Algebraicity and transcendence of power series: combinatorial and computational aspects

Alin Bostan

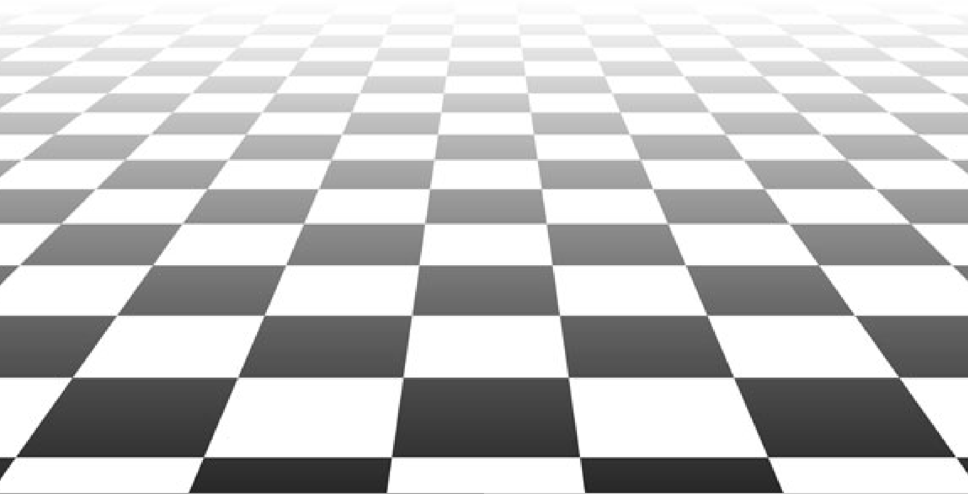
informatics mathematics Inria

Algorithmic and Enumerative Combinatorics
RISC, Hagenberg, August 1–5, 2016

Overview

1. Monday: Context and Examples
2. Tuesday: Properties and Criteria (1)
3. Wednesday: Properties and Criteria (2)
4. Thursday: Algorithmic Proofs of Algebraicity
5. Friday: Transcendence in Lattice Path Combinatorics

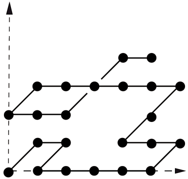
Part IV: Algorithmic Proofs of Algebraicity



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

Question: Find the nature of the generating function

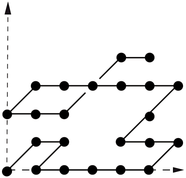
$$G(t;x,y) = \sum_{i,j,n=0}^{\infty} g(n;i,j)\, x^i y^j t^n \;\in \mathbb{Q}[[x,y,t]]$$



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

Question: Find the nature of the generating function

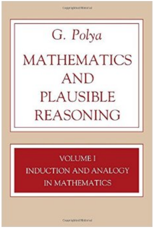
$$G(t;x,y) = \sum_{i,j,n=0}^{\infty} g(n;i,j)\, x^i y^j t^n \;\in \mathbb{Q}[[x,y,t]]$$



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

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

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



Guessing and Proving

George Pólya

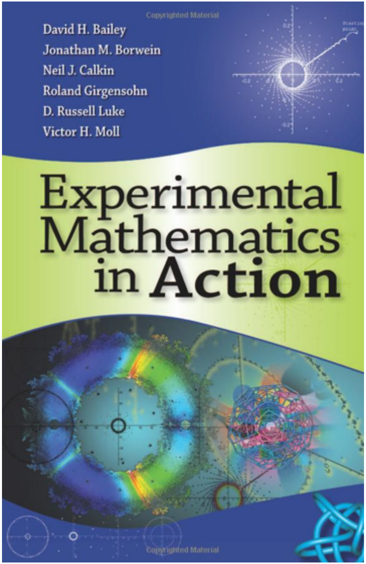
What is "scientific method"? Philosophers and non-philosophers have discussed this question and have not yet finished discussing it. Yet as a first introduction it can be described in three syllables:

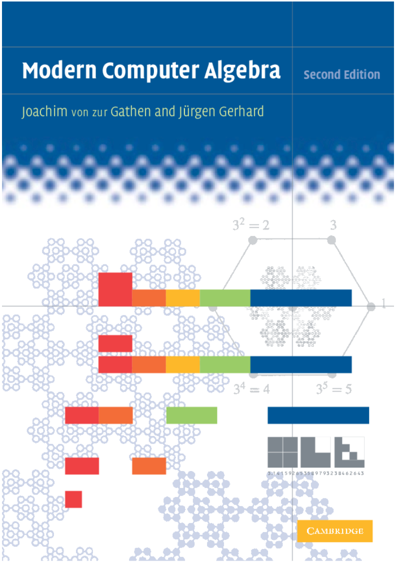
Guess and test.

Mathematicians too follow this advice in their research although they sometimes refuse to confess it. They have, however, something which the other scientists cannot really have. For mathematicians the advice is

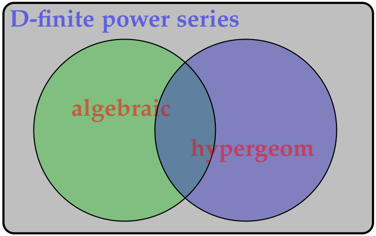
First guess, then prove.

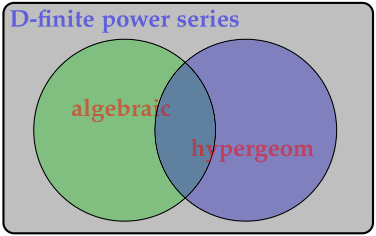
Personal bias: Experimental Mathematics using Computer Algebra





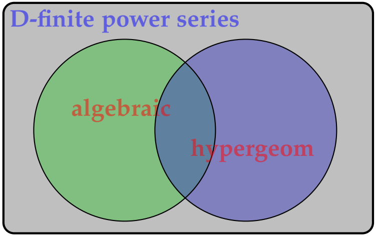
Classification of univariate power series





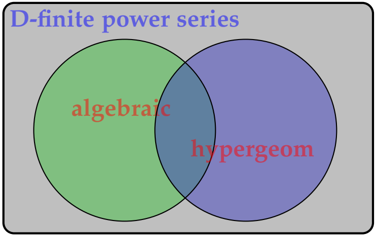
▷ *Algebraic*: $S(t) \in \mathbb{Q}[[t]]$ root of a polynomial $P \in \mathbb{Q}[t, T]$, i.e., $P\big(t, S(t)\big) = 0$.

Classification of univariate power series



▷ *Algebraic*: $S(t) \in \mathbb{Q}[[t]]$ root of a polynomial $P \in \mathbb{Q}[t,T]$, i.e., $P\big(t, S(t)\big) = 0$.

▷ *D-finite*: $S(t) \in \mathbb{Q}[[t]]$ satisfying a linear differential equation with polynomial coefficients $c_r(t)S^{(r)}(t) + \cdots + c_0(t)S(t) = 0$.



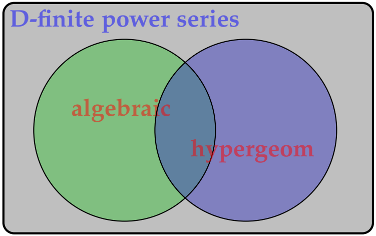
▷ *Algebraic*: $S(t) \in \mathbb{Q}[[t]]$ root of a polynomial $P \in \mathbb{Q}[t, T]$, i.e., $P\big(t, S(t)\big) = 0$.

▷ *D-finite*: $S(t) \in \mathbb{Q}[[t]]$ satisfying a linear differential equation with polynomial coefficients $c_r(t)S^{(r)}(t) + \cdots + c_0(t)S(t) = 0$.

▷ *Hypergeometric*: $S(t) = \sum_{n=0}^{\infty} s_n t^n$ such that $\frac{s_{n+1}}{s_n} \in \mathbb{Q}(n)$. E.g.,

$${}_2F_1\left(\begin{matrix} a\ b \\ c \end{matrix} \,\middle|\, t\right) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \frac{t^n}{n!}, \quad (a)_n = a(a+1)\cdots(a+n-1).$$

Classification of univariate power series

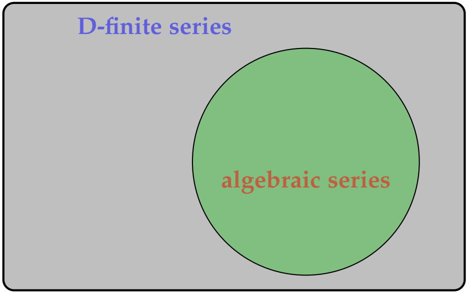


▷ *Algebraic*: $S(t) \in \mathbb{Q}[[t]]$ root of a polynomial $P \in \mathbb{Q}[t, T]$, i.e., $P(t, S(t)) = 0$.

▷ *D-finite*: $S(t) \in \mathbb{Q}[[t]]$ satisfying a linear differential equation with polynomial coefficients $c_r(t)S^{(r)}(t) + \cdots + c_0(t)S(t) = 0$.

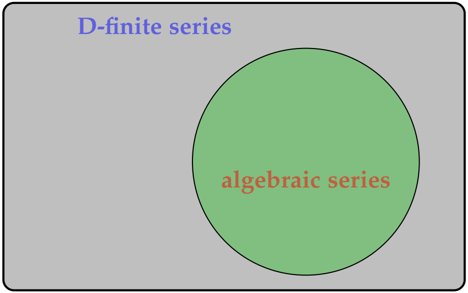
▷ *Hypergeometric*: $S(t) = \sum_{n=0}^{\infty} s_n t^n$ such that $\frac{s_{n+1}}{s_n} \in \mathbb{Q}(n)$. E.g.,

$$ {}_3F_2\left(\begin{matrix} a\ b\ c \\ d\ e \end{matrix} \,\middle|\, t\right) = \sum_{n=0}^{\infty} \frac{(a)_n(b)_n(c)_n}{(d)_n(e)_n} \frac{t^n}{n!}, \quad (a)_n = a(a+1)\cdots(a+n-1). $$



▷ $S \in \mathbb{Q}[[x, y, t]]$ is *algebraic* if it is the root of a polynomial $P \in \mathbb{Q}[x, y, t, T]$.

Classification of multivariate power series



▷ $S \in \mathbb{Q}[[x,y,t]]$ is *algebraic* if it is the root of a polynomial $P \in \mathbb{Q}[x,y,t,T]$.

▷ $S \in \mathbb{Q}[[x,y,t]]$ is *D-finite* if it satisfies a system of linear partial differential equations with polynomial coefficients

$$\sum_i a_i(t,x,y)\frac{\partial^i S}{\partial x^i} = 0, \quad \sum_i b_i(t,x,y)\frac{\partial^i S}{\partial y^i} = 0, \quad \sum_i c_i(t,x,y)\frac{\partial^i S}{\partial t^i} = 0.$$

Gessel's walks

$$\mathfrak{S} = \{\nearrow, \swarrow, \leftarrow, \rightarrow\}$$

THE ON–LINE ENCYCLOPEDIA OF INTEGER SEQUENCES®

founded in 1964 by N. J. A. Sloane

1,2,11,85 Search Hints

(Greetings from The On-Line Encyclopedia of Integer Sequences!)

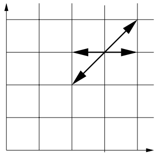
Search: **seq:1,2,11,85**

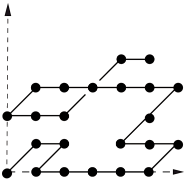
Displaying 1-1 of 1 result found. page 1

Sort: relevance | references | number | modified | created Format: long | short | data

A135404 Gessel sequence: the number of paths of length 2m in the plane, starting and ending at (0,1), with unit steps in the four directions (north, east, south, west) and staying in the region y>0, x>-y. +20 6

1, 2, 11, 85, 782, 8004, 88044, 1020162, 12294260, 152787976, 1946310467, 25302036071, 334560525538, 4488007049900, 60955295750460, 836838395382645, 11597595644244186, 162074575606984788, 2281839419729917410, 32340239369121304038, 461109219391987625316, 6610306991283738684600 (list; graph; refs; listen; history; text; internal format)



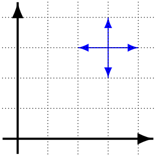


Conjecture 1 The generating function of Gessel excursions is equal to

$$G(t;0,0) = {}_3F_2\left(\left.\begin{matrix}5/6 & 1/2 & 1\\ & 5/3 & 2\end{matrix}\right|16t^2\right) = \sum_{n=0}^{\infty} \frac{(5/6)_n(1/2)_n}{(5/3)_n(2)_n}(4t)^{2n} = 1 + 2t^2 + 11t^4 + 85t^6 + 782t^7 + \cdots$$

Conjecture 2
The full generating function $G(t;x,y)$ is not D-finite.

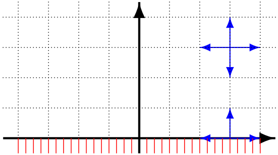
The simple walk in the plane

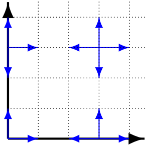


[Pólya, 1921]:

▷ Formula $\binom{2n}{n}^2$ for $2n$-excursions
▷ Rational generating function

The simple walk in the half-plane and in the quarter-plane

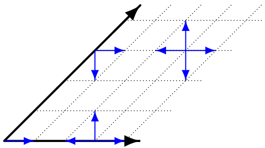


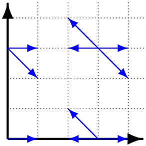


▷ Formulas $\binom{2n+1}{n}C_n$, resp. $C_n C_{n+1}$, for $2n$-excursions [Arquès, 1986]
▷ Full generating functions: algebraic [Bousquet-Mélou & Petkovšek, 2000], resp. D-finite [Bousquet-Mélou, 2002]

Genesis of Gessel's questions – the "simple walk" in different cones

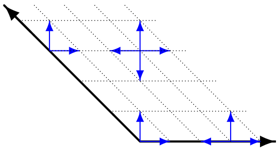
The simple walk in the cone with angle 45°

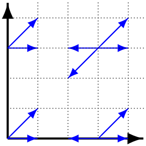




▷ Formula $C_nC_{n+2} - C_{n+1}^2$ for $2n$-excursions [Gouyou-Beauchamps, 1986]
▷ D-finite generating function [Gessel & Zeilberger, 1992]

What about the simple walk in the cone with angle 135°?

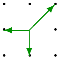


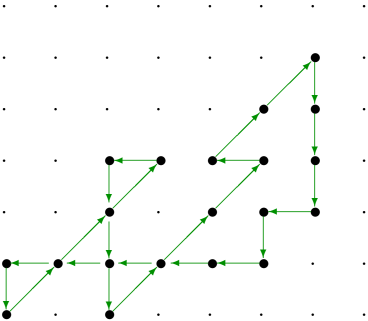


A relative of Gessel walks: Kreweras walks

$\mathfrak{S} = \{\downarrow, \leftarrow, \nearrow\}$ $\qquad F_{\mathfrak{S}}(t;x,y) \equiv K(t;x,y)$

$\mathfrak{S} = \{\nearrow, \swarrow, \leftarrow, \rightarrow\}$ $\qquad F_{\mathfrak{S}}(t;x,y) \equiv G(t;x,y)$





Example: A Kreweras excursion.

Methodology for proving algebraicity

Experimental mathematics –Guess'n'Prove– approach:

(S1) Generate data

(S2) Conjecture

(S3) Prove

Methodology for proving algebraicity

Experimental mathematics –Guess'n'Prove– approach:

(S1) Generate data
compute a high order expansion of the series $F_{\mathfrak{S}}(t;x,y)$;

(S2) Conjecture
guess a candidate for the minimal polynomial of $F_{\mathfrak{S}}(t;x,y)$, using Hermite-Padé approximation;

(S3) Prove
rigorously certify the minimal polynomials, using (exact) polynomial computations.

Experimental mathematics –Guess'n'Prove– approach:

(S1) Generate data
compute a high order expansion of the series $F_{\mathfrak{S}}(t; x, y)$;

(S2) Conjecture
guess candidates for minimal polynomials of $F_{\mathfrak{S}}(t; x, 0)$ and $F_{\mathfrak{S}}(t; 0, y)$, using Hermite-Padé approximation;

(S3) Prove
rigorously certify the minimal polynomials, using (exact) polynomial computations.

Methodology for proving algebraicity

Experimental mathematics –Guess'n'Prove– approach:

(S1) Generate data
compute a high order expansion of the series $F_{\mathfrak{S}}(t;x,y)$;

(S2) Conjecture
guess candidates for minimal polynomials of $F_{\mathfrak{S}}(t;x,0)$ and $F_{\mathfrak{S}}(t;0,y)$, using Hermite-Padé approximation;

(S3) Prove
rigorously certify the minimal polynomials, using (exact) polynomial computations.

+ Efficient Computer Algebra

Step (S1): high order series expansions

$f_{\mathfrak{S}}(n;i,j)$ satisfies the recurrence with constant coefficients

$$f_{\mathfrak{S}}(n+1;i,j) = \sum_{(u,v)\in\mathfrak{S}} f_{\mathfrak{S}}(n;i-u,j-v) \quad \text{for} \quad n,i,j \geq 0$$

+ initial conditions $f_{\mathfrak{S}}(0;i,j) = \delta_{0,i,j}$ and $f_{\mathfrak{S}}(n;-1,j) = f_{\mathfrak{S}}(n;i,-1) = 0$.

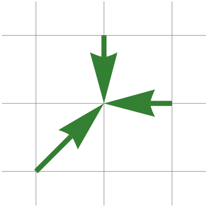
$f_{\mathfrak{S}}(n;i,j)$ satisfies the recurrence with constant coefficients

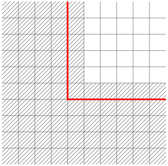
$$f_{\mathfrak{S}}(n+1;i,j) = \sum_{(u,v)\in\mathfrak{S}} f_{\mathfrak{S}}(n;i-u,j-v) \quad \text{for} \quad n,i,j \geq 0$$

+ initial conditions $f_{\mathfrak{S}}(0;i,j) = \delta_{0,i,j}$ and $f_{\mathfrak{S}}(n;-1,j) = f_{\mathfrak{S}}(n;i,-1) = 0$.

Example: for the Kreweras model,

$$\begin{aligned} k(n+1;i,j) &= k(n;i+1,j) \\ &\quad + k(n;i,j+1) \\ &\quad + k(n;i-1,j-1) \end{aligned}$$





Step (S1): high order series expansions

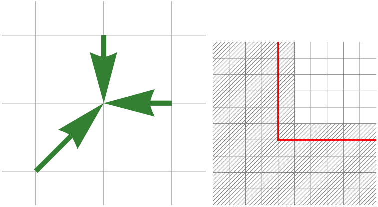
$f_{\mathfrak{S}}(n;i,j)$ satisfies the recurrence with constant coefficients

$$f_{\mathfrak{S}}(n+1;i,j) = \sum_{(u,v)\in\mathfrak{S}} f_{\mathfrak{S}}(n;i-u,j-v) \quad \text{for} \quad n,i,j \geq 0$$

+ initial conditions $f_{\mathfrak{S}}(0;i,j) = \delta_{0,i,j}$ and $f_{\mathfrak{S}}(n;-1,j) = f_{\mathfrak{S}}(n;i,-1) = 0$.

Example: for the Kreweras model,

$$\begin{aligned} k(n+1;i,j) = {} & k(n;i+1,j) \\ & + k(n;i,j+1) \\ & + k(n;i-1,j-1) \end{aligned}$$



▷ Recurrence is used to compute $F_{\mathfrak{S}}(t;x,y) \bmod t^N$ for large N.

$$\begin{aligned} K(t;x,y) = {} & 1 + xyt + (x^2y^2 + y + x)t^2 + (x^3y^3 + 2xy^2 + 2x^2y + 2)t^3 \\ & + (x^4y^4 + 3x^2y^3 + 3x^3y^2 + 2y^2 + 6xy + 2x^2)t^4 \\ & + (x^5y^5 + 4x^3y^4 + 4x^4y^3 + 5xy^3 + 12x^2y^2 + 5x^3y + 8y + 8x)t^5 + \cdots \end{aligned}$$

In terms of generating series, the recurrence on $k(n;i,j)$ reads

$$\boxed{\begin{aligned}&(xy-(x+y+x^2y^2)t)K(t;x,y)\\&\qquad = xy - xt\,K(t;x,0) - yt\,K(t;0,y)\end{aligned}} \qquad \text{(KerEq)}$$

▷ A similar kernel equation holds for $F_{\mathfrak{S}}(t;x,y)$, for any $\mathfrak{S}$-walk.

Corollary. $F_{\mathfrak{S}}(t;x,y)$ is algebraic (resp. D-finite) if and only if $F_{\mathfrak{S}}(t;x,0)$ and $F_{\mathfrak{S}}(t;0,y)$ are both algebraic (resp. D-finite).

▷ Crucial simplification: equations for $G(t;x,y)$ are huge ($\approx$ 30 Gb)

Step (S2): guessing equations for $F_{\mathfrak{S}}(t;x,0)$ & $F_{\mathfrak{S}}(t;0,y)$

Task 1: Given the first N terms of $S = F_{\mathfrak{S}}(t;x,0) \in \mathbb{Q}[x][[t]]$, search for a differential equation satisfied by S at precision N:

$$c_r(x,t) \cdot \frac{\partial^r S}{\partial t^r} + \cdots + c_1(x,t) \cdot \frac{\partial S}{\partial t} + c_0(x,t) \cdot S = 0 \mod t^N.$$

Step (S2): guessing equations for $F_{\mathfrak{S}}(t;x,0)$ & $F_{\mathfrak{S}}(t;0,y)$

Task 1: Given the first N terms of $S = F_{\mathfrak{S}}(t;x,0) \in \mathbb{Q}[x][[t]]$, search for a differential equation satisfied by S at precision N:

$$c_r(x,t) \cdot \frac{\partial^r S}{\partial t^r} + \cdots + c_1(x,t) \cdot \frac{\partial S}{\partial t} + c_0(x,t) \cdot S = 0 \mod t^N.$$

Task 2: Search for an algebraic equation $\mathcal{P}_{x,0}(S) = 0 \mod t^N$.

Step (S2): guessing equations for $F_{\mathfrak{S}}(t;x,0)$ & $F_{\mathfrak{S}}(t;0,y)$

Task 1: Given the first N terms of $S = F_{\mathfrak{S}}(t;x,0) \in \mathbb{Q}[x][[t]]$, search for a differential equation satisfied by S at precision N:

$$c_r(x,t) \cdot \frac{\partial^r S}{\partial t^r} + \cdots + c_1(x,t) \cdot \frac{\partial S}{\partial t} + c_0(x,t) \cdot S = 0 \mod t^N.$$

Task 2: Search for an algebraic equation $\mathcal{P}_{x,0}(S) = 0 \mod t^N$.

- Both tasks amount to linear algebra in size N over $\mathbb{Q}(x)$.
- In practice, we use modular Hermite-Padé approximation (Beckermann-Labahn algorithm) combined with (rational) evaluation-interpolation and rational number reconstruction.
- Fast (FFT-based) arithmetic in $\mathbb{F}_p[t]$.

Step (S2): guessing equations for $K(t;x,0)$

Using $N = 80$ terms of $K(t;x,0)$, one can guess

▷ a linear differential equation of order 4, degrees $(14, 11)$ in (t, x), such that

$$
\begin{aligned}
&t^3 \cdot (3t-1) \cdot (9t^2+3t+1) \cdot (3t^2+24t^2x^3-3xt-2x^2) \cdot \\
&\cdot (16t^2x^5+4x^4-72t^4x^3-18x^3t+5t^2x^2+18xt^3-9t^4) \cdot \\
&\qquad \cdot (4t^2x^3-t^2+2xt-x^2) \cdot \frac{\partial^4 K(t;x,0)}{\partial t^4} + \cdots \\
&\qquad\qquad = 0 \bmod t^{80}
\end{aligned}
$$

▷ a polynomial of tridegree $(6, 10, 6)$ in (T, t, x)

$$
\begin{aligned}
\mathcal{P}_{x,0} &= x^6t^{10}T^6 - 3x^4t^8(x-2t)T^5 + \\
&\quad + x^2t^6\left(12t^2+3t^2x^3-12xt+\frac{7}{2}x^2\right)T^4 + \cdots
\end{aligned}
$$

such that $\mathcal{P}_{x,0}(K(t;x,0), t, x) = 0 \bmod t^{80}$.

Using $N = 1200$ terms of $G(t;x,y)$, our guesser found candidates

- $\mathcal{P}_{x,0}$ in $\mathbb{Z}[x,t,T]$ of degree $(32,43,24)$, coefficients of 21 digits
- $\mathcal{P}_{0,y}$ in $\mathbb{Z}[y,t,T]$ of degree $(40,44,24)$, coefficients of 23 digits

such that

$$\mathcal{P}_{x,0}(x,t,G(t;x,0)) = \mathcal{P}_{0,y}(y,t,G(t;0,y)) = 0 \mod t^{1200}.$$

Step (S2): guessing equations for $G(t;x,0)$ and $G(t;0,y)$

Using $N = 1200$ terms of $G(t;x,y)$, our guesser found candidates

- $\mathcal{P}_{x,0}$ in $\mathbb{Z}[x,t,T]$ of degree $(32,43,24)$, coefficients of 21 digits
- $\mathcal{P}_{0,y}$ in $\mathbb{Z}[y,t,T]$ of degree $(40,44,24)$, coefficients of 23 digits

such that

$$\mathcal{P}_{x,0}(x,t,G(t;x,0)) = \mathcal{P}_{0,y}(y,t,G(t;0,y)) = 0 \mod t^{1200}.$$

$\triangleright$ Guessing $\mathcal{P}_{x,0}$ by undetermined coefficients would have required to solve a dense linear system of size $\approx 100\,000$, and ≈ 1000 digits entries!

Step (S2): guessing equations for $G(t;x,0)$ and $G(t;0,y)$

Using $N = 1200$ terms of $G(t;x,y)$, our guesser found candidates

- $\mathcal{P}_{x,0}$ in $\mathbb{Z}[x,t,T]$ of degree $(32,43,24)$, coefficients of 21 digits
- $\mathcal{P}_{0,y}$ in $\mathbb{Z}[y,t,T]$ of degree $(40,44,24)$, coefficients of 23 digits

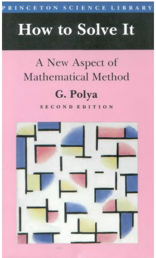
such that

$$\mathcal{P}_{x,0}(x,t,G(t;x,0)) = \mathcal{P}_{0,y}(y,t,G(t;0,y)) = 0 \mod t^{1200}.$$

▷ Guessing $\mathcal{P}_{x,0}$ by undetermined coefficients would have required to solve a dense linear system of size $\approx 100\,000$, and ≈ 1000 digits entries!

▷ We actually first guessed differential equations[†], then computed their p-curvatures to empirically certify them. This led us suspect the algebraicity of $G(t;x,0)$ and $G(t;0,y)$, using Grothendieck's conjecture as an oracle.

† of order 11, and bidegree $(96,78)$ for $G(t;x,0)$, and $(68,28)$ for $G(t;0,y)$



Guessing and Proving

George Pólya

Guessing is good, proving is better.

Step (S3): warm-up – Gessel excursions are algebraic

Theorem. $g(t) := G(\sqrt{t};0,0) = \sum_{n=0}^{\infty} \frac{(5/6)_n(1/2)_n}{(5/3)_n(2)_n}(16t)^n$ is algebraic.

Step (S3): warm-up – Gessel excursions are algebraic

Theorem. $g(t) := G(\sqrt{t};0,0) = \sum_{n=0}^{\infty} \frac{(5/6)_n(1/2)_n}{(5/3)_n(2)_n}(16t)^n$ is algebraic.

Proof: First guess a polynomial $P(t,T)$ in $\mathbb{Q}[t,T]$, then prove that P admits the power series $g(t) = \sum_{n=0}^{\infty} g_n t^n$ as a root.

Step (S3): warm-up – Gessel excursions are algebraic

Theorem. $g(t) := G(\sqrt{t}; 0, 0) = \sum_{n=0}^{\infty} \frac{(5/6)_n (1/2)_n}{(5/3)_n (2)_n} (16t)^n$ is algebraic.

Proof: First guess a polynomial $P(t, T)$ in $\mathbb{Q}[t, T]$, then prove that P admits the power series $g(t) = \sum_{n=0}^{\infty} g_n t^n$ as a root.

1. Such a P can be guessed from the first 100 terms of $g(t)$.

Theorem. $g(t) := G(\sqrt{t};0,0) = \sum_{n=0}^{\infty} \frac{(5/6)_n (1/2)_n}{(5/3)_n (2)_n} (16t)^n$ is algebraic.

Proof: First guess a polynomial $P(t,T)$ in $\mathbb{Q}[t,T]$, then prove that P admits the power series $g(t) = \sum_{n=0}^{\infty} g_n t^n$ as a root.

1. Such a P can be guessed from the first 100 terms of $g(t)$.
2. Implicit function theorem: $\exists!$ root $r(t) \in \mathbb{Q}[[t]]$ of P.

Step (S3): warm-up – Gessel excursions are algebraic

Theorem. $g(t) := G(\sqrt{t};0,0) = \sum_{n=0}^{\infty} \frac{(5/6)_n(1/2)_n}{(5/3)_n(2)_n}(16t)^n$ is algebraic.

Proof: First guess a polynomial $P(t,T)$ in $\mathbb{Q}[t,T]$, then prove that P admits the power series $g(t) = \sum_{n=0}^{\infty} g_n t^n$ as a root.

1. Such a P can be guessed from the first 100 terms of $g(t)$.
2. Implicit function theorem: $\exists!$ root $r(t) \in \mathbb{Q}[[t]]$ of P.
3. $r(t) = \sum_{n=0}^{\infty} r_n t^n$ being algebraic, it is D-finite, and so is (r_n):

$$(n+2)(3n+5)r_{n+1} - 4(6n+5)(2n+1)r_n = 0, \qquad r_0 = 1$$

$\Rightarrow$ solution $r_n = \frac{(5/6)_n(1/2)_n}{(5/3)_n(2)_n}16^n = g_n$, thus $g(t) = r(t)$ is algebraic.

Step (S3): rigorous proof for Kreweras walks 

1. Setting $y_0 = \frac{x-t-\sqrt{x^2-2tx+t^2(1-4x^3)}}{2tx^2} = t + \frac{1}{x}t^2 + \frac{x^3+1}{x^2}t^3 + \cdots$ in the kernel equation

$$\underbrace{(xy - (x + y + x^2y^2)t)}_{\overset{!}{=}\, 0} K(t;x,y) = xy - xtK(t;x,0) - ytK(t;0,y)$$

Step (S3): rigorous proof for Kreweras walks 

1. Setting $y_0 = \frac{x-t-\sqrt{x^2-2tx+t^2(1-4x^3)}}{2tx^2} = t + \frac{1}{x}t^2 + \frac{x^3+1}{x^2}t^3 + \cdots$ in the kernel equation

$$\underbrace{(xy-(x+y+x^2y^2)t)}_{\overset{!}{=}\,0}K(t;x,y) = xy - xtK(t;x,0) - ytK(t;y,0)$$

Step (S3): rigorous proof for Kreweras walks 

1. Setting $y_0 = \frac{x-t-\sqrt{x^2-2tx+t^2(1-4x^3)}}{2tx^2} = t + \frac{1}{x}t^2 + \frac{x^3+1}{x^2}t^3 + \cdots$ in the kernel equation

$$\underbrace{(xy-(x+y+x^2y^2)t)}_{\overset{!}{=}\,0}K(t;x,y) = xy - xtK(t;x,0) - ytK(t;y,0)$$

shows that $U = K(t;x,0)$ satisfies the reduced kernel equation

$$\boxed{0 = x\cdot y_0 - x\cdot t\cdot U(t,x) - y_0\cdot t\cdot U(t,y_0)} \qquad \text{(RKerEq)}$$

Step (S3): rigorous proof for Kreweras walks 

1. Setting $y_0 = \frac{x-t-\sqrt{x^2-2tx+t^2(1-4x^3)}}{2tx^2} = t + \frac{1}{x}t^2 + \frac{x^3+1}{x^2}t^3 + \cdots$ in the kernel equation

$$\underbrace{(xy-(x+y+x^2y^2)t)}_{\overset{!}{=}\,0}K(t;x,y) = xy - xtK(t;x,0) - ytK(t;y,0)$$

shows that $U = K(t;x,0)$ satisfies the reduced kernel equation

$$\boxed{0 = x\cdot y_0 - x\cdot t\cdot U(t,x) - y_0\cdot t\cdot U(t,y_0)} \qquad \text{(RKerEq)}$$

2. $U = K(t;x,0)$ is the unique solution in $\mathbb{Q}[[x,t]]$ of (RKerEq).

Step (S3): rigorous proof for Kreweras walks 

1. Setting $y_0 = \frac{x-t-\sqrt{x^2-2tx+t^2(1-4x^3)}}{2tx^2} = t + \frac{1}{x}t^2 + \frac{x^3+1}{x^2}t^3 + \cdots$ in the kernel equation

$$\underbrace{(xy-(x+y+x^2y^2)t)}_{\stackrel{!}{=}\,0}K(t;x,y) = xy - xtK(t;x,0) - ytK(t;y,0)$$

shows that $U = K(t;x,0)$ satisfies the reduced kernel equation

$$\boxed{0 = x\cdot y_0 - x\cdot t\cdot U(t,x) - y_0\cdot t\cdot U(t,y_0)} \qquad \text{(RKerEq)}$$

2. $U = K(t;x,0)$ is the unique solution in $\mathbb{Q}[[x,t]]$ of (RKerEq).

3. The guessed candidate $\mathcal{P}_{x,0}$ has one solution $H(t,x)$ in $\mathbb{Q}[[x,t]]$.

Step (S3): rigorous proof for Kreweras walks 

1. Setting $y_0 = \frac{x-t-\sqrt{x^2-2tx+t^2(1-4x^3)}}{2tx^2} = t + \frac{1}{x}t^2 + \frac{x^3+1}{x^2}t^3 + \cdots$ in the kernel equation

$$\underbrace{(xy-(x+y+x^2y^2)t)}_{\overset{!}{=}\,0}K(t;x,y) = xy - xtK(t;x,0) - ytK(t;y,0)$$

   shows that $U = K(t;x,0)$ satisfies the reduced kernel equation

$$\boxed{0 = x\cdot y_0 - x\cdot t\cdot U(t,x) - y_0\cdot t\cdot U(t,y_0)} \qquad \text{(RKerEq)}$$

2. $U = K(t;x,0)$ is the unique solution in $\mathbb{Q}[[x,t]]$ of (RKerEq).

3. The guessed candidate $\mathcal{P}_{x,0}$ has one solution $H(t,x)$ in $\mathbb{Q}[[x,t]]$.

4. Resultant computations + verification of initial terms
   $\Longrightarrow \quad U = H(t,x)$ also satisfies (RKerEq).

Step (S3): rigorous proof for Kreweras walks 

1. Setting $y_0 = \frac{x-t-\sqrt{x^2-2tx+t^2(1-4x^3)}}{2tx^2} = t + \frac{1}{x}t^2 + \frac{x^3+1}{x^2}t^3 + \cdots$ in the kernel equation

$$\underbrace{(xy-(x+y+x^2y^2)t)}_{\stackrel{!}{=}0}K(t;x,y) = xy - xtK(t;x,0) - ytK(t;y,0)$$

shows that $U = K(t;x,0)$ satisfies the reduced kernel equation

$$\boxed{0 = x \cdot y_0 - x \cdot t \cdot U(t,x) - y_0 \cdot t \cdot U(t,y_0)} \qquad \text{(RKerEq)}$$

2. $U = K(t;x,0)$ is the unique solution in $\mathbb{Q}[[x,t]]$ of (RKerEq).

3. The guessed candidate $\mathcal{P}_{x,0}$ has one solution $H(t,x)$ in $\mathbb{Q}[[x,t]]$.

4. Resultant computations + verification of initial terms
   $\Longrightarrow \quad U = H(t,x)$ also satisfies (RKerEq).

5. Uniqueness: $H(t,x) = K(t;x,0) \implies K(t;x,0)$ is algebraic!

Algebraicity of Kreweras walks: a computer proof in a nutshell

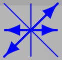
```
[bostan@inria ~]$ maple
    |\^/|     Maple 19 (APPLE UNIVERSAL OSX)
._|\|   |/|_. Copyright (c) Maplesoft, a division of Waterloo Maple Inc. 2014
 \  MAPLE  /  All rights reserved. Maple is a trademark of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.

# HIGH ORDER EXPANSION (S1)
> st,bu:=time(),kernelopts(bytesused):
> f:=proc(n,i,j)
  option remember;
    if i<0 or j<0 or n<0 then 0
    elif n=0 then if i=0 and j=0 then 1 else 0 fi
    else f(n-1,i-1,j-1)+f(n-1,i,j+1)+f(n-1,i+1,j) fi
  end:
> S:=series(add(add(f(k,i,0)*x^i,i=0..k)*t^k,k=0..80),t,80):

# GUESSING (S2)
> libname:=".",libname:gfun:-version();
                                      3.62
> gfun:-seriestoalgeq(S,Fx(t)):
> P:=collect(numer(subs(Fx(t)=T,%[1])),T):

# RIGOROUS PROOF (S3)
> ker := (T,t,x) -> (x+T+x^2*T^2)*t-x*T:
> pol := unapply(P,T,t,x):
> p1 := resultant(pol(z-T,t,x),ker(t*z,t,x),z):
> p2 := subs(T=x*T,resultant(numer(pol(T/z,t,z)),ker(z,t,x),z)):
> normal(primpart(p1,T)/primpart(p2,T));
                                        1

# time (in sec) and memory consumption (in Mb)
> trunc(time()-st),trunc((kernelopts(bytesused)-bu)/1000^2);
                                     7, 617
```

Step (S3): rigorous proof for Gessel walks 

Same strategy, but several complications:

- stepset diagonal symmetry is lost: $G(t;x,y) \neq G(t;y,x)$;
- $G(t;0,0)$ occurs in (KerEq) (because of the step $\swarrow$);
- equations are $\approx 5\,000$ times bigger.

$\longrightarrow$ replace equation (RKerEq) by a system of 2 reduced kernel equations.

$\longrightarrow$ fast algorithms needed (e.g., [B., Flajolet, Salvy & Schost 2006] for computations with algebraic series).

ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Symbolic Computation 41 (2006) 1–29

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Fast computation of special resultants

Alin Bostan[a,*], Philippe Flajolet[a], Bruno Salvy[a], Éric Schost[b]

[a] *Algorithms Project, Inria Rocquencourt, 78153 Le Chesnay, France*

[b] *LIX, École polytechnique, 91128 Palaiseau, France*

Received 3 September 2003; accepted 9 July 2005

Available online 25 October 2005

Summary

- ☺ Guess'n'Prove is a powerful method, especially when combined with efficient computer algebra

- ☺ It is robust: it can be used to uniformly prove algebraicity

- ☺ Brute-force and/or use of naive algorithms = hopeless.
  E.g. size of algebraic equations for $G(t; x, y) \approx 30\,\text{Gb}$.

INSIDE THE BOX

–Hermite-Padé approximants–

Definition

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

(1) $\mathbf{P} \cdot \mathbf{F} = P_1 f_1 + \cdots + P_n f_n = O(x^\sigma)$ with $\sigma = \sum_i (d_i + 1) - 1$,

(2) $\deg(P_i) \leq d_i$ for all i.

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

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

- [Hermite 1873]: e is transcendent.
- [Lindemann 1882]: π is transcendent; so does e^α for any $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$.
- [Apéry 1978, Beukers 1981]: $\zeta(3) = \sum_{n \geq 1} \frac{1}{n^3}$ is irrational.
- [Rivoal 2000]: there exist infinite values of k such that $\zeta(2k+1) \notin \mathbb{Q}$.

Worked example

Let us compute a Hermite-Padé approximant of type $(1,1,1)$ for $(1, C, C^2)$, where $C(x) = 1 + x + 2x^2 + 5x^3 + 14x^4 + 42x^5 + O(x^6)$.
This boils down to finding $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ (not all zero) such that

$$\alpha_0 + \alpha_1 x + (\beta_0 + \beta_1 x)(1 + x + 2x^2 + 5x^3 + 14x^4) + (\gamma_0 + \gamma_1 x)(1 + 2x + 5x^2 + 14x^3 + 42x^4) = O(x^5)$$

Identifying coefficients, this is equivalent to a homogeneous linear system:

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

By homogeneity, one can choose $\gamma_1 = 1$.
Then, the violet minor shows that one can take $(\beta_0, \beta_1, \gamma_0) = (-1, 0, 0)$.
The other values are $\alpha_0 = 1,\ \alpha_1 = 0$.

Thus the approximant is $(1, -1, x)$, which corresponds to $P = 1 - y + xy^2$ such that $P(x, C(x)) = 0 \bmod x^5$.

Algebraic and differential approximation = guessing

- Hermite-Padé approximants of $n = 2$ power series are related to Padé approximants, i.e. to approximation of series by rational functions
- algebraic approximants = Hermite-Padé approximants for $f_\ell = A^{\ell-1}$, where $A \in \mathbb{Q}[[x]]$ seriestoalgeq, listtoalgeq
- differential approximants = Hermite-Padé approximants for $f_\ell = A^{(\ell-1)}$, where $A \in \mathbb{Q}[[x]]$ seriestodiffeq, listtodiffeq

```
> listtoalgeq([1,1,2,5,14,42,132,429],y(x));
                                                  2
                          [1 - y(x) + x y(x) , ogf]

> listtodiffeq([1,1,2,5,14,42,132,429],y(x));
                                       / 2        \
                         /d      \     |d         |
[{-2 y(x) + (2 - 4 x) |-- y(x)| + x |--- y(x)|, y(0) = 1, D(y)(0) = 1}, egf]
                         \dx     /     |  2       |
                                       \dx        /
```

Existence and naive computation

Theorem For any vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{Q}[[x]]^n$ and for any n-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, there exists a Hermite-Padé approx. of type $\mathbf{d}$ for $\mathbf{F}$.

Proof: The undetermined coefficients of $P_i = \sum_{j=0}^{d_i} p_{i,j} x^j$ satisfy a linear homogeneous system with $\sigma = \sum_i (d_i + 1) - 1$ eqs and $\sigma + 1$ unknowns.

Corollary Computation in $O(\sigma^\omega)$, for $2 \leq \omega \leq 3$ (linear algebra exponent)

▷ There are better algorithms (the linear system is structured, Sylvester-like):

- Derksen's algorithm (Gaussian-like elimination) $O(\sigma^2)$
- Beckermann-Labahn's algorithm (DAC) $\tilde{O}(\sigma) = O(\sigma \log^2 \sigma)$

Theorem [Beckermann, Labahn, 1994] One can compute a Hermite-Padé approximant of type $(d, \dots, d)$ for $\mathbf{F} = (f_1, \dots, f_n)$ in $\tilde{O}(n^\omega d)$ ops. in $\mathbb{Q}$

Ideas:

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

Algorithm:

1. If $\sigma = n(d+1) - 1 \leq$ threshold, call the naive algorithm
2. Else:
   1. recursively compute $\mathbf{P}_1 \in \mathbb{Q}[x]^{n \times n}$ s.t. $\mathbf{P}_1 \cdot \mathbf{F} = O(x^{\sigma/2})$, $\deg(\mathbf{P}_1) \approx \frac{d}{2}$
   2. compute "residue" $\mathbf{R}$ such that $\mathbf{P}_1 \cdot \mathbf{F} = x^{\sigma/2} \cdot \left(\mathbf{R} + O(x^{\sigma/2})\right)$
   3. recursively compute $\mathbf{P}_2 \in \mathbb{Q}[x]^{n \times n}$ s.t. $\mathbf{P}_2 \cdot \mathbf{R} = O(x^{\sigma/2})$, $\deg(\mathbf{P}_2) \approx \frac{d}{2}$
   4. return $\mathbf{P} := \mathbf{P}_2 \cdot \mathbf{P}_1$

▷ The precise choices of degrees is a delicate issue

▷ Corollary: Gcd, extended gcd, Padé approximants in $\tilde{O}(d)$

INSIDE THE BOX

–Special resultants–

Conversion coefficients $\leftrightarrow$ power sums [Schönhage, 1982]

Any polynomial $F = x^n + a_1 x^{n-1} + \cdots + a_n$ in $\mathbb{Q}[x]$ can be represented by its first n power sums $S_i = \sum_{F(\alpha)=0} \alpha^i$

Conversions coefficients $\leftrightarrow$ power sums can be performed

- either in $O(n^2)$ using Newton identities (naive way):

$$i a_i + S_1 a_{i-1} + \cdots + S_i = 0, \quad 1 \le i \le n$$

- or in $\tilde{O}(n)$ using generating series

$$\frac{\mathsf{rev}(F)'}{\mathsf{rev}(F)} = -\sum_{i \ge 0} S_{i+1} x^i \quad \Longleftrightarrow \quad \mathsf{rev}(F) = \exp\left(-\sum_{i \ge 1} \frac{S_i}{i} x^i\right)$$

Manipulation of algebraic numbers: composed products and sums

$$F \otimes G = \prod_{F(\alpha)=0, G(\beta)=0} (x - \alpha\beta), \quad F \oplus G = \prod_{F(\alpha)=0, G(\beta)=0} (x - (\alpha + \beta))$$

Output size: $N = \deg(F)\deg(G)$

Linear algebra: χ_{xy}, χ_{x+y} in $\mathbb{Q}[x,y]/(F(x), G(y))$ $O(N^{\omega})$

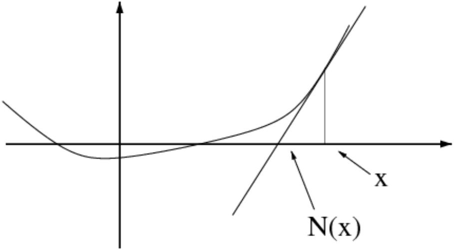
Resultants: $\mathrm{Res}_y\left(F(y), y^{\deg(G)} G(x/y)\right)$, $\mathrm{Res}_y\left(F(y), G(x-y)\right)$ $O(N^2)$

Better: $\otimes$ and $\oplus$ are easy in Newton representation $\tilde{O}(N)$

$$\sum \alpha^s \sum \beta^s = \sum (\alpha\beta)^s \qquad \text{and}$$

$$\sum \frac{\sum (\alpha+\beta)^s}{s!} x^s = \left(\sum \frac{\sum \alpha^s}{s!} x^s\right)\left(\sum \frac{\sum \beta^s}{s!} x^s\right)$$

Newton's tangent method: real case [Newton, 1671]



$$x_{\kappa+1} = \mathcal{N}(x_\kappa) = x_\kappa - (x_\kappa^2 - 2)/(2x_\kappa), \quad x_0 = 1$$

$$\begin{aligned}
x_1 &= 1.5000000000000000000000000000000\\
x_2 &= 1.4166666666666666666666666666667\\
x_3 &= 1.4142156862745098039215686274510\\
x_4 &= 1.4142135623746899106262955788901\\
x_5 &= 1.4142135623730950488016896235025
\end{aligned}$$

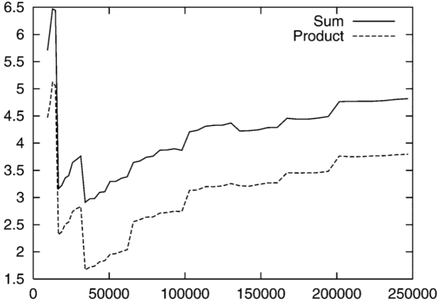
Newton's tangent method: power series case

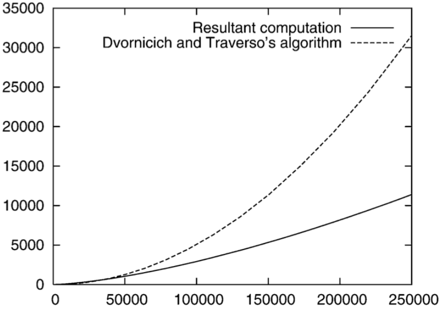
In order to solve $\varphi(x, g) = 0$ in $\mathbb{Q}[[x]]$ iterate

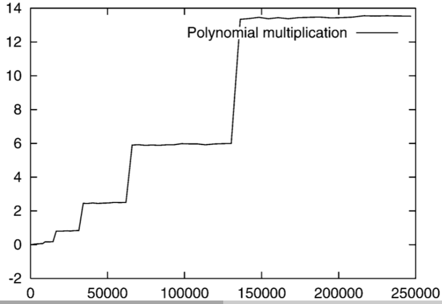
$$g_{\kappa+1} = g_\kappa - \frac{\varphi(g_\kappa)}{\varphi_y(g_\kappa)} \mod x^{2^{\kappa+1}}$$

- ▷ The number of correct coefficients doubles after each iteration
- ▷ Total cost $=$ **2** $\times \Big($ the cost of the last iteration $\Big)$

Theorem [Cook 1966, Sieveking 1972 & Kung 1974, Brent 1975]
Division, logarithm and exponential of power series in $\mathbb{Q}[[x]]$ can be computed at precision N using $\tilde{O}(N)$ operations in $\mathbb{Q}$


Sum
Product
6.5
6
5.5
5
4.5
4
3.5
3
2.5
2
1.5
0
50000
100000
150000
200000
250000


Resultant computation
Dvornicich and Traverso's algorithm
35000
30000
25000
20000
15000
10000
5000
0
0
50000
100000
150000
200000
250000


Polynomial multiplication
14
12
10
8
6
4
2
0
-2
0
50000
100000
150000
200000
250000

Thanks for your attention!