_{\text{as above}}, \qquad \underbrace{t^{\mu_i}}_{\mu_i\in\mathbb{N}^*} = (z-\rho).$$

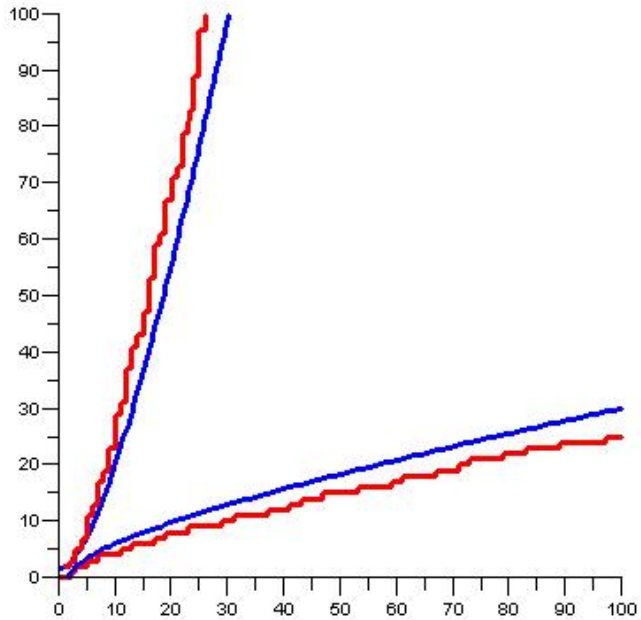
Algorithms for everything [Tournier87,vanHoeij97]
Incorporated in ESF: http://algo.inria.fr/esf [MeSa03]

Not Everything is D-finite

Analytic behaviour

- $\tan z$ is not D-finite;
- Bernoulli numbers are not D-finite ($\sum B_n z^n/n! = z/(e^z-1)$);
- sequences $\log n$, n^α ($\alpha \notin \mathbb{N}$), p_n not D-finite [FlGeSa05];

$$\pi(x) \sim \mathrm{Li}(x) + R(x) \Rightarrow p_n - nH_n \sim n \log\log n \Rightarrow \text{g.f.} \sim \frac{\log\log(1-z)}{(1-z)^2}$$



Not Everything is D-finite

Analytic behaviour

- $\tan z$ is not D-finite;
- Bernoulli numbers are not D-finite ($\sum B_n z^n/n! = z/(e^z-1)$);
- sequences $\log n$, n^α ($\alpha \notin \mathbb{N}$), p_n not D-finite [FlGeSa05];

Algebraic behaviour (mostly Galois theory)

- f and $1/f$ D-finite iff f'/f algebraic [HaSi85];
- f_n and $1/f_n$ D-finite iff f_n interlacing of hypergeometric sequences ($=$ rec. of order 1) [vdPSi97];
- f and $\exp \int f$ D-finite iff f algebraic;
- g algebraic of genus ≥ 1. f and $g \circ f$ D-finite iff f is algebraic. [Singer86]

IV Polynomial and rational solutions of LDEs

Motivation

- Indefinite hypergeometric summation [Gosper78]

$$\sum_{k=0}^{n} \frac{(3k)!}{k!(k+1)!(k+2)!27^k} = \frac{(81n^2+261n+200)(3n+2)!}{40(n+2)!(n+1)!n!27^n} - \frac{9}{2}$$

- Definite summation and integration [Zeilberger90, Chyzak00]

$$\sum_{n=0}^{\infty} J_{2n+1/2}(x) = \int_0^x \frac{\cos t}{\sqrt{2\pi t}}\, dt$$

- Liouvillian solutions of LDEs [Marotte1898, Kovacic86, Singer81,...]
- Hypergeometric solutions of LREs [Petkovšek90]
- Desingularization of LDEs and LREs [ChDuLeMaMiSa07]

They all

- need rational or polynomial solutions of LDEs or LREs;
- waste time when none exists.

Timings

$$(2x+1)^3y''+(2x+1)(8x+3-4N(1+2x))y'+2N((4x+2)N-4x-1)y=0$$

has no polynomial solution ... but it takes time to detect this.

N	ABP	New	New
2^{12}	62.59	0.44	0.03
2^{14}	4597.2	2.40	0.07
2^{16}	$>$ 4Gb	14.67	0.19
2^{22}		3060.1	2.54
	$\tilde{\mathcal{O}}(N^2)$	$\tilde{\mathcal{O}}(N)$	$\tilde{\mathcal{O}}(\sqrt{N})$
	deterministic		proba.

Timings

$$(2x+1)^3y''+(2x+1)(8x+3-4N(1+2x))y'+2N((4x+2)N-4x-1)y=0$$

has no polynomial solution ... but it takes time to detect this.

N	ABP	New	New
2^{12}	62.59	0.44	0.03
2^{14}	4597.2	2.40	0.07
2^{16}	$>$ 4Gb	14.67	0.19
2^{22}		3060.1	2.54
	$\tilde{\mathcal{O}}(N^2)$	$\tilde{\mathcal{O}}(N)$	$\tilde{\mathcal{O}}(\sqrt{N})$
	deterministic		proba.

Open problem: Polynomial complexity (in $\log N$).

Liouville (1833) did most of it!

$$a_0(x)y^{(d)}(x) + \cdots + a_d(x)y(x) = 0.$$

- Polynomial solutions:

  Si l'on se bornait à demander les intégrales entières, le problème n'offrirait aucune difficulté.

- Algorithm for rational solutions, later improved by Abramov *et alii*.

[BoCISa05]: better complexity (still exponential).

Basic Algorithm

Liouville: bound on degree and undeterminate coefficients

$$\begin{pmatrix} * & * & * & & & & \\ * & * & * & * & & & \\ & * & * & * & * & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & * & * & * & * \\ & & & & * & * & * \end{pmatrix}$$

Basic Algorithm

Liouville: bound on degree and undeterminate coefficients

$$\begin{pmatrix} * & * & * & & & & \\ * & * & * & * & & & \\ & * & * & * & * & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & * & * & * & * \\ & & & & * & * & * \end{pmatrix}$$

Abramov *et alii*: alternate view via recurrence

$$(n+3)(n+2)u_{n+3} + \cdots + 8(n-N)(n-N+1)u_n = 0$$

and basis of power series solutions of the LDE

$$1 + 0x + \cdots + *x^N + *x^{N+1} + *x^{N+2} + *x^{N+3} + O(x^{N+4})$$
$$0 + 1x + \cdots + *x^N + *x^{N+1} + *x^{N+2} + *x^{N+3} + O(x^{N+4})$$

Same Complexity

Basic Algorithm

Liouville: bound on degree and undeterminate coefficients

$$\begin{pmatrix} * & * & * & & & & \\ * & * & * & * & & & \\ & * & * & * & * & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & * & * & * & * \\ & & & & * & * & * \end{pmatrix}$$

Abramov *et alii*: alternate view via recurrence

$$(n+3)(n+2)u_{n+3} + \cdots + 8(n-N)(n-N+1)u_n = 0$$

and basis of power series solutions of the LDE

$$* x^{N+1} + * x^{N+2} + * x^{N+3}$$
$$* x^{N+1} + * x^{N+2} + * x^{N+3}$$

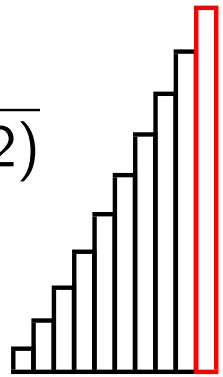
Binary Splitting for Polynomial Solutions

$$* + *x + \cdots + *x^N + *x^{N+1} + *x^{N+2} + *x^{N+3} + O(x^{N+4})$$

$$(n+3)(n+2)u_{n+3} + \cdots + 8(n-N)(n-N+1)u_n = 0$$

First order recurrence on vectors $U_n = {}^t(u_{n+3}, u_{n+2}, u_{n+1})$:

$$U_N = \underbrace{\begin{pmatrix} * & * & * \\ (N+3)(N+2) & 0 & 0 \\ 0 & (N+3)(N+2) & 0 \end{pmatrix}}_{C(N)} \frac{U_{N-1}}{(N+3)(N+2)}$$

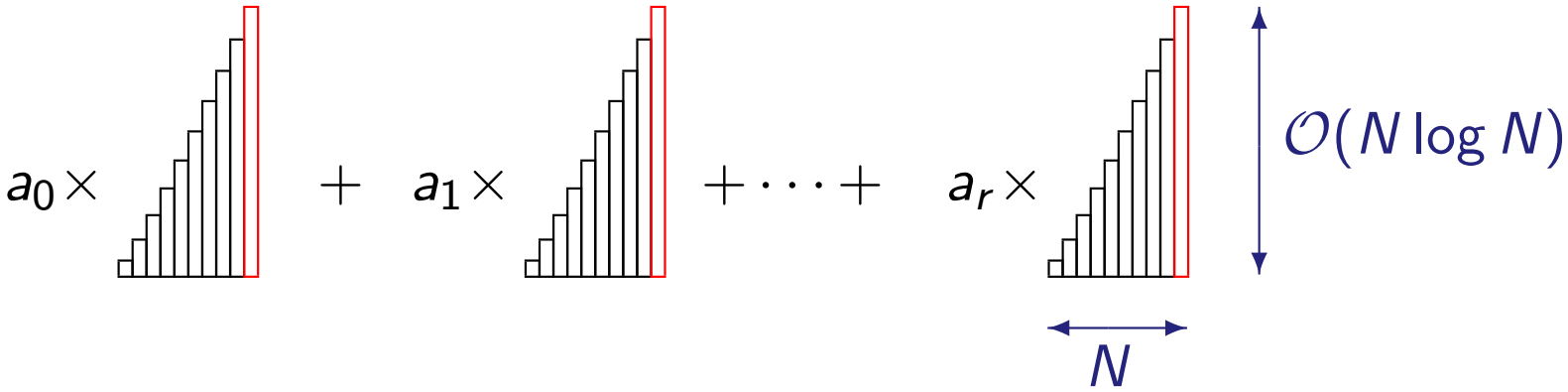


$$= \underbrace{C(N)\cdots C(-1)}_{\textbf{matrix factorial}} \frac{U_{-2}}{(N+2)(N+1)!^2}.$$

Complexity: like for $N!$.

Shape of Recurrent Sequences

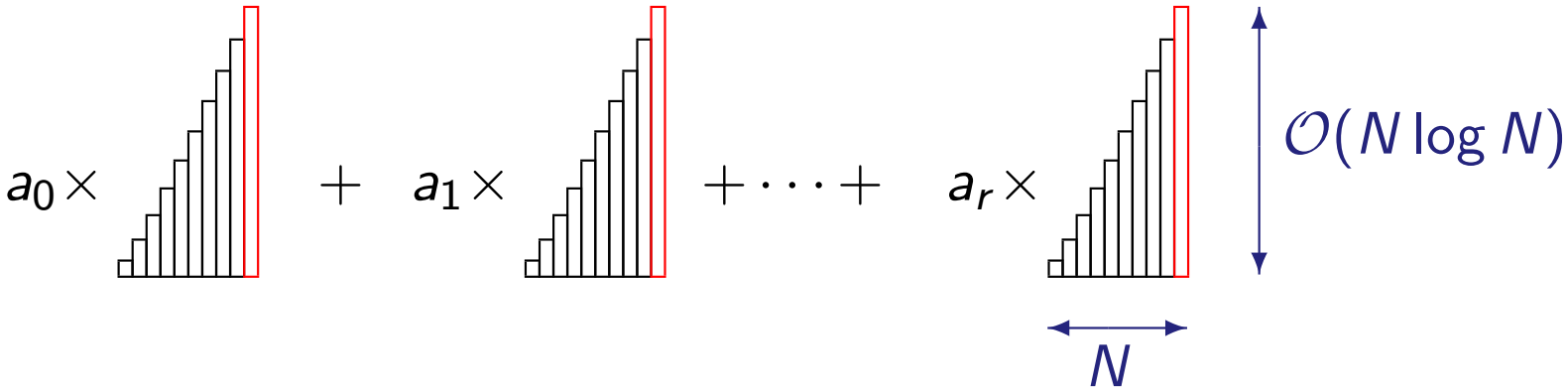
$$a_r(n)u_{n+r} + \cdots + a_0(n)u_n = 0, \qquad a_i \in \mathbb{Q}[n].$$



Total size N first terms: $\mathcal{O}(\max \text{size}\, a_i + N^2 \log N)$

Shape of Recurrent Sequences

$$a_r(n)u_{n+r} + \cdots + a_0(n)u_n = 0, \qquad a_i \in \mathbb{Q}[n].$$



Total size N first terms: $\mathcal{O}(\max \text{size}\, a_i + N^2 \log N)$

Definition (Compact Representation of a Polynomial Solution)

Linear recurrence on its coefficients + initial conditions
+ bound N on degree.

Data-structure of size $\mathcal{O}(\text{size ini. cond.} + \log N)$
for a polynomial of size $\tilde{\mathcal{O}}(\text{size ini. cond.} + N^2)$.

Operations on Compact Representations

Lemma (Classical)

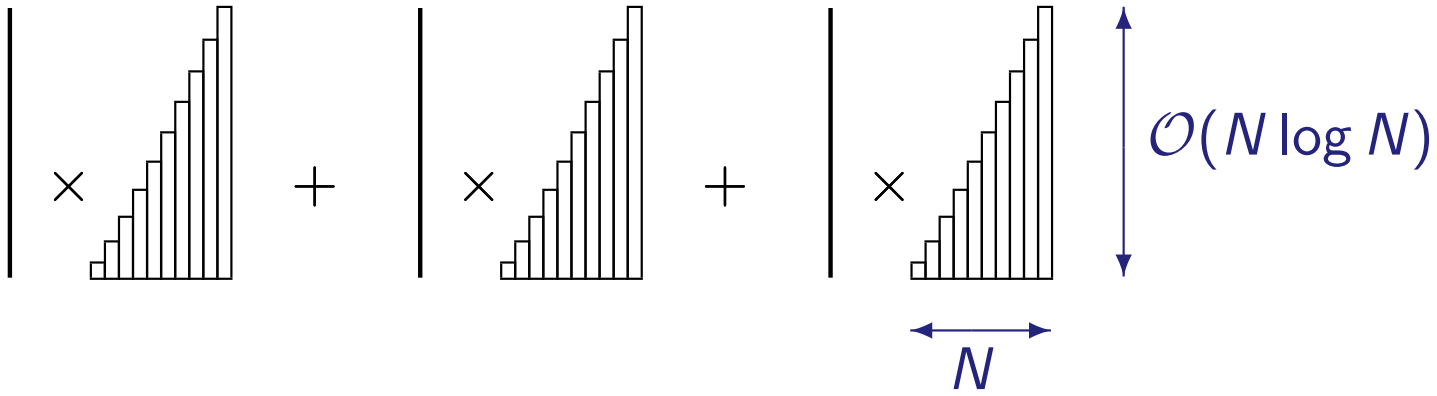
If u_n and v_n satisfy linear recurrences, so does $w_N := \sum_{n=0}^{N} u_n v_n$.

Corollary

P polynomial in compact representation, a algebraic number, then $P^{(k)}(a)$ can be computed in $\tilde{\mathcal{O}}(N)$ bit operations (with $k = \mathcal{O}(N)$).

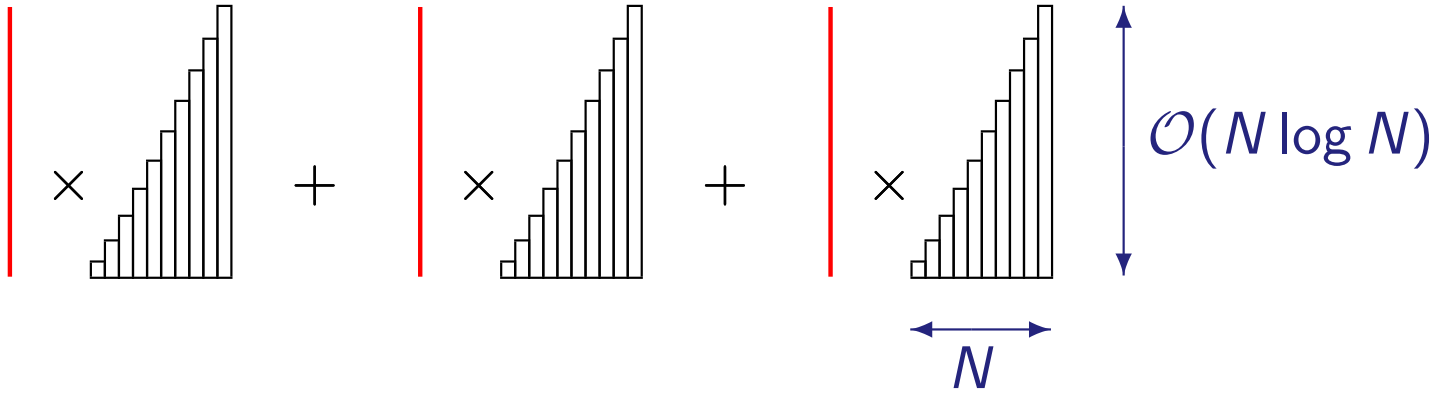
$\longrightarrow$ Compact representations can be evaluated, differentiated and shifted to another point efficiently.

Shape of Polynomial Solutions



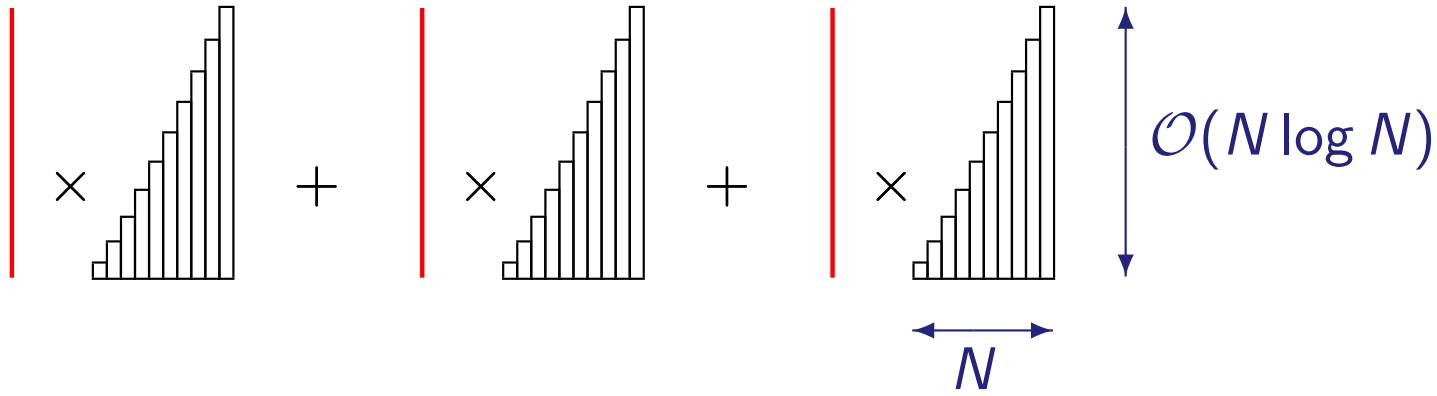
- Size of Solutions: $\mathcal{O}(N^2 \log N)$ bits
- Compact representation: $\mathcal{O}(N \log N)$ bits

Shape of Polynomial Solutions



- Size of Solutions: $\mathcal{O}(N^2 \log N)$ bits
- Compact representation: $\mathcal{O}(N \log N)$ bits

Shape of Polynomial Solutions



- Size of Solutions: $\mathcal{O}(N^2 \log N)$ bits
- Compact representation: $\mathcal{O}(N \log N)$ bits

Theorem (BoCISa05)

One can compute the compact representation and the degree of polynomial solutions in $\tilde{\mathcal{O}}(N)$ bit operations. Knowing the degree D, the expanded polynomial is computed in $\tilde{\mathcal{O}}(D^2)$ bit ops.

Quasi-optimal!

Probabilistic Algorithm

Theorem (BoCISa05)

Given $c \geq 0$, one can compute the degrees of polynomial solutions with $\tilde{\mathcal{O}}(\sqrt{N})$ bit operations. The result is correct with probability $\geq 1 - 1/(2\log^c N)$.

Probabilistic Algorithm

Theorem (BoCISa05)

Given $c \geq 0$, one can compute the degrees of polynomial solutions with $\tilde{\mathcal{O}}(\sqrt{N})$ bit operations. The result is correct with probability $\geq 1 - 1/(2\log^c N)$.

Idea:

1. Compute the matrix factorial
   – with only $\tilde{\mathcal{O}}(\sqrt{N})$ operations
   – modulo a prime of bit size only $\mathcal{O}(\log N)$
2. Bound the probability that the rank drops.

Rational Solutions of LDE

$$\mathcal{L}y(x) = a_0(x)y^{(d)}(x) + \cdots + a_d(x)y(x) = 0.$$

- Cauchy: singular points only at roots of a_0.
- Indicial polynomial $P_\rho(\sigma)$: $\mathcal{L}(x-\rho)^\sigma \sim P_\rho(\sigma)(x-\rho)^{\sigma+m}$.

$$P_\rho(n+r)u_{n+r} + \cdots + P_\infty(n)u_n = 0$$

$\longrightarrow$ (Exponential) bound on orders of poles and degree;

$\longrightarrow$ Rational solutions [Liouville1833,Abramov89]: patch up local polar behaviours

$$y(x) := \frac{\tilde{y}(x)}{\prod_{\substack{a_0(\rho)=0,\\ P_\rho(-N_\rho)=0,\\ N_\rho\in\mathbb{N}}} (x-\rho)^{N_\rho}}.$$

Compact Rational Solutions of LDEs

1. Compute the negative integer roots $-N_\rho < -N'_\rho < -N''_\rho < \cdots$ of the indicial polynomials P_ρ;
2. Change the unknown function into $Y(x)/\prod(x-\rho)^{N_\rho}$ and normalize equation (no explosion);
3. Compute a compact representation of this numerator $Y(x)$;
4. For each ρ, divide $Y(x)$ by its gcd with $(x-\rho)^{N_\rho}$:
   1. check whether $Y^{(i)}(\rho) = 0$, for $i \in \{N'_\rho, N''_\rho, \dots\}$;
   2. if so, translate the compact representation at ρ and shift its indices by i.

All in $\tilde{O}(N_\infty + \sum_\rho N_\rho)$.

Compact Rational Solutions of LDEs

1. Compute the negative integer roots $-N_\rho < -N'_\rho < -N''_\rho < \cdots$ of the indicial polynomials P_ρ;
2. Change the unknown function into $Y(x)/\prod(x-\rho)^{N_\rho}$ and normalize equation (no explosion);
3. Compute a compact representation of this numerator $Y(x)$;
4. For each ρ, divide $Y(x)$ by its gcd with $(x-\rho)^{N_\rho}$:
   1. check whether $Y^{(i)}(\rho) = 0$, for $i \in \{N'_\rho, N''_\rho, \dots\}$;
   2. if so, translate the compact representation at ρ and shift its indices by i.

All in $\tilde{O}(N_\infty + \sum_\rho N_\rho)$.

The result can then be expanded if desired.