# Fast algorithms for the $p$-curvature of differential operators

Alin Bostan

joint work with
Xavier Caruso (Univ. Rennes 1) and Éric Schost (Univ. Western Ontario)

Journées Holonomes
Grenoble, February 12, 2014

# Introduction

# Main objects & Aim

- $k$ = a field with prime characteristic $p$, typically $\mathbb{F}_p$
- $k(x)\langle\partial\rangle$ = the non-commutative (right-) Euclidean algebra of linear differential operators $L = \ell_0(x) + \ell_1(x)\partial + \cdots + \ell_r(x)\partial^r$

*Def*: $p$-curvature $\mathbf{A}_p(L)$ of $L$ = the matrix in $\mathscr{M}_r(k(x))$ whose $j$-th column contains the coefficients of $\partial^{p+j} \bmod L$ for $0 \le j < r$

Aim: design efficient algorithms for computing

- the *p-curvature* $\mathbf{A}_p(L)$ of $L$
- its *characteristic polynomial* $\chi(\mathbf{A}_p(L))$
- the *solution space* of $L$

- Efficiency = complexity estimates with a low exponent in $p$
- Complexity is measured in number of arithmetic operations in $k$

# Basics on differential equations in characteristic $p$

- Main differences between characteristic zero and $p$

1. (Honda 1981) solutions are simpler in characteristic $p$

$$\dim_{k(x^p)} \mathcal{S}_L(k[x]) = \dim_{k(x^p)} \mathcal{S}_L(k(x)) = \dim_{k((x^p))} \mathcal{S}_L(k[[x]])$$

2. Cauchy's theorem does not hold: the common dimension $\dim \mathcal{S}_L$ of the solution spaces is generally $< r = \mathrm{ord}(L)$

Example: $y' = y$ has no solution in $k[[x]]$

- Connection between solutions and $p$-curvature

*Theorem.* (Katz & Cartier 1970) $\mathrm{rank}(\mathbf{A}_p(L)) = r - \dim(\mathcal{S}_L)$

$\longrightarrow$ $p$-curvature measures to what extent $\dim(\mathcal{S}_L)$ is close to $r$

# Two famous statements on $p$-curvatures

*Def.* A power series $\sum_{n\geq 0} \frac{a_n}{b_n} x^n$ in $\mathbb{Q}[[x]]$ is called a *G-series* if it is (a) D-finite; (b) analytic at $x=0$; (c) $\exists C>0$, $\mathrm{lcm}(b_0, \ldots, b_n) \leq C^n$.

Examples: ${}_2F_1\left(\begin{matrix}\alpha\ \beta\\ \gamma\end{matrix}\middle| x\right)$, $\alpha, \beta, \gamma \in \mathbb{Q}$; algebraic functions (Eisenstein).

*Chudnovsky's theorem (1985)* The minimal-order operator $\Gamma \in \mathbb{Q}[x]\langle\partial\rangle$ annihilating a $G$-series is *globally nilpotent*: for almost all prime numbers $p$, the $p$-curvature $\mathbf{A}_p(\Gamma)$ is nilpotent.

Examples: $x(1-x)\partial^2 + (\gamma - (\alpha+\beta+1)x)\partial - \alpha\beta x$; algebraic resolvents.

*Grothendieck's conjecture* $\Gamma(f)=0$ with $\Gamma \in \mathbb{Q}[x]\langle\partial\rangle$ has a basis of algebraic solutions over $\mathbb{Q}(x)$ iff $\mathbf{A}_p(\Gamma)=0$ for almost all primes $p$

# $p$-curvature in Computer Algebra

- van der Put 1995: $p$-curvature publicised in computer algebra, as a tool for factoring operators in $k(x)\langle\partial\rangle$
- Cluzeau 2003: first complexity analysis and implementation of van der Put's algorithms; extension to systems
- Cluzeau, van Hoeij 2004: polynomial solutions mod $p$ and $p$-curvature used as filters in modular algorithms for $\mathbb{Q}(x)\langle\partial\rangle$

- Concrete applications:
  - enumerative combinatorics (classification of lattice walks)
  - statistical physics (square lattice Ising model)

## Why $p$-curvature is very useful in concrete applications

• Power series arising in Combinatorics / Physics often have integer coefficients (up to scaling), by design

• E.g. ordinary generating series in counting problems, or multiple integrals of algebraic functions with parameters

• Sometimes, they are even D-finite by design (e.g. integrals), sometimes not (e.g. solutions of functional equations)

• To conjecture D-finiteness, one common computational technique is *differential guessing*: one guesses a plausible annihilating differential operator from the first terms of the power series

• One way to empirically certify guessed operators is to *look at their p-curvatures* for random (large) primes $p$

• If they are nilpotent (or have a large valuation), then the guessed operator is very probably correct, because of Chudnovsky's theorem

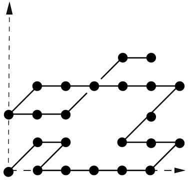
• If, in addition, they are even zero, then the power series is very probably algebraic, because of Grothendieck's conjecture

## Combinatorial application: Gessel's conjecture

- Gessel walks: walks in $\mathbb{N}^2$ using only steps in $\mathcal{S} = \{\nearrow, \swarrow, \leftarrow, \rightarrow\}$
- $g(i, j, n)$ = number of walks from $(0, 0)$ to $(i, j)$ with $n$ steps in $\mathcal{S}$

**Question**: Nature of the generating function

$$G(x, y, t) = \sum_{i,j,n=0}^{\infty} g(i, j, n)\, x^i y^j t^n \ \in \mathbb{Q}[[x, y, t]]$$



*Theorem.* (B. & Kauers 2010) $G(x, y, t)$ is an algebraic function.†

$\rightarrow$ Effective, computer-driven discovery and proof

$\rightarrow$ Key step in discovery: $p$-curvature computation of two 11th order (guessed) differential operators for $G(x, 0, t)$, and $G(0, y, t)$

†Minimal polynomial $P(x, y, t, G(x, y, t)) = 0$ has $> 10^{11}$ terms; $\approx$30Gb (!)

## Previous work

① $p$-curvature: generic size $\Theta(p)$, but complexity $\mathcal{O}(p^2)$

▶ Main difficulty: non-commutativity of $k(x)\langle\partial\rangle$ prevents from using binary powering techniques for $\mathbf{A}_p(L)$ via $\partial^p$ mod $L$

• Katz 1982: first algorithm, based on the matrix recurrence

$$\mathbf{A}_1 = \mathbf{A}, \quad \mathbf{A}_{k+1} = \mathbf{A}'_k + \mathbf{A} \cdot \mathbf{A}_k,$$

where $\mathbf{A} \in \mathscr{M}_r(k(x))$ is the companion matrix associated to $L$

• van der Put, Cluzeau: variants, all of complexity $\mathcal{O}(p^2)$

② Its characteristic polynomial: required computation of $\mathbf{A}_p$ itself

③ Polynomial solutions mod $p$:

• Cluzeau 2003: quadratic degree bound for elements in $\mathcal{S}_L(k[x])$

• Honda 1981, Dwork 1982: linear bound when $r = 2$, or $\mathbf{A}_p = 0$

• Cluzeau 2003: general algorithm of complexity $\mathcal{O}(p^3)$; different $\mathcal{O}(p^2)$ algorithm in the special case $\mathbf{A}_p = 0$

# New results

1. on computing the $p$-curvature $\mathbf{A}_p$

(1.a) for first order operators in time $\mathcal{O}(\log(p))$

(1.b) for certain second order operators in time $\tilde{\mathcal{O}}(p)$

(1.c) for arbitrary operators in time $\tilde{\mathcal{O}}(p^{1.79})$

(1.d) deciding nullity of $\mathbf{A}_p$ for arbitrary operators in time $\tilde{\mathcal{O}}(p)$

2. on computing the characteristic polynomial of $\mathbf{A}_p$

(2.a) for arbitrary operators in time $\tilde{\mathcal{O}}(\sqrt{p})$

3. on the space $\mathcal{S}_L$ of polynomial solutions

(3.a) degree bound linear in $p$ for all elements in a basis of $\mathcal{S}_L$

(3.b) testing if $\mathcal{S}_L = 0$ in time $\tilde{\mathcal{O}}(\sqrt{p})$

(3.c) computing a whole basis of $\mathcal{S}_L$ in time $\tilde{\mathcal{O}}(p)$

# Computing the $p$-curvature

## $p$-curvature of 1st order operators

Specific features of 1st order operators $L = \partial - u$ in $k(x)\langle\partial\rangle$

- $p$-curvature admits a *closed form expression*:

$$\mathbf{A}_p(L) = u^{(p-1)} + u^p \qquad \text{(van der Put, 1995)}$$

- $p$-curvature is *sparse*: numerator/denominator have $\mathcal{O}(1)$ terms:

$\mathbf{A}_p(L)$ is the $p$-th power of the rational function $f = \left(u^{(p-1)}\right)^{\frac{1}{p}} + u$.

*Theorem* (BoSc'09) $\mathbf{A}_p(L)$ *can be computed in time* $\mathcal{O}(\log(p))$.

Idea: If $u = \sum_{i\geq 0} a_i x^i$, then $\left(u^{(p-1)}\right)^{\frac{1}{p}} = -\sum_{i\geq 1} a_{ip-1} x^{i-1}$ (Wilson)

$\longrightarrow$ it is sufficient to compute by binary powering the $\mathcal{O}(1)$ terms $a_{p-1}, a_{2p-1}, \dots, a_{\deg(u)p-1}$ of the recurrent sequence $(a_n)_{n\geq 0}$.

## $p$-curvature of arbitrary operators

*Theorem.* (BoSc'09) The $p$-curvature of any $L$ in $k[x]\langle\partial\rangle$ can be computed in subquadratic time $\tilde{\mathcal{O}}(p^{1+\frac{\omega}{3}}) \subset \mathcal{O}(p^{1.79})$.

If $\mathbf{A} = \mathrm{CompanionMatrix}(L)$ and $\Lambda = \partial + \mathbf{A}$, then $\mathbf{A}_p = \Lambda^{p-1}(\mathbf{A})$

---

① Compute $\Gamma = \Lambda^k$ by binary powering.

Basic operation: product in bidegree $(k, k)$ in $k(x)\langle\partial\rangle$.

Cost: $\mathcal{O}(k^\omega)$ (B., Chyzak & Le Roux'08)

② Compute $\mathbf{A}_{(1)} = \mathbf{A},\ \mathbf{A}_{(i)} = \Gamma\mathbf{A}_{(i-1)},\ i = 2, \dots, \ell = (p-1)/k$.

Basic operation: $L(f)$ with $\mathrm{bideg}_{(x,\partial)}(L) = (k, k)$ and $\deg(f) \le ik$.

Cost: $\tilde{\mathcal{O}}(\ell^{\omega-1}k^2)$ (see next slide)

③ Return $\mathbf{A}_p = \mathbf{A}_{(\ell)}$.

---

Total cost: $\tilde{\mathcal{O}}(p^{1+\frac{\omega}{3}})$ obtained for $k \approx p^{2/3}$.

# Fast evaluation of differential operators

*Theorem.* Given $L \in k[x]\langle\partial\rangle$ of bidegree $(k, k)$ and $f \in k[x]$ of degree $ik$, $(i \leq s := \sqrt{k})$, one can compute $Lf$ in time $\tilde{\mathcal{O}}(i^{\omega-2}k^2)$.

*Algo* [baby steps / giant steps strategy inspired by Brent-Kung'78]

① (baby steps) Compute $f_0 = f, \ f_1 = \partial f, \ \dots, \ f_{s-1} = \partial^{s-1} f$

② (rewriting) Cut $L$ into $s$ slices of bidegree $(k, s)$ in $(x, \partial)$:

$$L = L_0 + \partial^s L_1 + \cdots + \partial^{(s-1)s} L_{s-1}$$

③ (recombination) Deduce $L_0 f, \dots, L_{s-1} f$ at once by a product of polynomial matrices of sizes $(s, s) \times (s, i)$ and degree $k$

④ (giant steps) Compute and return $Lf = \sum_{0 \leq j < s} \partial^{js} L_j f$

*Cost*: $\tilde{\mathcal{O}}(ik^{3/2})$ for ① and ④; $\tilde{\mathcal{O}}(k^2)$ for ② and $\tilde{\mathcal{O}}(i^{\omega-2}k^2)$ for ③

# Computing polynomial solutions

# Computing polynomial solutions (I)

- $\mathcal{S}_L$ = the $k(x^p)$-vector space of polynomial solutions of $Lf = 0$
- $\mathcal{G}$ = the $k$-vector space $\mathcal{S}_L \cap k[x]_{<pd}$ where $d = \max(\deg(\ell_i))$

*Theorem.* (BoSc'09) $\mathcal{S}_L$ admits a $k(x^p)$-basis included in $\mathcal{G}$.

*Algorithm* for computing $\mathcal{S}_L$:

---

① Decide if $\mathcal{S}_L = 0$ ($\Leftrightarrow$ decide if $\mathcal{G} = 0$). If so, stop.

② If not, compute a $k$-basis $(f_1, \ldots, f_k)$ of $\mathcal{G}$.

③ $(f_1, \ldots, f_k)$ generates $\mathcal{S}_L$ over $k(x^p)$. Extract a basis.

---

Cost: $\tilde{\mathcal{O}}(\sqrt{p})$ for ① and $\tilde{\mathcal{O}}(p)$ for ② and ③

*Corollary.* One can decide nullity of $\mathbf{A}_p(L)$ in time $\tilde{\mathcal{O}}(p)$.

# Computing polynomial solutions (II)

*Pb*: Compute an $k$-basis of sols $f = \sum_{i=0}^{pd-1} c_i x^i \in k[x]$ of $Lf = 0$.

- Band-diagonal linear system (S1) of size $\mathcal{O}(p)$ and width $\mathcal{O}(1)$
- Technical difficulty: some rightmost band elements can be zero!

*Algorithm* [generalization of (ABP1995) & (BCluzeauSalvy2005)]

① From (S1), deduce an equivalent system (S2) of size $\mathcal{O}(1)$

Basic operation: *matrix factorial* $C(p-1)\cdots C(r)$

Cost: $\tilde{\mathcal{O}}(\sqrt{p})$ (Chudnovsky$^2$ 1987)

② From a basis of (S2), deduce a basis of (S1)

Basic operation: forward substitution

Cost: $\mathcal{O}(p)$

# Example

$$L = (5x^2+4)\partial^2 + (4x^2+6x+5)\partial + 2x + 2 \in \mathbb{F}_7[x]\langle\partial\rangle$$

Polynomial solution $f = \sum_{i=0}^{7\cdot 2-1} c_i x^i$ in $\mathbb{F}_7[x]$ s.t. $Lf = 0$:

$$(S1)\left\{\begin{array}{c}
2c_0+5c_1+c_2=0,\\
2c_0+c_1+3c_2+3c_3=0,\\
6c_1+3c_2+c_3+6c_4=0,\\
3c_2+c_3+6c_4+3c_5=0,\\
2c_4+4c_5+c_6=0,\\
4c_4+6c_5+2c_6=0,\\
c_5+6c_6=0,\\
5c_6+2c_7+5c_8+c_9=0,\\
2c_7+c_8+3c_9+3c_{10}=0,\\
6c_8+3c_9+c_{10}+6c_{11}=0,\\
3c_9+c_{10}+6c_{11}+3c_{12}=0,\\
2c_{11}+4c_{12}+c_{13}=0,\\
4c_{11}+6c_{12}+2c_{13}=0,\\
c_{12}+6c_{13}=0,\\
5c_{13}=0.
\end{array}\right.
\Leftrightarrow
\begin{bmatrix}
2&5&1&&&&&&&&&&&\\
2&1&3&3&&&&&&&&&&\\
0&6&3&1&6&&&&&&&&&\\
&0&3&1&6&3&&&&&&&&\\
&&0&0&2&4&1&&&&&&&\\
&&&0&4&6&2&0&&&&&&\\
&&&&0&1&6&0&0&&&&&\\
&&&&&0&5&2&5&1&&&&\\
&&&&&&0&2&1&3&3&&&\\
&&&&&&&0&6&3&1&6&&\\
&&&&&&&&0&3&1&6&3&\\
&&&&&&&&&0&0&2&4&1\\
&&&&&&&&&&0&4&6&2\\
&&&&&&&&&&&0&1&6\\
&&&&&&&&&&&&0&5
\end{bmatrix}
\times
\begin{bmatrix} c_0\\ c_1\\ c_2\\ c_3\\ c_4\\ c_5\\ c_6\\ c_7\\ c_8\\ c_9\\ c_{10}\\ c_{11}\\ c_{12}\\ c_{13}\end{bmatrix} = 0$$

➥ Rewriting the equations in red using the unknowns in blue yields

$$c_4 = 5c_1,\ c_5 = 2c_1,\ c_6 = 3c_1,\ c_{11} = 5c_8 + 5c_1,\ c_{12} = 2c_8,\ c_{13} = 3c_8 + 4c_1$$

➥ Plugging them back into the red equations gives

$$(S2): \qquad 3c_1 = 0, 6c_1 = 0, 3c_8 = 0, c_8 + 6c_1 = 0, 6c_8 + 3c_1 = 0$$

➥ $\dim(S1) = \dim(S2) = 2$ and Basis(S1) is obtained by subst. from Basis(S2) $= \{(c_0, c_1, c_7, c_8) = (1, 0, 0, 0), (c_0, c_1, c_7, c_8) = (0, 0, 1, 0)\}$

# Application: deciding nilpotency of the $p$-curvature for second order operators

*Lemma* One can compute the trace of $\mathbf{A}_p(L)$ in $\mathcal{O}(\log(p))$.

*Proof*: If $L = \ell_0(x) + \ell_1(x)\partial + \cdots + \ell_r(x)\partial^r$, then

$$\operatorname{trace}(\mathbf{A}_p(L)) = \mathbf{A}_p\big(\ell_r(x)\partial + \ell_{r-1}(x)\big) \qquad \text{(Katz, 1982)}$$

*Lemma* One can decide if $\mathbf{A}_p(L)$ is invertible in $\tilde{\mathcal{O}}(\sqrt{p})$.

*Proof*: By (Cartier & Katz 1970): $\det(\mathbf{A}_p(L)) = 0$ iff $\dim(\mathcal{S}_L) > 0$.

*Theorem* (BoSc'09) If $\operatorname{ord}(L) = 2$, one can decide nilpotency of $\mathbf{A}_p(L)$ in time $\tilde{\mathcal{O}}(\sqrt{p})$.

*Proof*: $\mathbf{A}_p = \mathbf{A}_p(L)$ is nilpotent iff $\operatorname{trace}(\mathbf{A}_p)$ and $\det(\mathbf{A}_p) = 0$.

# Computing the characteristic polynomial of the $p$-curvature

# Useful operator rings

- $k[x]\langle\partial^{\pm 1}\rangle$ and $k(x)\langle\partial^{\pm 1}\rangle$ are rings, with multiplication

$$\partial^{-1} f = \sum_{i=0}^{p-1} (-1)^i f^{(i)}\, \partial^{-i-1}, \quad \text{for all } f \in k(x).$$

- $k[\theta]\langle\partial^{\pm 1}\rangle$ and $k(\theta)\langle\partial^{\pm 1}\rangle$ are rings, with multiplication

$$\partial^i g(\theta) = g(\theta + i)\, \partial^i, \quad \text{for all } i \in \mathbb{Z} \text{ and } g \in k(\theta).$$

- Isomorphism of $k$-algebras

$$\begin{array}{rcl} k[x]\langle\partial^{\pm 1}\rangle & \rightleftarrows & k[\theta]\langle\partial^{\pm 1}\rangle \\ x & \mapsto & \theta\partial^{-1} \\ x\partial & \leftarrow\!\shortmid & \theta \\ \partial^{\pm 1} & \leftrightarrow & \partial^{\pm 1} \end{array}$$

- The central element $\theta^p - \theta$ corresponds to $x^p\partial^p$, since

$$\theta^p = \sum_{k=1}^{p} \left\{ {p \atop k} \right\} x^k \partial^k, \quad \text{and} \quad p \text{ divides } \left\{ {p \atop k} \right\} \text{ for } 1 < k < p.$$

## $p$-curvature, revisited

*Recall*: Given $L$ in $k(x)\langle\partial\rangle$ of degree $r$ in $\partial$, $\mathbf{A}_p(L)$ is the matrix of $\partial^p$ acting on $k(x)\langle\partial\rangle/k(x)\langle\partial\rangle L$ w.r.t. the basis $(1, \partial, \dots, \partial^{r-1})$.

- $\partial^p$ is $k(x)$-linear, since

$$\partial^p(fV) = \sum_{j=0}^{p} \binom{p}{j} f^{(j)} \partial^{p-j} V, \quad \text{and } p \text{ divides } \binom{p}{j} \text{ for } 1 < j < p.$$

- The coefficients of the characteristic polynomial

$$\chi(\mathbf{A}_p(L))(z) = \det(z \cdot \mathrm{Id} - \mathbf{A}_p(L))$$

belong to $k(x^p)$.

*Def*: Given $L$ in $k(x)\langle\partial\rangle$, define

$$\Xi_{x,\partial}(L) = \mathrm{lc}(L)^p \cdot \chi(\mathbf{A}_p(L))(\partial^p)$$

- By multiplicativity, $\Xi_{x,\partial}$ can be extended to $k(x)\langle\partial^{\pm 1}\rangle$.
- $\Xi_{x,\partial}(L)$ belongs to the centre $k(x^p)[\partial^{\pm p}]$ of $k(x)\langle\partial^{\pm 1}\rangle$.

# A simpler $p$-curvature

*Def*: Given $L$ in $k(\theta)\langle\partial\rangle$ of degree $r$ in $\partial$, let $\mathbf{B}_p(L)$ be the matrix of $\partial^p$ acting on $k(\theta)\langle\partial\rangle/k(\theta)\langle\partial\rangle L$ w.r.t. the basis $(1, \partial, \ldots, \partial^{r-1})$.

*Theorem* (BoCaSc'14) Let $L \in k(\theta)\langle\partial\rangle$ and let $\mathbf{B}(\theta) \in \mathscr{M}_r(k(\theta))$ denote its companion matrix. Then:

$$\mathbf{B}_p(L) = \mathbf{B}(\theta) \cdot \mathbf{B}(\theta+1) \cdots \mathbf{B}(\theta+p-1).$$

- This is the analogue of Katz's formula for the usual $p$-curvature
- Computation of $\mathbf{B}_p(L)$ in time $\tilde{\mathcal{O}}(\sqrt{p})$ via *matrix factorials*.

*Def*: Given $L$ in $k(\theta)\langle\partial\rangle$, define

$$\Xi_{\theta,\partial}(L) = \mathrm{lc}(L)(\theta) \cdots \mathrm{lc}(L)(\theta+p-1) \cdot \chi(\mathbf{B}_p(L))(\partial^p)$$

- By multiplicativity, $\Xi_{\theta,\partial}$ can be extended to $k(\theta)\langle\partial^{\pm 1}\rangle$.
- $\Xi_{\theta,\partial}(L)$ belongs to the centre $k(\theta^p-\theta)[\partial^{\pm p}]$ of $k(\theta)\langle\partial^{\pm 1}\rangle$.

# Relation between the two $p$-curvatures

*Theorem* (BoCaSc'14) The following diagram commutes:

$$\begin{array}{ccc} k[\theta]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Xi_{\theta,\partial}} & k[\theta^p - \theta][\partial^{\pm p}] \\ {\scriptstyle \theta \mapsto x\partial}\big\downarrow{\scriptstyle \sim} & & {\scriptstyle \sim}\big\downarrow{\scriptstyle \theta^p - \theta \mapsto x^p\partial^p} \\ k[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Xi_{x,\partial}} & k[x^p][\partial^{\pm p}] \end{array}$$

*"Proof"*: $k[x]\langle\partial^{\pm 1}\rangle$ and $k[\theta]\langle\partial^{\pm 1}\rangle$ are *Azumaya algebras*, and thus isomorphic to *matrix algebras* (after an étale extension), and thus endowed with *reduced norm maps* (Revoy'73, Knus-Ojanguren'74)

*Corollary* (BoCaSc'14) $\Xi_{x,\partial}(L)$, and thus $\chi(\mathbf{A}_p(L))$, can be computed in time $\tilde{\mathcal{O}}(\sqrt{p})$.

# Implementation and timings

- For random linear differential operators of degrees $(d, r)$ in $k[x]\langle\partial\rangle$

| | $p$ | | | | | | |
|---|---|---|---|---|---|---|---|
| | **83** | **281** | **983** | **3 433** | **12 007** | **42 013** | **120 011** |
| $d = 5$, $r = 5$ | 0.11 s | 0.26 s | 0.75 s | 1.95 s | 5.09 s | 12.43 s | 33.78 s |
| $d = 5$, $r = 8$ | 0.19 s | 0.47 s | 1.32 s | 3.43 s | 9.20 s | 22.55 s | 65.25 s |
| $d = 5$, $r = 11$ | 0.26 s | 0.66 s | 1.85 s | 5.01 s | 14.68 s | 37.91 s | 104.86 s |
| $d = 5$, $r = 14$ | 0.37 s | 0.86 s | 2.38 s | 6.61 s | 20.52 s | 59.47 s | 154.76 s |
| $d = 5$, $r = 17$ | 0.52 s | 1.21 s | 3.26 s | 8.29 s | 24.18 s | 76.81 s | 234.28 s |
| $d = 5$, $r = 20$ | 0.76 s | 1.74 s | 4.67 s | 11.93 s | 33.88 s | 109.02 s | 298.72 s |
| $d = 8$, $r = 20$ | 1.12 s | 2.41 s | 6.69 s | 18.86 s | 56.24 s | 239.49 s | 881.45 s |
| $d = 11$, $r = 20$ | 1.96 s | 4.33 s | 10.42 s | 30.87 s | 92.84 s | 388.50 s | 922.34 s |
| $d = 14$, $r = 20$ | 3.05 s | 6.11 s | 14.45 s | 45.53 s | 141.81 s | 507.89 s | 1224.98 s |
| $d = 17$, $r = 20$ | 5.26 s | 9.19 s | 20.85 s | 56.83 s | 195.74 s | 699.08 s | 1996.87 s |
| $d = 20$, $r = 20$ | 7.76 s | 13.94 s | 28.40 s | 82.43 s | 240.47 s | 889.48 s | 2419.56 s |

- For operators with physical relevance: e.g., $\phi_H^{(5)}$ in $(\mathbb{Z}/27449\,\mathbb{Z})[x]\langle\partial\rangle$, of degree $(108, 28)$ in $(x, \partial)$ [Maillard et al. 2007]

$\longrightarrow$ high valuation (17) of $\Xi_{x,\partial}(\phi_H^{(5)})$ agrees with the empirical prediction that the (globally nilpotent) minimal-order operator for $\phi_H^{(5)}$ has order 17.

$\longrightarrow$ 27449-curvature itself (size 28, deg $\approx 3 \cdot 10^6$) impossible to compute!

# Matrix factorials

## Fast multiplication and division of power series

### [Schönhage-Strassen, 1971] and [Sieveking-Kung, 1972]

Schönhage-Strassen, 1971: FFT-multiplication in $k[x]_{<N}$ in $\tilde{\mathcal{O}}(N)$

Sieveking-Kung, 1972: To compute the reciprocal of $f \in k[[x]]$, use Newton iteration:

$$g_0 = \frac{1}{f_0} \quad \text{and} \quad g_{\kappa+1} = g_\kappa + g_\kappa(1 - fg_\kappa) \quad \text{mod } x^{2^{\kappa+1}} \quad \text{for } \kappa \geq 0$$

$$\mathrm{R}(N) = \mathrm{R}(N/2) + \tilde{\mathcal{O}}(N) \quad \Longrightarrow \quad \mathrm{R}(N) = \tilde{\mathcal{O}}(N)$$

Corollary: Division of power series at precision $N$ in $\tilde{\mathcal{O}}(N)$

# Application: fast polynomial Euclidean division

## [Strassen, 1973]

Given $F, G \in k[x]_{\leq N}$, compute $(Q, R)$ in division $F = QG + R$

Schoolbook algorithm: $\mathcal{O}(N^2)$

Better idea: look at $F = QG + R$ from the infinity: $Q \sim_{+\infty} F/G$

Formally: Let $N = \deg(F)$, $n = \deg(G)$, then $\deg(Q) = N - n$, $\deg(R) < n$ and

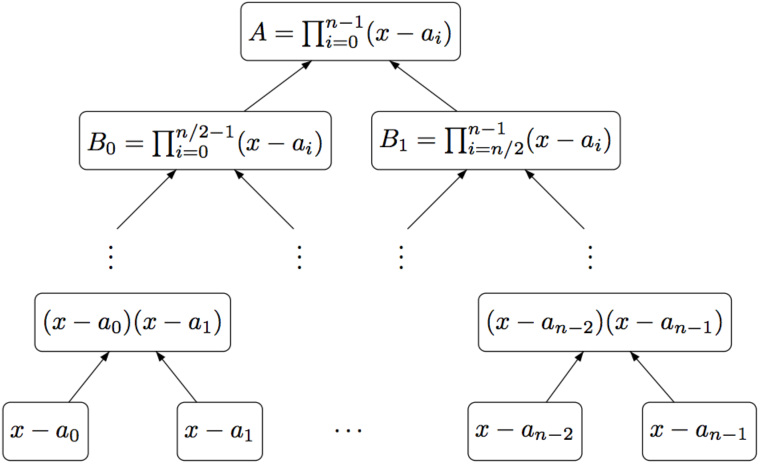
$$\underbrace{F(1/x)x^N}_{\mathrm{rev}(F)} = \underbrace{G(1/x)x^n}_{\mathrm{rev}(G)} \cdot \underbrace{Q(1/x)x^{N-n}}_{\mathrm{rev}(Q)} + \underbrace{R(1/x)x^{\deg(R)}}_{\mathrm{rev}(R)} \cdot x^{N-\deg(R)}$$

Strassen's Algorithm: $\tilde{\mathcal{O}}(N)$

- Compute $\mathrm{rev}(Q) = \mathrm{rev}(F)/\mathrm{rev}(G) \mod x^{N-n+1}$ $\tilde{\mathcal{O}}(N)$
- Recover $Q$ $\mathcal{O}(N)$
- Deduce $R = F - QG$ $\tilde{\mathcal{O}}(N)$

# Subproduct tree

Problem: Given $a_0, \dots, a_{n-1} \in k$, compute $A = \prod_{i=0}^{n-1}(x - a_i)$




Cost: $\mathsf{S}(n) = 2 \cdot \mathsf{S}(n/2) + \tilde{\mathcal{O}}(n) \implies \mathsf{S}(n) = \tilde{\mathcal{O}}(n)$.

# Fast multipoint evaluation

## [Borodin-Moenck, 1974]

Given $a_0, \dots, a_{n-1} \in k$, $P \in k[x]_{<n}$, compute $P(a_0), \dots, P(a_{n-1})$

Naive algorithm: Compute the $P(a_i)$ independently $O(n^2)$

Idea: Use recursively Bézout's identity $P(a) = P(x) \bmod (x - a)$

Divide and conquer: FFT-type idea, evaluation by repeated division

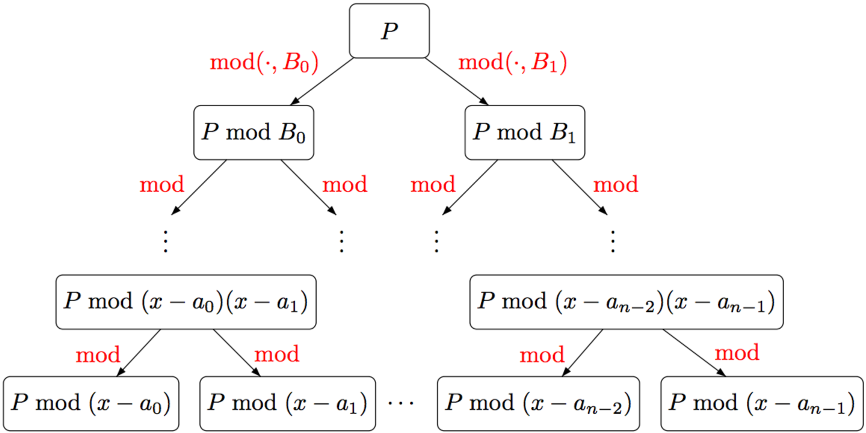
- $P_0 = P \mod (x - a_0) \cdots (x - a_{n/2-1})$
- $P_1 = P \mod (x - a_{n/2}) \cdots (x - a_{n-1})$

$$\Longrightarrow \quad \begin{cases} P_0(a_0) = P(a_0), \quad \dots, \quad P_0(a_{n/2-1}) = P(a_{n/2-1}) \\ P_1(a_{n/2}) = P(a_{n/2}), \quad \dots, \quad P_1(a_{n-1}) = P(a_{n-1}) \end{cases}$$

# Fast multipoint evaluation

## [Borodin-Moenck, 1974]

Given $a_0, \dots, a_{n-1} \in k$, $P \in k[x]_{<n}$, compute $P(a_0), \dots, P(a_{n-1})$




Cost: $\mathsf{E}(n) = 2 \cdot \mathsf{E}(n/2) + \tilde{\mathcal{O}}(n) \implies \mathsf{E}(n) = \tilde{\mathcal{O}}(n)$.

# Fast factorials and matrix factorials

Problem: Compute $N! = 1 \times 2 \times \cdots \times N$

Naive algorithm: unroll the recurrence $\mathcal{O}(N)$

Better algorithm (Strassen, 1976): BS-GS $\tilde{\mathcal{O}}(\sqrt{N})$

(BS) Compute $P = (x+1)(x+2)\cdots(x+\sqrt{N})$ $\tilde{\mathcal{O}}(\sqrt{N})$

(GS) Evaluate $P$ at $0, \sqrt{N}, 2\sqrt{N}, \ldots, (\sqrt{N}-1)\sqrt{N}$ $\tilde{\mathcal{O}}(\sqrt{N})$

Return $u_N = P((\sqrt{N}-1)\sqrt{N}) \cdots P(\sqrt{N}) \cdot P(0)$ $\mathcal{O}(\sqrt{N})$

Chudnovsky$^2$, 1987: generalization to matrix factorials in $\mathcal{O}(\sqrt{N})$

# Fast computation of the $N$-th term

Problem: Compute the $N$-th term $u_N$ of a $P$-recursive sequence

$$p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0, \qquad (n \in \mathbb{N})$$

Naive algorithm: unroll the recurrence $\mathcal{O}(N)$

Better algorithm: $U_n = (u_n, \dots, u_{n+r-1})^T$ satisfies the 1st order rec

$$U_{n+1} = \frac{A(n)}{p_r(n)} U_n, \text{ for } A(n) = \begin{bmatrix} & p_r(n) & & \\ & & \ddots & \\ & & & p_r(n) \\ -p_0(n) & -p_1(n) & \dots & -p_{r-1}(n) \end{bmatrix}$$

$\Longrightarrow u_N$ reads off the matrix factorial $A(N-1)\cdots A(0)$ in $\tilde{\mathcal{O}}(\sqrt{N})$

# Conclusion

# Conclusion, open questions

So far:

- characteristic polynomial of $p$-curvature $\mathbf{A}_p(L)$ in $\tilde{\mathcal{O}}(\sqrt{p})$
- algorithm of quasi-optimal complexity for solving $Lf = 0$.

Still open:

- Can one compute the $p$-curvature in quasi-linear time? (at least for second order operators!)
- Can one decide if $\mathbf{A}_p(L)$ is nilpotent in time less than $\tilde{\mathcal{O}}(\sqrt{p})$?