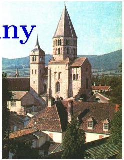
Fast computation of the Nth term of an algebraic series in positive characteristic

Philippe Dumas

JNCF 2015, Cluny

Joint work with
Alin Bostan and Gilles Christol

Ubiquity of algebraic functions (combinatorics, number theory)

Confluence of several domains:

- functional equations
- automatic sequences
- complexity theory

> *One of the most difficult questions in modular computations is the complexity of computations mod p for a large prime p of coefficients in the expansion of an algebraic function.*

D. Chudnovsky & G. Chudnovsky, 1990

Computer Algebra in the Service of

Mathematical Physics and Number Theory

Input:

- field $\mathbb{K}$ of characteristic p
- $f(x) \in \mathbb{K}[[x]]$ solution of $E(x, f(x)) = 0$ with $E(x, y) \in \mathbb{K}[x, y]$, $f(0) = 0$
- $N \in \mathbb{N}_{\geq 0}$

Output:

- the Nth coefficient from the series $f(x)$

Input:

- field $\mathbb{K}$ of characteristic p
- $f(x) \in \mathbb{K}[[x]]$ solution of $E(x, f(x)) = 0$ with $E(x, y) \in \mathbb{K}[x, y]$, $f(0) = 0$
- $N \in \mathbb{N}_{\geq 0}$

Output:

- the Nth coefficient from the series $f(x)$

Main result:

- arithmetic complexity linear in $\log N$ and almost linear in p

Method	char. 0	char. p
Undetermined coefficients	$O(N^d)$	✓
Fixed point iteration	$\widetilde{O}(N^2)$	✓
Newton iteration	$\widetilde{O}(N)$	✓
Linear recurrence	$O(N)$	✓*

*with p-adic computations

Kung + Traub, 1976
All algebraic functions can be computed fast

FFT used all along: multiplication cost for series at order N is $\widetilde{O}(N)$

Method	char. 0	char. p
Undetermined coefficients	$O(N^d)$	✓
Fixed point iteration	$\widetilde{O}(N^2)$	✓
Newton iteration	$\widetilde{O}(N)$	✓
Linear recurrence	$O(N)$	✓*

* with p-adic computations

not appropriate
for one coefficient

FFT used all along: multiplication cost for series at order N is $\widetilde{O}(N)$

Nth coefficient via shift operator

$$f(x) = \sum_{n \geq 0} f_n x^n$$

shift

$$S f_n = f_{n+1}$$

$$S f(x) = \frac{f(x) - f(0)}{x}$$

vector

operators

$$f(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots$$

$$S f(x) = f_1 + f_2 x + f_3 x^2 + f_4 x^3 + \cdots$$

$$S^2 f(x) = f_2 + f_3 x + f_4 x^2 + f_5 x^3 + \cdots$$

$$\vdots$$

$$S^N f(x) = f_N + f_{N+1} x + f_{N+2} x^2 + \cdots$$

linear form

$$S^N f(0) = f_N$$

$$f(x) = \frac{a(x)}{b(x)} \qquad b(0) = 1$$

$$f(x) = \frac{a(x)}{b(x)} \qquad b(0) = 1$$

$$f(x) = \frac{1 + x^3}{1 - x - 2x^2 - 3x^3 - 4x^4 - 5x^5} = 1 + x + 3x^2 + 9x^3 + \cdots$$

$$Sf(x) = \frac{1 + 2x + 4x^2 + 4x^3 + 5x^4}{1 - x - 2x^2 - 3x^3 - 4x^4 - 5x^5} \qquad Sf(0) = 1$$

$$S^2 f(x) = \frac{3 + 6x + 7x^2 + 9x^3 + 5x^4}{1 - x - 2x^2 - 3x^3 - 4x^4 - 5x^5} \qquad S^2 f(0) = 3$$

$$S^3 f(x) = \frac{9 + 13x + 18x^2 + 17x^3 + 15x^4}{1 - x - 2x^2 - 3x^3 - 4x^4 - 5x^5} \qquad S^3 f(0) = 9$$

$$\vdots$$

$$f(x) = \frac{1+x^3}{1-x-2x^2-3x^3-4x^4-5x^5} = 1 + x + 3x^2 + 9x^3 + \cdots$$

$$Sf(x) = \frac{1+2x+4x^2+4x^3+5x^4}{1-x-2x^2-3x^3-4x^4-5x^5} \qquad Sf(0) = 1$$

$$S^2f(x) = \frac{3+6x+7x^2+9x^3+5x^4}{1-x-2x^2-3x^3-4x^4-5x^5} \qquad S^2f(0) = 3$$

$$S^3f(x) = \frac{9+13x+18x^2+17x^3+15x^4}{1-x-2x^2-3x^3-4x^4-5x^5} \qquad S^3f(0) = 9$$

$$\vdots$$

pseudo-shift operator T $\qquad$ $Sb^{-1} = b^{-1}T$

$\mathbb{K}[x]_{<d_x}$ stable by T $\qquad$ finite dimension d_x

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Linear form

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 1 \\ 5 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad C = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

basis: $(1, x, x^2, x^3, x^4)$

Action

$$\frac{1}{b} T1 = S\frac{1}{b} = \frac{\frac{1}{b} - \frac{1}{b(0)}}{x}$$
$$= \frac{1 + 2x + 3x^2 + 4x^3 + 5x^4}{b}$$

Coordinates

$$a(x) = 1 + x^3$$

$$f_N = S^N f(0) \quad \Leftrightarrow \quad f_N = LA^N C$$

Binary powering

example: $N = 1234$

$$A^{1234} = A^2 \times A^{16} \times A^{64} \times A^{128} \times A^{1024}$$

arithmetic complexity $O(\log_2 N)$

Miller + Brown, 1966, *An algorithm for evaluation of remote terms in a linear recurrence sequence*

- shift operator to express f_N
- space of polynomials with pseudo-shift
- finite dimensional space $\to$ linear representation
- binary powering $\to$ good arithmetic complexity

- shift operator to express f_N
- space of polynomials with pseudo-shift
- finite dimensional space $\rightarrow$ linear representation
- binary powering $\rightarrow$ good arithmetic complexity

To come: mimicking this approach in the algebraic case

Method	char. 0	char. p
Baby steps – Giant steps	$\widetilde{O}(\sqrt{N}) + O(1)$	✓*
Divide and Conquer	✘	$O(\log_p N) + \widetilde{O}(p^d)$

*with p-adic computations

Baby steps – Giant steps after precomputing

algebraic equation $\longrightarrow$ differential equation $\longrightarrow$ linear recurrence

Chudnovsky + Chudnovsky, 1988
Approximations and complex multiplication according to Ramanujan

Method	char. 0	char. p
Baby steps – Giant steps	$\widetilde{O}(\sqrt{N}) + O(1)$	✓*
Divide and Conquer	✘	$O(\log_p N) + \widetilde{O}(p^d)$

*with p-adic computations

Baby steps – Giant steps after precomputing

algebraic equation $\longrightarrow$ differential equation $\longrightarrow$ linear recurrence

Divide and Conquer after precomputing

algebraic equation $\longrightarrow$ Mahler equation $\longrightarrow$ DAC recurrence

Christol + Kamae
+ Mendès France + Rauzy, 1980,
Suites algébriques, automates et substitutions

Algebraic equation $\quad y = 2x + 5xy + 4xy^2 + xy^3$

$p = 3$

$$
\begin{array}{c|cccc}
 & y & y^3 & y^9 & y^{27} \\
\hline
\begin{array}{c} 1 \\ y \\ y^2 \end{array} &
\multicolumn{4}{c}{\left[\begin{array}{cccc}
0 & 1 & \frac{1+2x^2+x^3}{x^3} & \frac{1+2x^2+x^3+2x^5+x^6+x^8+x^9+2x^{11}+x^{12}}{x^{12}} \\
1 & \frac{1+x}{x} & \frac{1+x+2x^2+x^3+x^4}{x^4} & \frac{1+x+2x^2+x^3+x^4+2x^5+2x^6+2x^7+x^8+x^9+x^{10}+2x^{11}+x^{12}+x^{13}}{x^{13}} \\
0 & 2 & 2\,\frac{1+x+2x^2+x^3}{x^3} & \frac{2+2x+x^2+2x^3+2x^4+x^5+x^6+x^7+2x^8+2x^9+2x^{10}+x^{11}+2x^{12}}{x^{12}}
\end{array}\right]}
\end{array}
$$

Mahler equation $\qquad c_0(x) = \left(2x^2 + 2x^3 + x^4\right)$

$$
\begin{aligned}
&c_0(x)f(x) \\
&\qquad + \left(1 + x^2 + 2x^3 + 2x^4 + x^5 + 2x^6\right) f(x^3) \\
&\qquad\qquad + \left(2 + 2x^3 + 2x^5 + x^6 + 2x^9\right) f(x^9) + x^9 f(x^{27}) = 0
\end{aligned}
$$

Frobenius $f(x)^p = f(x^p)$ $\qquad (a+b)^p = a^p + b^p$

Algebraic equation $y = 2x + 5xy + 4xy^2 + xy^3$

Mahler equation $c_0(x) = \left(2x^2 + 2x^3 + x^4\right)$

$$
\begin{aligned}
c_0(x)f(x) & \\
& + \left(1 + x^2 + 2x^3 + 2x^4 + x^5 + 2x^6\right) f(x^3) \\
& \quad + \left(2 + 2x^3 + 2x^5 + x^6 + 2x^9\right) f(x^9) + x^9 f(x^{27}) = 0
\end{aligned}
$$

Divide-and-conquer recurrence

$$
\begin{aligned}
2f_{n-2} + 2f_{n-3} + f_{n-4} & \\
& + f_{\frac{n}{3}} + f_{\frac{n-2}{3}} + 2f_{\frac{n-3}{3}} + 2f_{\frac{n-4}{3}} + f_{\frac{n-5}{3}} + 2f_{\frac{n-6}{3}} \\
& \quad + 2f_{\frac{n}{9}} + 2f_{\frac{n-3}{9}} + 2f_{\frac{n-5}{9}} + f_{\frac{n-6}{9}} + 2f_{\frac{n-9}{9}} + f_{\frac{n-9}{27}} = 0
\end{aligned}
$$

$f_x = 0$ if $x \notin \mathbb{N}_{\geq 0}$

Divide-and-conquer recurrence $p = 3$

$$2f_{n-2} + 2f_{n-3} + f_{n-4} + f_{\frac{n}{3}} + f_{\frac{n-2}{3}} + 2f_{\frac{n-3}{3}} + 2f_{\frac{n-4}{3}} + f_{\frac{n-5}{3}} + 2f_{\frac{n-6}{3}} + 2f_{\frac{n}{9}} + 2f_{\frac{n-3}{9}} + 2f_{\frac{n-5}{9}} + f_{\frac{n-6}{9}} + 2f_{\frac{n-9}{9}} + f_{\frac{n-9}{27}} = 0$$

$N = 100$

100

Divide-and-conquer recurrence $p = 3$

$$
\begin{aligned}
&2f_{n-2} + 2f_{n-3} + f_{n-4} \\
&\qquad + f_{\frac{n}{3}} + f_{\frac{n-2}{3}} + 2f_{\frac{n-3}{3}} + 2f_{\frac{n-4}{3}} + f_{\frac{n-5}{3}} + 2f_{\frac{n-6}{3}} \\
&\qquad\quad + 2f_{\frac{n}{9}} + 2f_{\frac{n-3}{9}} + 2f_{\frac{n-5}{9}} + f_{\frac{n-6}{9}} + 2f_{\frac{n-9}{9}} + f_{\frac{n-9}{27}} = 0
\end{aligned}
$$

$N = 100$

100 99 98

34 33 32

11

Divide-and-conquer recurrence $p = 3$

$$
\begin{aligned}
&2f_{n-2} + 2f_{n-3} + f_{n-4} \\
&\qquad + f_{\frac{n}{3}} + f_{\frac{n-2}{3}} + 2f_{\frac{n-3}{3}} + 2f_{\frac{n-4}{3}} + f_{\frac{n-5}{3}} + 2f_{\frac{n-6}{3}} \\
&\qquad\quad + 2f_{\frac{n}{9}} + 2f_{\frac{n-3}{9}} + 2f_{\frac{n-5}{9}} + f_{\frac{n-6}{9}} + 2f_{\frac{n-9}{9}} + f_{\frac{n-9}{27}} = 0
\end{aligned}
$$

$N = 100$

100 99 98 97 96

34 33 32 31 30

12 11 10 9

4 3 1

Divide-and-conquer recurrence $p = 3$

$$2f_{n-2} + 2f_{n-3} + f_{n-4} + f_{\frac{n}{3}} + f_{\frac{n-2}{3}} + 2f_{\frac{n-3}{3}} + 2f_{\frac{n-4}{3}} + f_{\frac{n-5}{3}} + 2f_{\frac{n-6}{3}} + 2f_{\frac{n}{9}} + 2f_{\frac{n-3}{9}} + 2f_{\frac{n-5}{9}} + f_{\frac{n-6}{9}} + 2f_{\frac{n-9}{9}} + f_{\frac{n-9}{27}} = 0$$

$N = 100$

100 99 98 97 96 95 94 ...

34 33 32 31 30 29 28 ...

12 11 10 9 8 7 ...

4 3 2 1 0

arithmetic complexity $O(N)$ for f_N

Change of unknowns $f(x) = c_0(x)g(x)$ yields

$$
\begin{aligned}
g(x) = {} & (x^2 + x^3 + x^7 + x^8 + x^9 + x^{10})g(x^3) \\
& + \big(2x^{14} + 2x^{15} + x^{16} + 2x^{19} + 2x^{20} + x^{21} + x^{22} + 2x^{23} \\
& + 2x^{26} + x^{28} + 2x^{30} + x^{31} + 2x^{32} + x^{33} + 2x^{35} + 2x^{36} + x^{37}\big)\, g(x^9) \\
& + \big(x^{59} + x^{60} + 2x^{61} + 2x^{62} + 2x^{63} + x^{64} + 2x^{65} + 2x^{66} + x^{67} + 2x^{71} \\
& + 2x^{72} + x^{73} + x^{74} + x^{75} + 2x^{76} + x^{77} + x^{78} + 2x^{79} + x^{83} + x^{84} \\
& + 2x^{85} + x^{89} + x^{90} + 2x^{91} + 2x^{92} + 2x^{93} + x^{94} + 2x^{95} + 2x^{96} \\
& + x^{97} + 2x^{101} + 2x^{102} + x^{103} + x^{104} + x^{105} + 2x^{106} + x^{107} \\
& + x^{108} + 2x^{109}\big)\, g(x^{27})
\end{aligned}
$$

Change of unknowns $f_n = 2g_{n-2} + 2g_{n-3} + g_{n-4}$

$$
\begin{aligned}
g_n = {} & g_{\frac{n-2}{3}} + g_{\frac{n-3}{3}} + g_{\frac{n-7}{3}} + g_{\frac{n-8}{3}} + g_{\frac{n-9}{3}} + g_{\frac{n-10}{3}} \\
& + 2g_{\frac{n-14}{9}} + 2g_{\frac{n-15}{9}} + g_{\frac{n-16}{9}} + 2g_{\frac{n-19}{9}} + 2g_{\frac{n-20}{9}} + \cdots + g_{\frac{n-37}{9}} \\
& + g_{\frac{n-59}{27}} + g_{\frac{n-60}{27}} + \cdots + 2g_{\frac{n-109}{27}}
\end{aligned}
$$

$N = 100$

98 97 96

Change of unknowns $f_n = 2g_{n-2} + 2g_{n-3} + g_{n-4}$

$$\begin{aligned} g_n = {} & g_{\frac{n-2}{3}} + g_{\frac{n-3}{3}} + g_{\frac{n-7}{3}} + g_{\frac{n-8}{3}} + g_{\frac{n-9}{3}} + g_{\frac{n-10}{3}} \\ & + 2g_{\frac{n-14}{9}} + 2g_{\frac{n-15}{9}} + g_{\frac{n-16}{9}} + 2g_{\frac{n-19}{9}} + 2g_{\frac{n-20}{9}} + \cdots + g_{\frac{n-37}{9}} \\ & + g_{\frac{n-59}{27}} + g_{\frac{n-60}{27}} + \cdots + 2g_{\frac{n-109}{27}} \end{aligned}$$

$N = 100$

98 97 96

32 31 30 29

9 8 7

1 0

Change of unknowns $f_n = 2g_{n-2} + 2g_{n-3} + g_{n-4}$

$$\begin{aligned} g_n = {} & g_{\frac{n-2}{3}} + g_{\frac{n-3}{3}} + g_{\frac{n-7}{3}} + g_{\frac{n-8}{3}} + g_{\frac{n-9}{3}} + g_{\frac{n-10}{3}} \\ & + 2g_{\frac{n-14}{9}} + 2g_{\frac{n-15}{9}} + g_{\frac{n-16}{9}} + 2g_{\frac{n-19}{9}} + 2g_{\frac{n-20}{9}} + \cdots + g_{\frac{n-37}{9}} \\ & + g_{\frac{n-59}{27}} + g_{\frac{n-60}{27}} + \cdots + 2g_{\frac{n-109}{27}} \end{aligned}$$

$N = 100$

98 97 96

32 31 30 29

10 9 8 7

2 1 0

arithmetic complexity $O(\log_p N)$ for f_N

Introduction

Special case of rational series

Algorithms with low complexity

Sections and diagonal

Partial powering

Section operators

$$S_r \sum_{n\geq 0} u_n x^n = \sum_{k\geq 0} u_{pk+r} x^k, \qquad 0 \leq r < p$$

Section operators

$$S_r \sum_{n\geq 0} u_n x^n = \sum_{k\geq 0} u_{pk+r} x^k, \qquad 0 \leq r < p$$

$$\begin{aligned} f(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + \cdots \\ S_0 f(x) &= f_0 + f_2 x + f_4 x^2 + f_6 x^3 + f_8 x^4 + \cdots \\ S_1 f(x) &= f_1 + f_3 x + f_5 x^2 + f_7 x^3 + f_9 x^4 + \cdots \end{aligned} \qquad p = 2$$

linear operators $\quad S_r\big(\,g(x) \times h(x^p)\,\big) = \big(\,S_r g(x)\,\big) \times h(x)$

$$
\begin{aligned}
100000 &= 5 \times 16807 + 6 \times 2401 + 4 \times 343 + 3 \times 49 + 5 \times 7 + 5 \times 1 \\
&= (5, 6, 4, 3, 5, 5)_7
\end{aligned}
$$

$$
\begin{aligned}
f(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + f_5 x^5 + \cdots \\
S_5 f(x) &= f_5 + f_{12} x + f_{19} x^2 + f_{26} x^3 + f_{33} x^4 + f_{40} x^5 + \cdots \\
S_5 S_5 f(x) &= f_{40} + f_{89} x + f_{138} x^2 + f_{187} x^3 + f_{236} x^4 + f_{285} x^5 + \cdots \\
S_3 S_5 S_5 f(x) &= f_{187} + f_{530} x + f_{873} x^2 + f_{1216} x^3 + f_{1559} x^4 + f_{1902} x^5 + \cdots \\
S_4 S_3 S_5 S_5 f(x) &= f_{1559} + f_{3960} x + f_{6361} x^2 + f_{8762} x^3 + f_{11163} x^4 + \cdots \\
S_6 S_4 S_3 S_5 S_5 f(x) &= f_{15965} + f_{32772} x + f_{49579} x^2 + f_{66386} x^3 + f_{83193} x^4 + \cdots \\
S_5 S_6 S_4 S_3 S_5 S_5 f(x) &= f_{100000} + f_{217649} x + f_{335298} x^2 + f_{452947} x^3 + \cdots \\
S_5 S_6 S_4 S_3 S_5 S_5 f(0) &= f_{100000}
\end{aligned}
$$

Nth coefficient via section operators

vector

$$
\begin{aligned}
f(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + f_5 x^5 + \cdots \\
S_5 f(x) &= f_5 + f_{12} x + f_{19} x^2 + f_{26} x^3 + f_{33} x^4 + f_{40} x^5 + \cdots \\
S_5 S_5 f(x) &= f_{40} + f_{89} x + f_{138} x^2 + f_{187} x^3 + f_{236} x^4 + f_{285} x^5 + \cdots \\
S_3 S_5 S_5 f(x) &= f_{187} + f_{530} x + f_{873} x^2 + f_{1216} x^3 + f_{1559} x^4 + f_{1902} x^5 + \cdots \\
S_4 S_3 S_5 S_5 f(x) &= f_{1559} + f_{3960} x + f_{6361} x^2 + f_{8762} x^3 + f_{11163} x^4 + \cdots \\
S_6 S_4 S_3 S_5 S_5 f(x) &= f_{15965} + f_{32772} x + f_{49579} x^2 + f_{66386} x^3 + f_{83193} x^4 + \cdots \\
S_5 S_6 S_4 S_3 S_5 S_5 f(x) &= f_{100000} + f_{217649} x + f_{335298} x^2 + f_{452947} x^3 + \cdots \\
S_5 S_6 S_4 S_3 S_5 S_5 f(0) &= f_{100000}
\end{aligned}
$$

operators

linear form

$$E(x, f(x)) = 0 \qquad E(x,y) \in \mathbb{K}[x,y]$$

$$\Updownarrow$$

$$f(x) = \mathcal{D}F(x,y) \qquad F(x,y) \in \mathbb{K}(x,y)$$

Furstenberg, 1967,
Algebraic functions over finite fields

Christol, 1974,
Éléments algébriques

$$E(x,f(x))=0 \qquad E(x,y)\in\mathbb{K}[x,y]$$

$$\Updownarrow$$

$$f(x)=\mathcal{D}F(x,y) \qquad F(x,y)\in\mathbb{K}(x,y)$$

$E_y(0,0)\neq 0$

$$F(x,y)=y^2\,\frac{E_y(xy,y)}{E(xy,y)}$$

$$E(x,y)=2x+(5x-1)\,y+4xy^2+xy^3$$

$$F(x,y)=\frac{y(1-5xy-8xy^2-3xy^3)}{1-2x-5xy-4xy^2-xy^3}$$

Furstenberg, 1967, *Algebraic functions over finite fields*

Christol, 1974, *Éléments algébriques*

$$f(x) = 2x + 3x^2 + 3x^3 + x^4 + 6x^5 + 5x^6 + 6x^7 + 3x^8 + x^9 + 4x^{10} + x^{14} + 5x^{15} + \cdots$$

$$p = 7$$

$$F(x, y) =$$

$$\begin{array}{ccccccccccc}
y & + 2xy & + 4x^2y & + x^3y & + 2x^4y & + 4x^5y & + x^6y & + 2x^7y & + 4x^8y & + x^9y & + 2x^{10}y \\
 & & + 3x^2y^2 & + 5x^3y^2 & + x^4y^2 & + 5x^5y^2 & + 2x^6y^2 & + 2x^7y^2 & & + 6x^9y^2 & + 3x^{10}y^2 \\
 & + 3xy^3 & & + 3x^3y^3 & & + 6x^5y^3 & + 4x^6y^3 & + x^7y^3 & + 6x^8y^3 & & + 6x^{10}y^3 \\
 & + 5xy^4 & + 6x^2y^4 & & + x^4y^4 & + x^5y^4 & & + x^7y^4 & + 3x^8y^4 & + 5x^9y^4 & \\
 & & + 2x^2y^5 & + 2x^3y^5 & & + 6x^5y^5 & + 4x^6y^5 & + 5x^7y^5 & & + 4x^9y^5 & + 4x^{10}y^5 \\
 & & + 2x^2y^6 & + 3x^3y^6 & + 5x^4y^6 & & + 5x^6y^6 & + 6x^7y^6 & & + 4x^9y^6 & + 6x^{10}y^6 \\
 & & + 5x^2y^7 & + 6x^3y^7 & & + 5x^5y^7 & & + 6x^7y^7 & & + 3x^9y^7 & + 5x^{10}y^7 \\
 & & & & + 2x^4y^8 & + 3x^5y^8 & + 2x^6y^8 & & + 3x^8y^8 & + 6x^9y^8 & + 5x^{10}y^8 \\
 & & & + x^3y^9 & + x^4y^9 & + 3x^5y^9 & + 6x^6y^9 & + 6x^7y^9 & & + x^9y^9 & + 6x^{10}y^9 \\
 & & & + 5x^3y^{10} & & + 6x^5y^{10} & + 2x^6y^{10} & & + x^8y^{10} & & + 4x^{10}y^{10} \\
 & & & & + x^4y^{11} & + x^5y^{11} & + 5x^6y^{11} & + 4x^7y^{11} & + 4x^8y^{11} & + 2x^9y^{11} & \\
 & & & & & + 6x^5y^{12} & + 2x^6y^{12} & + x^7y^{12} & & + 3x^9y^{12} & + 3x^{10}y^{12} \\
 & & & & + 5x^4y^{13} & & + 5x^6y^{13} & & & + 3x^9y^{13} & + x^{10}y^{13} \\
 & & & & & + 5x^5y^{14} & & + 3x^7y^{14} & & + 4x^9y^{14} & + 2x^{10}y^{14} \\
 & & & & & + 6x^5y^{15} & + x^6y^{15} & + 3x^7y^{15} & + x^8y^{15} & + 2x^9y^{15} & + 4x^{10}y^{15} \\
 & & & & & + 5x^5y^{16} & + 4x^6y^{16} & + 4x^7y^{16} & & + 5x^9y^{16} & + 4x^{10}y^{16} \\
 & & & & & & + \cdots & & & &
\end{array}$$

$$S_r f = S_r \mathcal{D} F = \mathcal{D} S_{r,r} F$$

$$F = \frac{a}{b} = b^{-1} a$$

$$b(0,0) = 1$$

$$S_r f = \mathcal{D} S_{r,r} b^{-1} a$$

$$= \mathcal{D} S_{r,r} b^{-p} b^{p-1} a = \mathcal{D} b^{-1} S_{r,r} b^{p-1} a$$

$$S_r f = \mathcal{D} b^{-1} T_r a$$

$$T_r = S_{r,r} b^{p-1}$$

T_r pseudo-section operator

$$S_{r,r} b^{-p} = b^{-1} T_r$$

f is algebraic $\Leftrightarrow$ f is rational with respect to the radix p

Christol + Kamae + Mendès France + Rauzy, 1980, Suites algébriques, automates et substitutions

Allouche + Shallit, 1992 The ring of k-regular sequences

f is algebraic	$\Leftrightarrow$	f is rational with respect to the radix p

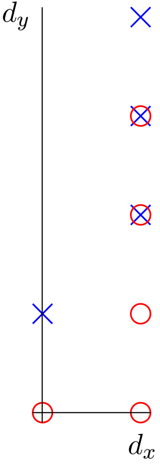
$$f = \mathcal{D}\frac{a}{b}$$

f is algebraic	$\Leftrightarrow$	a generates a finite dimensional vector space under the action of the pseudo-section operators T_r.

Algebraic equation $\quad y = 2x + 5xy + 4xy^2 + xy^3 \qquad\qquad f = \mathcal{D}\frac{a}{b}$

$a = y + 2xy^2 + 6xy^3 + 4xy^4$

$b = 1 + 5x + 2xy + 3xy^2 + 6xy^3$

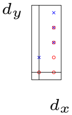


$$d_x = \max(\deg_x a, \deg_x b)$$

$$d_y = \max(\deg_y a, \deg_y b)$$

$$a = y + 2xy^2 + 6xy^3 + 4xy^4$$

$$b = 1 + 5x + 2xy + 3xy^2 + 6xy^3$$

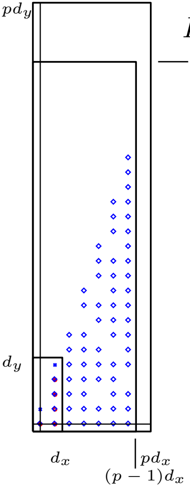


$a = y + 2xy^2 + 6xy^3 + 4xy^4$ ×

$b = 1 + 5x + 2xy + 3xy^2 + 6xy^3$ ○

$B = b^{p-1}$ ◇

$p = 7$

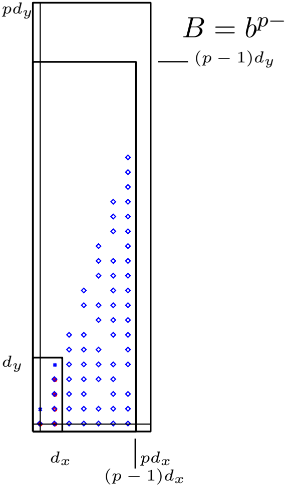


$T_r = S_{r,r}B$

$a = y + 2xy^2 + 6xy^3 + 4xy^4$ ×

$b = 1 + 5x + 2xy + 3xy^2 + 6xy^3$ ○

$B = b^{p-1}$ ◇



$p = 7$

$T_r = S_{r,r}B$

$\mathbb{K}[x,y]_{\le d_x, \le d_y}$ stable by T_r, $0 \le r < p$

finite dimension $(1+d_x)(1+d_y)$

Rational series wrt p and linear representation

$$\begin{aligned}100000 &= 5\times 16807 + 6\times 2401 + 4\times 343 + 3\times 49 + 5\times 7 + 5\times 1\\ &= (5,6,4,3,5,5)_7\end{aligned}$$

vector

$$\begin{aligned}
f(x) &= f_0 + f_1x + f_2x^2 + f_3x^3 + f_4x^4 + f_5x^5 + \cdots\\
S_5f(x) &= f_5 + f_{12}x + f_{19}x^2 + f_{26}x^3 + f_{33}x^4 + f_{40}x^5 + \cdots\\
S_5S_5f(x) &= f_{40} + f_{89}x + f_{138}x^2 + f_{187}x^3 + f_{236}x^4 + f_{285}x^5 + \cdots\\
S_3S_5S_5f(x) &= f_{187} + f_{530}x + f_{873}x^2 + f_{1216}x^3 + f_{1559}x^4 + f_{1902}x^5 + \cdots\\
S_4S_3S_5S_5f(x) &= f_{1559} + f_{3960}x + f_{6361}x^2 + f_{8762}x^3 + f_{11163}x^4 + \cdots\\
S_6S_4S_3S_5S_5f(x) &= f_{15965} + f_{32772}x + f_{49579}x^2 + f_{66386}x^3 + f_{83193}x^4 + \cdots\\
S_5S_6S_4S_3S_5S_5f(x) &= f_{100000} + f_{217649}x + f_{335298}x^2 + f_{452947}x^3 + \cdots\\
S_5S_6S_4S_3S_5S_5f(0) &= f_{100000}
\end{aligned}$$

operators

linear form

$$\begin{aligned} 100000 &= 5 \times 16807 + 6 \times 2401 + 4 \times 343 + 3 \times 49 + 5 \times 7 + 5 \times 1 \\ &= (5, 6, 4, 3, 5, 5)_7 \end{aligned}$$

vector

$$\begin{aligned} a(x,y) &= y + 2xy^2 + 6xy^3 + 4xy^4 \\ T_5 a(x,y) &= 6 + 6y \\ T_5 T_5 a(x,y) &= 5 + 5y \\ T_3 T_5 T_5 a(x,y) &= 5 + 5y \\ T_4 T_3 T_5 T_5 a(x,y) &= 2 + 2y \\ T_6 T_4 T_3 T_5 T_5 a(x,y) &= 2 + 2y \\ T_5 T_6 T_4 T_3 T_5 T_5 a(x,y) &= 4 + 4y \\ T_5 T_6 T_4 T_3 T_5 T_5 a(0,0) &= f_{100000} = 4 \end{aligned}$$

operators

linear form

finite dimension $(1 + d_x)(1 + d_y)$

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Linear form

$$A_0, \quad A_1, \quad \dots \quad A_6$$

$$C = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 2 \\ 0 & 6 \\ 0 & 4 \end{bmatrix}$$

Action

basis: $\begin{matrix} 1 & x \\ y & xy \\ y^2 & xy^2 \\ y^3 & xy^3 \\ y^4 & xy^4 \end{matrix}$

Coordinates

$$a(x, y) = y + 2xy^2 + 6xy^3 + 4xy^4$$

finite dimension $(1 + d_x)(1 + d_y)$

$N = (N_{\ell-1} \ldots N_1 N_0)_p$

$$f_N = S_{N_{\ell-1}} \cdots S_{N_0} f(0)$$

$$\Updownarrow$$

$$f_N = T_{N_{\ell-1}} \cdots T_{N_0} a(0,0)$$

$$\Updownarrow$$

$$f_N = L A_{N_{\ell-1}} \cdots A_{N_0} C$$

arithmetic complexity $O(\log_p N)$

Allouche + Shallit, 1992
The ring of k-regular sequences

All information is in $B = b^{p-1}$.

$$\text{matrix } A_r\colon\ x^n y^m \xrightarrow[\text{translation}]{} x^n y^m B \xrightarrow[\text{selection}]{} S_{r,r} x^n y^m B$$

No computation, except raising b to the power $p-1$

cost: $\widetilde{O}(p^2)$ (binary powering, Kronecker substitution, FFT)

precomputation	computation
$B = b^{p-1}$	$f_N = LA_{N_{\ell-1}} \cdots A_{N_0} C$
$\widetilde{O}(p^2)$	$O(\log_p N)$

Theorem [New]: The Nth coefficient can be computed in time

$$\widetilde{O}(p^2) + O(\log_p N).$$

Task: Computation of A_0, A_1, ..., A_{p-1}

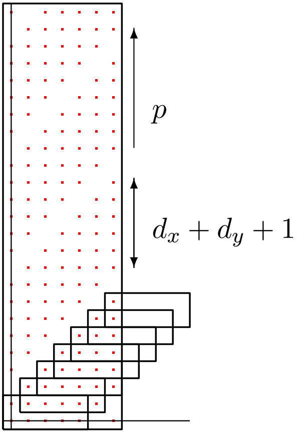
row index $i = (k, \ell)$
column index $j = (n, m)$

$$B = \sum_{\alpha,\beta} c_{\alpha,\beta} x^\alpha y^\beta$$

$$x^n y^m \xrightarrow[\text{translation}]{} x^n y^m B \xrightarrow[\text{selection}]{} S_{r,r} x^n y^m B$$

$$x^n y^m \longrightarrow \sum_{\alpha,\beta} c_{\alpha,\beta} x^{n+\alpha} y^{m+\beta} \longrightarrow \sum_{\substack{\alpha,\beta \\ (C)}} c_{\alpha,\beta} x^k y^\ell$$

$$(C) \begin{cases} n + \alpha = pk + r \\ m + \beta = p\ell + r \end{cases} \implies \beta - \alpha = p(\ell - k) + n - m$$

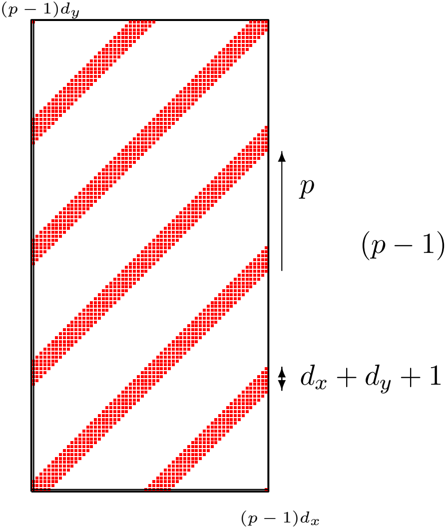


$p = 7$

$d_x = 1$

$d_y = 4$

Only a small part of $B = b^{p-1}$ is enough



$p = 31$

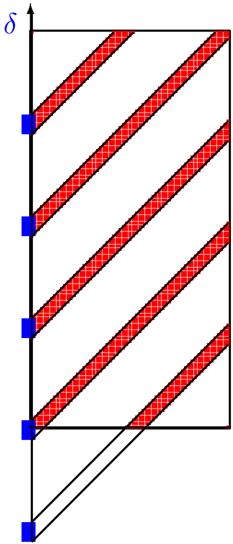
$d_x = 2$

$d_y = 4$

$$(p-1)d_x \times (p-1)d_y \times \frac{d_x + d_y + 1}{p} = O(p)$$

$$B(x/t,t) = \sum_{\alpha,\beta} c_{\alpha,\beta} x^{\alpha} t^{\beta-\alpha} = \sum_{\delta} \pi_{\delta}(x) t^{\delta}$$

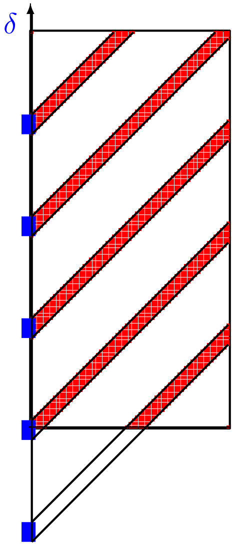
$\delta = \beta - \alpha = p(\ell - k) + n - m$



$$B(x/t,t) = \sum_{\alpha,\beta} c_{\alpha,\beta} x^\alpha t^{\beta-\alpha} = \sum_{\delta} \pi_\delta(x) t^\delta$$

$$\delta = \beta - \alpha = p(\ell - k) + n - m$$

$$B(x/t,t) = b(x/t,t)^{p-1} = \frac{b(x/t,t)^p}{b(x/t,t)} = \frac{b(x^p/t^p,t^p)}{b(x/t,t)}$$



$$B(x/t,t) = \sum_{\alpha,\beta} c_{\alpha,\beta} x^{\alpha} t^{\beta-\alpha} = \sum_{\delta} \pi_{\delta}(x) t^{\delta}$$

$$\delta = \beta - \alpha = p(\ell - k) + n - m$$

$$B(x/t,t) = b(x/t,t)^{p-1} = \frac{b(x/t,t)^p}{b(x/t,t)} = \frac{b(x^p/t^p,t^p)}{b(x/t,t)}$$

$$\frac{1}{b(x/t,t)} = \sum_u b_u^{(0)}(x) t^u \qquad b(x^p/t^p,t^p) = \textstyle\sum_v b_v^{(1)}(x^p) t^{pv}$$

rational series — for free

$$B(x/t,t) = \sum_{\alpha,\beta} c_{\alpha,\beta} x^{\alpha} t^{\beta-\alpha} = \sum_{\delta} \pi_{\delta}(x) t^{\delta}$$

$$B(x/t,t) = b(x/t,t)^{p-1} = \frac{b(x/t,t)^p}{b(x/t,t)} = \frac{b(x^p/t^p,t^p)}{b(x/t,t)}$$

$$\frac{1}{b(x/t,t)} = \sum_{u} b_u^{(0)}(x) t^u \qquad b(x^p/t^p,t^p) = \textstyle\sum_v b_v^{(1)}(x^p) t^{pv}$$

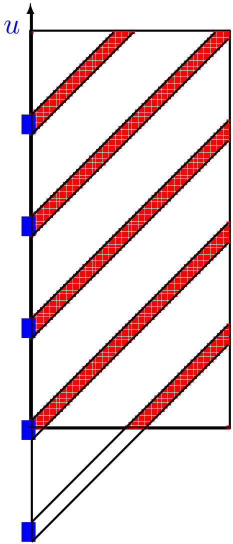
rational series — for free

$$\pi_{\delta}(x) = \sum_{u+pv=\delta} b_u^{(0)}(x) b_v^{(1)}(x^p) \qquad u + pv = \delta \Longrightarrow u \equiv \delta \mod p$$

same intervals

$$\frac{1}{b(x/t,t)} = \sum_u b_u^{(0)}(x) t^u \in \mathbb{K}(x)[[t]]$$

rational series



same intervals

$$\frac{1}{b(x/t,t)} = \sum_u b_u^{(0)}(x)t^u \in \mathbb{K}(x)[[t]]$$

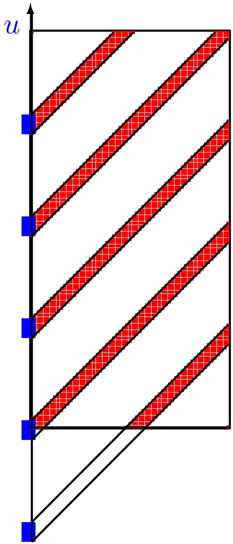
$$\frac{1}{b(\xi/t,t)} = \sum_u b_u^{(0)}(\xi)t^u \in \mathbb{K}[[t]], \qquad \xi \in \mathbb{K}$$

rational series with coefficients in $\mathbb{K}$

binary powering

about $d_x + d_y = O(1)$ large leaps of length p

$\longrightarrow$ cost $O(\log p)$



binary powering

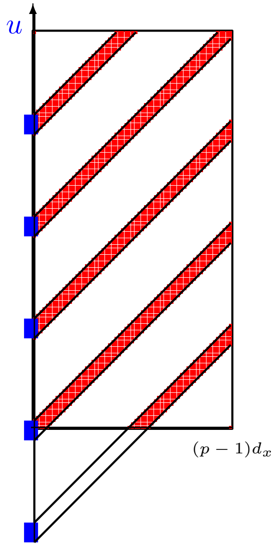
about $d_x + d_y = O(1)$ large leaps of length p

$\longrightarrow$ cost $O(\log p)$

interpolation

degree about $(p-1)d_x = O(p)$

$\longrightarrow$ cost $\widetilde{O}(p \log^2 p)$



binary powering

about $d_x + d_y$ large leaps of length p

$\longrightarrow$ cost $(d_x + d_y)\log p$

interpolation

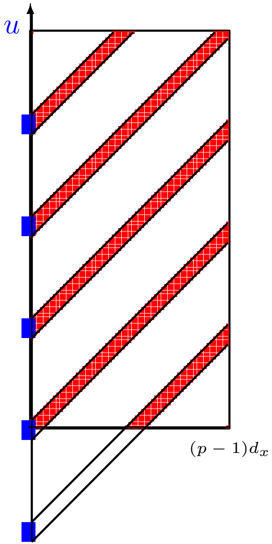
degree about pd_x

$\longrightarrow$ cost $\widetilde{O}(p\log^2 p)$

gathering

about $(d_x + d_y)^2 = O(1)$ indices

$\longrightarrow$ global cost $\widetilde{O}(p\log^2 p)$



Theorem [New and better]: The Nth coefficient can be computed in time

$$\widetilde{\boldsymbol{O}}(\boldsymbol{p}) + O(\log_p N).$$

Not quite obvious result following from the asymptotic expansions of the difference equation, shows that [...] requires only $O(p \cdot \log_p N)$ operations.

D. Chudnovsky & G. Chudnovsky, 1990

Computer Algebra in the Service of

Mathematical Physics and Number Theory

Theorem [New and better]: The Nth coefficient can be computed in time

$$\widetilde{\boldsymbol{O}}(\boldsymbol{p}) + O(\log_p N).$$

What is the minimal complexity of the computation of N-th coefficient of a power series expansion of an algebraic function mod p *for a fixed (large) prime p? It is reasonable to conjecture that [...] one needs at most $O(L(p)\log N)$ operations, where $L(p) = \exp(\sqrt{\log p \,\log\log p})$ at least for hyperelliptic algebraic functions.*

D. Chudnovsky & G. Chudnovsky, 1987

Computer assisted number theory with applications

Thank you for your attention!

$$+5x^{131}+2x^{130}+4x^{129}+x^{128}+2x^{127}+5x^{126}+3x^{125}+2x^{124}+4x^{123}+x^{122}+x^{121}+6x^{120}+6x^{119}$$
$$+2x^{118}+2x^{117}+5x^{116}+3x^{115}+6x^{114}+4x^{113}+2x^{112}+6x^{111}+4x^{110}+6x^{109}+5x^{108}+6x^{107}$$
$$+5x^{106}+6x^{105}+4x^{104}+3x^{103}+4x^{102}+x^{101}+2x^{100}+5x^{99}+3x^{98}+4x^{97}+5x^{71}+4x^{69}+2x^{68}+2x^{67}$$
$$+4x^{66}+5x^{65}+3x^{64}+x^{62}+2x^{57}+3x^{55}+3x^{54}+3x^{53}+6x^{52}+4x^{51}+5x^{50}+4x^{48}+2x^{46}+4x^{45}$$
$$+3x^{44}+x^{43}+6x^{42}+5x^{41}+2x^{40}\text{[illegible]}x^{39}\text{[illegible]}x^{38}+6x^{37}+3x^{36}+2x^{35}+x^{34}+4x^{33}\text{[illegible]}x^{32}+6x^{31}+5x^{30}$$
$$+3x^{29}+4x^{28}+x^{27}+3x^{26}+6x^{25}+5x^{24}+5x^{23}+5x^{22}+2x^{21}+4x^{20}+x^{18}+2x^{17}+5x^{16}+5x^{15}+3x^{14}$$
$$+4x^{13}+6x^{12}\text{[illegible]}x^{11}+4x^{10}+2x^{9}+x^{8}+2x^{7}+5x^{6}\text{[illegible]}+3x^{3}+4x^{2}+1\Big)f(x^{7})$$
$$+\Big(6x^{165}+5x^{164}+2x^{163}+2x^{162}+4x^{161}+3x^{160}+2x^{155}+3x^{153}+2x^{151}+4x^{150}+3x^{149}+6x^{147}$$
$$+x^{144}+2x^{143}+5x^{142}+4x^{141}+3x^{140}+6x^{139}+x^{137}+2x^{136}+5x^{135}+x^{134}+3x^{133}+5x^{132}+2x^{130}$$
$$+4x^{129}+3x^{128}+4x^{127}+6x^{126}+6x^{125}+6x^{123}+5x^{122}+2x^{121}+2x^{120}+4x^{119}+3x^{118}+5x^{116}$$
$$+3x^{115}+4x^{114}+4x^{113}+x^{112}+6x^{111}+4x^{106}+6x^{104}+4x^{102}+x^{101}+6x^{100}+5x^{98}+2x^{71}+3x^{69}$$
$$+x^{67}+2x^{66}+5x^{65}+5x^{64}+3x^{63}+4x^{62}+5x^{57}+4x^{55}+5x^{53}+3x^{52}+4x^{51}+x^{49}+5x^{46}+3x^{45}+4x^{44}$$
$$+6x^{43}+x^{42}+2x^{41}+5x^{39}+3x^{38}+4x^{37}+5x^{36}+x^{35}+4x^{34}+3x^{32}+6x^{31}+x^{30}+6x^{29}+2x^{28}+2x^{27}$$
$$+2x^{25}+4x^{24}+3x^{23}+6x^{21}+6x^{18}+5x^{17}+2x^{16}+2x^{15}+4x^{14}+3x^{13}+2x^{8}+3x^{6}+2x^{4}+4x^{3}+3x^{2}+6\Big)f(x^{49})$$
$$+\Big(x^{165}+2x^{164}+5x^{163}+5x^{162}+3x^{161}+4x^{160}+5x^{155}+4x^{153}+5x^{151}+3x^{150}+4x^{149}+x^{147}\Big)f(x^{343})=0$$