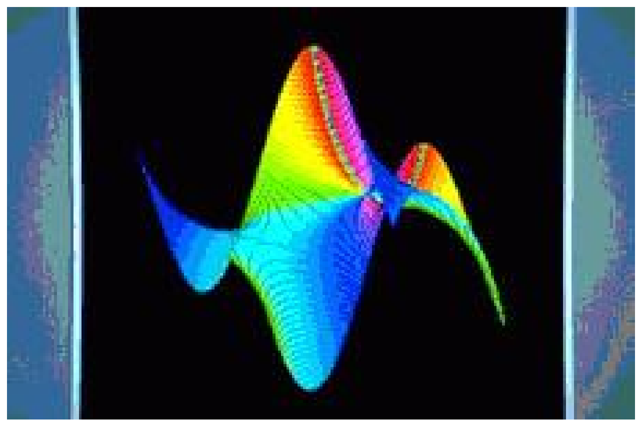
# Computer algebra for Combinatorics

Alin Bostan & Bruno Salvy



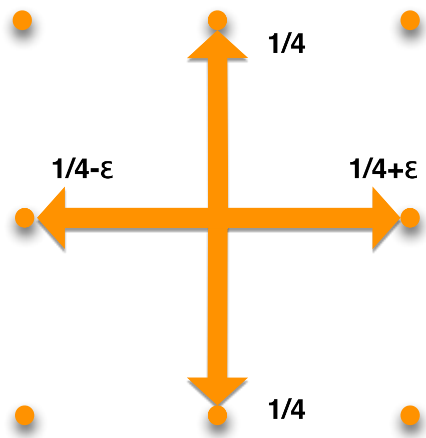
Algorithms Project, INRIA

ALEA 2012

# INTRODUCTION

## 1. Examples

# From the SIAM 100-Digit Challenge



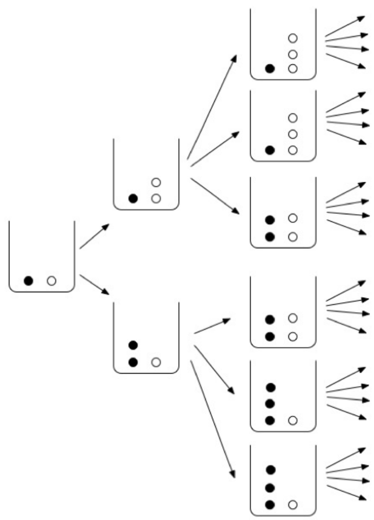

**Problem 6**

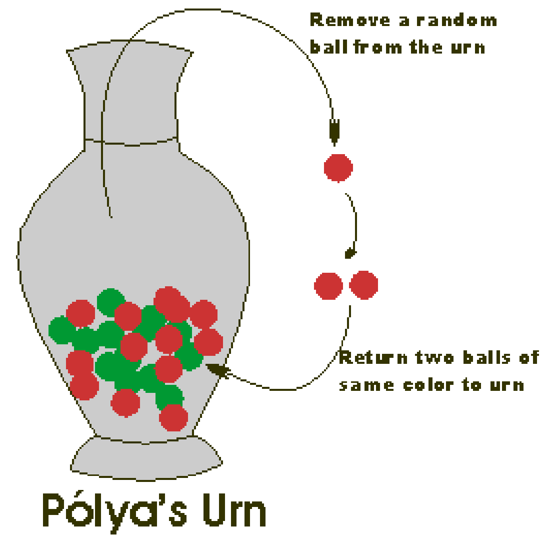
*A flea starts at $(0,0)$ on the infinite two-dimensional integer lattice and executes a biased random walk: At each step it hops north or south with probability $1/4$, east with probability $1/4+\epsilon$, and west with probability $1/4-\epsilon$. The probability that the flea returns to $(0,0)$ sometime during its wanderings is $1/2$. What is $\epsilon$?*

- Computer algebra conjectures and proves

$$p(\epsilon) = 1 - \sqrt{\frac{A}{2}} \cdot {}_2F_1\left( \left. \begin{matrix} \frac{1}{2}, \frac{1}{2} \\ 1 \end{matrix} \right| \frac{2\sqrt{1-16\epsilon^2}}{A} \right)^{-1}, \quad \text{with } A = 1 + 8\epsilon^2 + \sqrt{1-16\epsilon^2}.$$

# Algebraic balanced urns





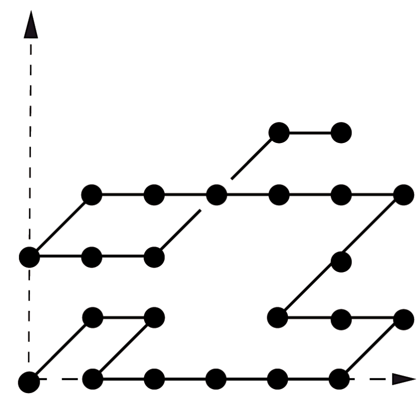

**Theorem [M.Fl11]**

The balanced urns class $\begin{pmatrix} 2\alpha & \beta \\ \alpha & \alpha+\beta \end{pmatrix}$, with $\alpha > 0, \beta \geqslant 0$, has an algebraic bivariate generating function.

- Computer algebra conjectures and proves larger classes of algebraic balanced urns.
- More in Basile Morcrette's talk!

# 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

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

▶ Computer algebra conjectures and proves:

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

$$G(1,1,t) = \frac{1}{2t} \cdot {}_2F_1\left( \begin{matrix} -1/12 & 1/4 \\ & 2/3 \end{matrix} \,\middle|\, -\frac{64t(4t+1)^2}{(4t-1)^4} \right) - \frac{1}{2t}.$$

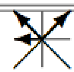
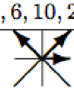
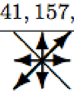
▶ A simpler variant as an exercise tomorrow.

---

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

# Inverse moment problem for walk sequences [B., Flajolet & Penson 2011]

Question: Given $(f_n)$, find $I \subseteq \mathbb{R}$ and $w : I \to \mathbb{R}$ s.t. $f_n = \int_I w(t)\, t^n \, dt \quad (n \geq 0)$.

| *Step set and walks sequence* | *GF* | *Measure* $(w(t))$; | $t$ : |
|---|---|---|---|
| **A126087**  $(1,1,3,5,15,29,87)$ | $\frac{2z-1+\sqrt{1-8z^2}}{2z(1-3z)}$ | $\frac{1}{2\pi}\frac{\sqrt{8-t^2}}{3-t}$ | $[-2\sqrt{2},2\sqrt{2}]$ |
| **A128386**  $(1,1,4,7,28,58,232,523,2092)$ | $\frac{2z-1+\sqrt{1-12z^2}}{2z(1-4z)}$ | $\frac{1}{2\pi}\frac{\sqrt{12-t^2}}{4-t}$ | $[-2\sqrt{3},2\sqrt{3}]$ |
| **A151282**  $(1,2,6,18,58,190,638)$ | $\frac{3z-1+\sqrt{1-2z-7z^2}}{2z(1-4z)}$ | $\frac{1}{2\pi}\frac{\sqrt{7+2t-t^2}}{4-t}$ | $[1-2\sqrt{2},1+2\sqrt{2}]$ |
| **A151292**  $(1,2,7,23,85,314,1207,4682)$ | $\frac{3z-1+\sqrt{1-2z-11z^2}}{2z(1-5z)}$ | $\frac{1}{2\pi}\frac{\sqrt{11+2t-t^2}}{5-t}$ | $[1-2\sqrt{3},1+2\sqrt{3}]$ |
| **A129400**  $(1,2,8,32,144,672,3264)$ | $\frac{1-2z-\sqrt{1-4z-12z^2}}{8z^2}$ | $\frac{1}{8\pi}\sqrt{(t+2)(6-t)}$ | $[-2,6]$ |
| **A151318**  $(1,3,13,55,249,1131,5253)$ | $\frac{5z-1+\sqrt{1-2z-15z^2}}{4z(1-5z)}$ | $\frac{1}{4\pi}\sqrt{\frac{3+t}{5-t}}$ | $[-3,5]$ |
| **A060899**  $(1,2,8,24,96,320,1280,4480)$ | $\frac{4z-1+\sqrt{1-16z^2}}{4z(1-4z)}$ | $\frac{1}{4\pi}\sqrt{\frac{4+t}{4-t}}$ | $[-4,4]$ |
| **A005773**  $(1,2,5,13,35,96,267,750,2123)$ | $\frac{3z-1+\sqrt{1-2z-3z^2}}{2z(1-3z)}$ | $\frac{1}{2\pi}\sqrt{\frac{1+t}{3-t}}$ | $[-1,3]$ |
| **A001405**  $(1,1,2,3,6,10,20,35,70,126)$ | $\frac{2z-1+\sqrt{1-4z^2}}{2z(1-2z)}$ | $\frac{1}{2\pi}\sqrt{\frac{2+t}{2-t}}$ | $[-2,2]$ |
| **A151281**  $(1,2,6,16,48,136,408,1184)$ | $\frac{4z-1+\sqrt{1-8z^2}}{4z(1-3z)}$ | $\frac{1}{4\pi}\frac{\sqrt{8-t^2}}{3-t}$ | $[-2\sqrt{2},2\sqrt{2}]$ |
| **A129637**  $(1,3,11,41,157,607,2367,9277)$ | $\frac{5z-1+\sqrt{1-2z-7z^2}}{4z(1-4z)}$ | $\frac{1}{4\pi}\frac{\sqrt{7+2t-t^2}}{4-t}$ | $[1-2\sqrt{2},1+2\sqrt{2}]$ |
| **A151323**  $(1,3,14,67,342,1790,9580)$ | $\frac{\sqrt[4]{\frac{1+2z}{1-6z}}-1}{2z}$ | $\frac{1}{2\sqrt{2}\pi}\sqrt[4]{\frac{2+t}{6-t}}$ | $[-2,6]$ |

# A SIAM Review combinatorial identity

*Problem* 87-8, *by* JOHN W. MOON (University of Alberta).

Show that

$$\sum_{n=1}^{\infty} \frac{56n^2+33n-8}{(n+2)(n+1)} f_n^2 = 1$$

where

$$f_n = \frac{4^{-n}}{n}\binom{2n-2}{n-1} \quad \text{for } n \geqq 1.$$

*Background.* A *branch* of a rooted tree $T_n$ is a maximal subtree that does not contain the root. A branch $B$ with $i$ nodes is a *primary* branch of $T_n$ if $n/2 \leqq i \leqq n-1$; if $T_n$ has a primary branch $B$ with $i$ nodes, then a branch $C$ with $j$ nodes is a *secondary* branch if $(n-i)/2 \leqq j \leqq n-1-i$. For many families $F$ of rooted trees, the fraction of trees $T_n$ in $F$ that have a primary branch tends to 1 as $n \to \infty$. (See A. Meir and J.W. Moon, *On major and minor branches of rooted trees*, Canad. J. Math., 39 (1987) 673-693). It can be shown that the fraction of plane trees $T_n$ that have a secondary branch tends to a limit $p$ as $n \to \infty$, where

$$p = 3 - 12 \sum_{n=1}^{\infty} \frac{13n^2+5n-2}{(n+1)(n+2)} f_n^2.$$

If we appeal to the proposed identity then we obtain the more rapidly converging expression

$$p = \frac{3}{14} + \frac{3}{14} \sum_{n=1}^{\infty} \frac{149n+8}{(n+1)(n+2)} f_n^2$$

from which we find that $p = .59 \cdots$.

- Computer algebra conjectures and proves $p = \frac{28}{15\pi}$.

# Monthly (AMM) problems with a combinatorial flavor that can be solved using computer algebra

**Expansion of a Symmetric Determinant**

E 2297 [1971, 543]. *Proposed by Richard Stanley, Harvard University*

Let $L(n)$ be the total number of distinct monomials appearing in the expansion of the determinant of an $n \times n$ symmetric matrix $A = (a_{ij})$. For instance, $L(3) = 5$. Show that

$$\sum_{n=0}^{\infty} L(n)x^n/n! = (1-x)^{-1/2}\exp(\tfrac{1}{2}x + \tfrac{1}{4}x^2),$$

where $|x| < 1$, and where we define $L(0) = 1$.

**Units of Chains**

6342 [1981, 294]. *Proposed by Richard Stanley, Massachusetts Institute of Technology.*

Let $f(n)$ be the number of nonisomorphic $n$-element partially ordered sets $P$ which do not contain three pairwise incomparable elements. (Equivalently, $P$ is a union of two chains.) Let

$$F(x) = 1 + \sum_{n \geq 1} f(n)x^n = 1 + x + 2x^2 + 4x^3 + 10x^4 + \cdots .$$

Show that

$$F(x) = \frac{4}{2 - 2x + \sqrt{1-4x} + \sqrt{1-4x^2}}.$$

### Noncrossing Trees

E 3170 [1986, 650]. *Proposed by The Howard University Group, Washington, D.C.*

Construct a graph as follows: Put $n + 1$ labeled vertices around a circle and let the edges be the straight line segments connecting any two vertices. A tree is noncrossing if no two edges intersect except at the vertices. Enumerate the number of noncrossing spanning trees for this graph. For $n = 1, 2, 3$, the numbers are 1, 3, 12, respectively.

## An Unexpected Appearance of the Catalan Numbers

**10905** [2001, 871]. *Proposed by Richard P. Stanley, Massachusetts Institute of Technology, Cambridge, MA.* Let $f(n) = \sum_P (-1)^{w(P)}$, where $P$ ranges over all lattice paths in the plane with $2n$ steps, starting and ending at the origin, with steps $(1, 0)$, $(0, 1)$, $(-1, 0)$, $(0, -1)$, and where $w(P)$ denotes the winding number of $P$ with respect to the point $(1/2, 1/2)$. Show that $f(n) = 4^n C_n$, where $C_n = \binom{2n}{n} \Big/ (n + 1)$, the $n$th Catalan number.

## Three-dimensional Lattice Walks in the Upper Half-Space

**10795** [2000, 367]. *Proposed by Emeric Deutsch, Polytechnic University, Brooklyn, NY.* A *3-dimensional lattice walk* of length $n$ takes $n$ successive unit steps, each in one of the six coordinate directions. How many 3-dimensional lattice walks of length $n$ are there that begin at the origin and never go below the horizontal plane?

## Another Type of Lattice Path

**10658** [1998, 366]. *Proposed by Emeric Deutsch, Polytechnic University, Brooklyn, NY.* Consider walks on the integer lattice in the plane that start at $(0,0)$, that stay in the first quadrant (they may touch the $x$-axis), and such that each step is either $(2,1)$, $(1,2)$, or $(1,-1)$. For each nonnegative integer $n$, how many paths are there to $(3n,0)$?

## The First Third

**6637 [1990, 621].** *Proposed by Herbert S. Wilf, University of Pennsylvania, Philadelphia, PA.*

Let $f(n)$ be the sum of the first one-third of the coefficients in the expansion of $(1+x)^{3n}$, i.e.,

$$f(n) = \sum_{k=0}^{n} \binom{3n}{k} \qquad (n = 0, 1, 2, \ldots).$$

Prove that

$$\sum_{n=0}^{\infty} f(n)\left(\frac{4u^2}{27}\right)^n = \frac{u}{u - 2\sin(\frac{1}{3}\arcsin u)} - \frac{2u}{2u - 3\sin(\frac{1}{3}\arcsin u)}.$$

**11501**. *Proposed by Finbarr Holland, University College Cork, Cork, Ireland.* (Correction) Let

$$g(z) = 1 - \frac{3}{\frac{1}{1-az} + \frac{1}{1-iz} + \frac{1}{1+iz}}.$$

Show that the coefficients in the Taylor series expansion of $g$ about 0 are all nonnegative if and only if $a \geq \sqrt{3}$.

**11567**. *Proposed by David Callan, University of Wisconsin-Madison, Madison, WI.* How many arrangements $(a_1, \ldots, a_{2n})$ of the multiset $\{1, 1, 2, 2, \ldots, n, n\}$ satisfy the following two conditions: (i) All entries between the two occurrences of any given value $i$ exceed $i$, and (ii) No three entries increase from left to right with the last two adjacent? (When $n = 3$, one such arrangement is 122133.)

**11573**. *Proposed by Rob Pratt, SAS Institute, Cary, NC.* A *Sudoku permutation matrix* (SPM) of order $n^2$ is a permutation matrix of order $n^2$ with exactly one 1 in each of the $n^2$ submatrices of order $n$ obtained by partitioning the original matrix into an $n$-by-$n$ array of submatrices. Thus, for $n = 2$, the permutation 1324 yields an SPM, but the identity permutation 1234 does not. Find the number of SPMs of order $n^2$.

**11610**. *Proposed by Richard P. Stanley, Massachussetts Institute of Technology, Cambridge, MA.* Let $f(n)$ be the number of binary words $a_1 \cdots a_n$ of length $n$ that have the same number of pairs $a_i a_{i+1}$ equal to 00 as equal to 01. Show that

$$\sum_{n=0}^{\infty} f(n)t^n = \frac{1}{2}\left(\frac{1}{1-t} + \frac{1+2t}{\sqrt{(1-t)(1-2t)(1+t+2t^2)}}\right).$$

► Last one as an exercise tomorrow.

# A money changing problem

Question[†]: The number of ways one can change any amount of banknotes of 10 €, 20 €, … using coins of 50 cents, 1 € and 2 € is always a perfect square.



[†] Free adaptation of Pb. 1, Ch. 1, p. 1, vol. 1 of Pólya and Szegö's Problems Book (1925)

This is equivalent to finding the number $M_{20k}$ of solutions $(a,b,c) \in \mathbb{N}^3$ of

$$a + 2b + 4c = 20k.$$

Euler-Comtet's denumerants: $$\sum_{n\geq 0} M_n x^n = \frac{1}{(1-x)(1-x^2)(1-x^4)}.$$

```
> f:=1/(1-x)/(1-x^2)/(1-x^4):
> S:=series(f,x,201):
> [seq(coeff(S,x,20*k),k=1..10)];
```

```
[36, 121, 256, 441, 676, 961, 1296, 1681, 2116, 2601]
```

```
> subs(n=20*k,gfun[ratpolytocoeff](f,x,n)):
```

$$\frac{17}{32} + \frac{(20k+1)(20k+2)}{16} + 5k + \frac{(-1)^{-20k}(20k+1)}{16} + \frac{5(-1)^{-20k}}{32} + \sum_{\alpha^2+1=0} \left( -\frac{(\frac{1}{16} - \frac{1}{16}\alpha)\alpha^{-20k}}{\alpha} \right)$$

```
> value(subs(_alpha^(-20*k)=1,%)):
> simplify(%) assuming k::posint:
> factor(%);
```

```
                    2
        (5 k + 1)
```

# INTRODUCTION

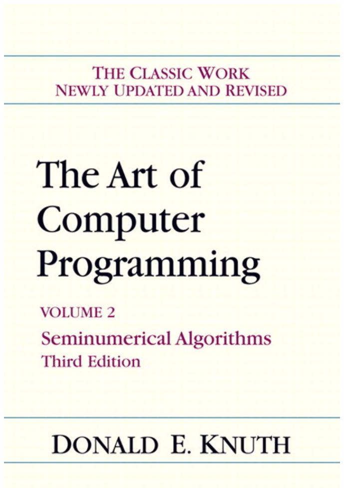
## 2. Computer Algebra

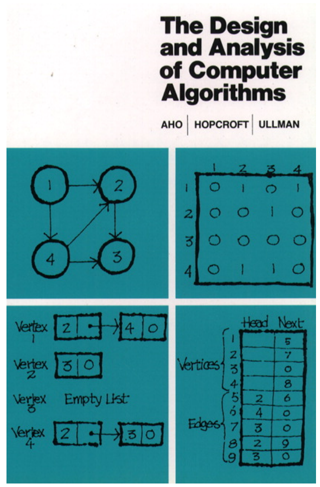
# General framework

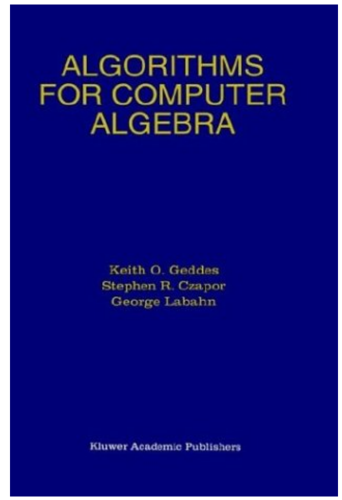
$$\text{Computer algebra} = \text{effective mathematics } and \text{ algebraic complexity}$$

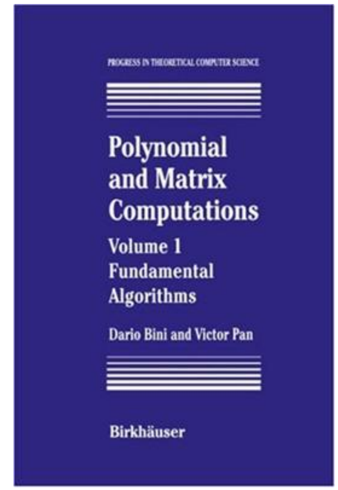
- Effective mathematics: what can we compute?
- their complexity: how fast?

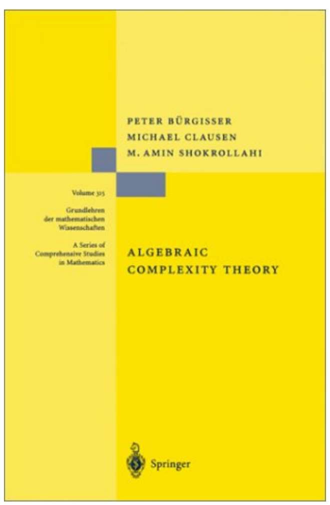
# Computer algebra books

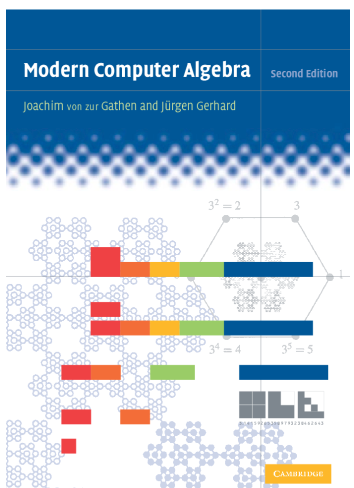


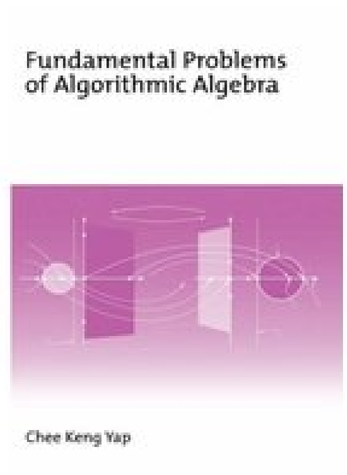



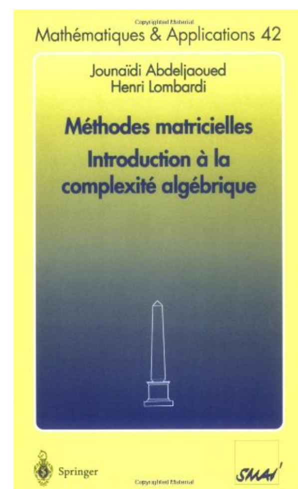



# Mathematical Objects

- Main objects
  - integers $\mathbb{Z}$
  - polynomials $\mathbb{K}[x]$
  - rational functions $\mathbb{K}(x)$
  - power series $\mathbb{K}[[x]]$
  - matrices $\mathcal{M}_r(\mathbb{K})$
  - linear recurrences with constant, or polynomial, coefficients $\mathbb{K}[n]\langle S_n \rangle$
  - linear differential equations with polynomial coefficients $\mathbb{K}[x]\langle \partial_x \rangle$

  where $\mathbb{K}$ is a field (generally supposed of characteristic 0 or large)

- Secondary/auxiliary objects
  - polynomial matrices $\mathcal{M}_r(\mathbb{K}[x])$
  - power series matrices $\mathcal{M}_r(\mathbb{K}[[x]])$

# Overview

Today

1. Introduction
2. High Precision Approximations
   – Fast multiplication, binary splitting, Newton iteration
3. Tools for Conjectures
   – Hermite-Padé approximants, $p$-curvature

Tomorrow morning

4. Tools for Proofs
   – Symbolic method, resultants, D-finiteness, creative telescoping

Tomorrow night

– Exercises with Maple

# HIGH PRECISION

## 1. Fast Multiplication

# Complexity yardsticks

Important features:

- addition is easy: naive algorithm already optimal
- multiplication is the most basic (non-trivial) problem
- almost all problems can be reduced to multiplication

Are there quasi-optimal algorithms for:

- integer/polynomial/power series multiplication? Yes!
- matrix multiplication? Big open problem!

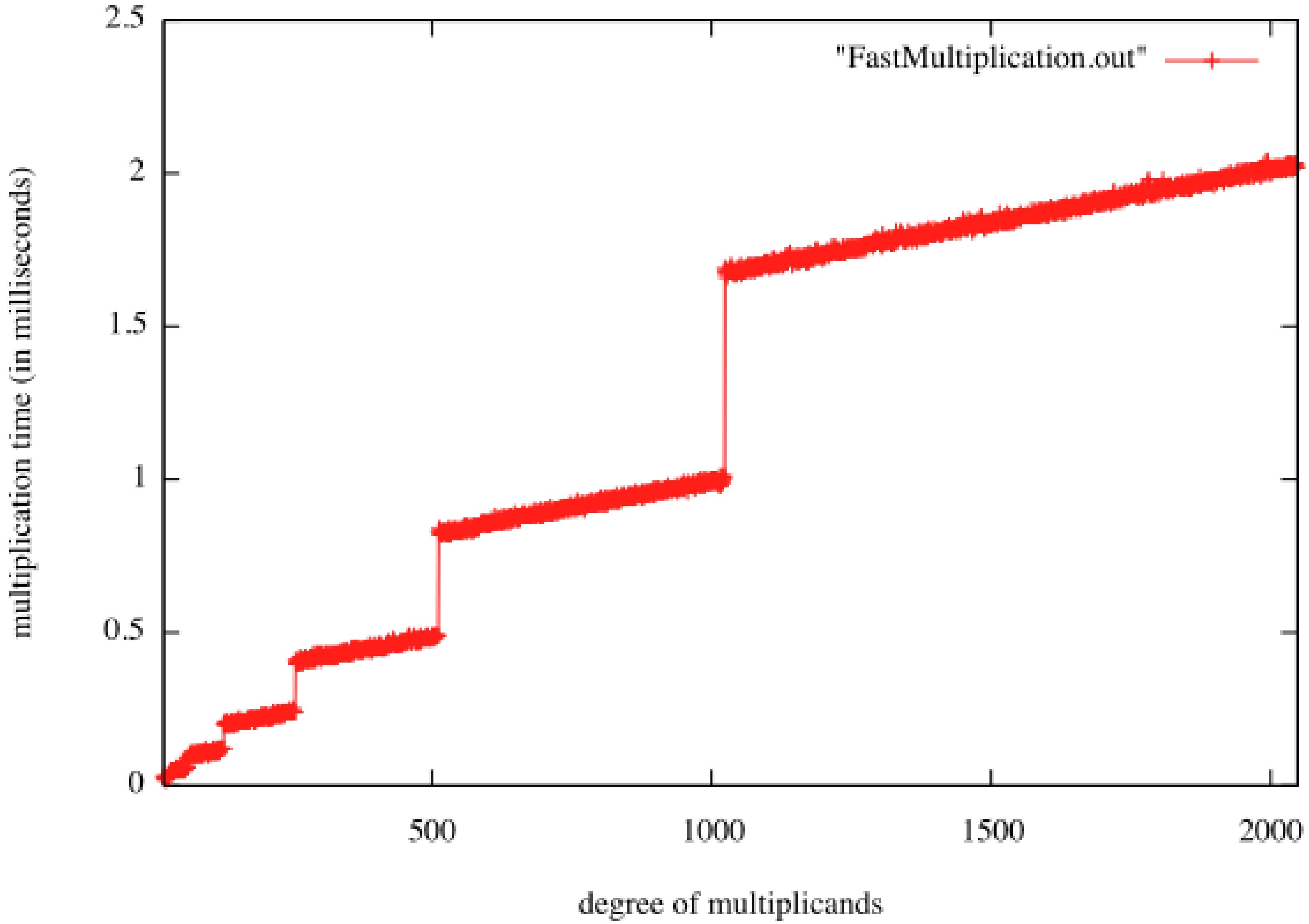
# Complexity yardsticks

$$
\begin{aligned}
\mathsf{M}(n) \quad &= \quad \text{complexity of } \textsf{multiplication} \text{ in } \mathbb{K}[x]_{<n}, \text{ and of } n\text{-bit integers} \\
&= \quad O(n^2) \ \text{ by the naive algorithm} \\
&= \quad O\big(n^{1.58}\big) \ \text{ by } \textsf{Karatsuba}\text{'s algorithm} \\
&= \quad O\big(n^{\log_\alpha (2\alpha-1)}\big) \ \text{ by the } \textsf{Toom-Cook} \text{ algorithm } (\alpha \geq 3) \\
&= \quad O\big(n \log n \operatorname{loglog} n\big) \ \text{ by the } \textsf{Schönhage-Strassen} \text{ algorithm}
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{MM}(r) \quad &= \quad \text{complexity of } \textsf{matrix product} \text{ in } \mathcal{M}_r(\mathbb{K}) \\
&= \quad O(r^3) \ \text{ by the naive algorithm} \\
&= \quad O(r^{2.81}) \ \text{ by } \textsf{Strassen}\text{'s algorithm} \\
&= \quad O(r^{2.38}) \ \text{ by the } \textsf{Coppersmith-Winograd} \text{ algorithm}
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{MM}(r,n) \quad &= \quad \text{complexity of } \textsf{polynomial matrix product} \text{ in } \mathcal{M}_r(\mathbb{K}[x]_{<n}) \\
&= \quad O(r^3\, \mathsf{M}(n)) \ \text{ by the naive algorithm} \\
&= \quad O(\mathsf{MM}(r)\, n \log(n) + r^2 n \log n \operatorname{loglog} n) \ \text{ by the } \textsf{Cantor-Kaltofen} \text{ algo} \\
&= \quad O(\mathsf{MM}(r)\, n + r^2\, \mathsf{M}(n)) \ \text{ by the } \textsf{B-Schost} \text{ algorithm}
\end{aligned}
$$

# Fast polynomial multiplication in practice




Practical complexity of Magma's multiplication in $\mathbb{F}_p[x]$, for $p = 29 \times 2^{57} + 1$.

# What can be computed in 1 minute with a CA system*

polynomial product† in degree 14,000,000 (>1 year with schoolbook)

product of two integers with 500,000,000 binary digits

factorial of $N = 20,000,000$ (output of 140,000,000 digits)

gcd of two polynomials of degree 600,000

resultant of two polynomials of degree 40,000

factorization of a univariate polynomial of degree 4,000

factorization of a bivariate polynomial of total degree 500

resultant of two bivariate polynomials of total degree 100 (output 10,000)

product/sum of two algebraic numbers of degree 450 (output 200,000)

determinant (char. polynomial) of a matrix with 4,500 (2,000) rows

determinant of an integer matrix with 32-bit entries and 700 rows

---

*on a PC, (Intel Xeon X5160, 3GHz processor, with 8GB RAM), running Magma V2.16-7

†in $\mathbb{K}[x]$, for $\mathbb{K} = \mathbb{F}_{67108879}$

# Discrete Fourier Transform

[Gauss 1866, Cooley-Tukey 1965]

DFT Problem: Given $n = 2^k$, $f \in \mathbb{K}[x]_{<n}$, and $\omega \in \mathbb{K}$ a primitive $n$-th root of unity, compute $(f(1), f(\omega), \ldots, f(\omega^{n-1}))$

Idea: Write $f = f_{\text{even}}(x^2) + x f_{\text{odd}}(x^2), \quad$ with $\deg(f_{\text{even}}), \deg(f_{\text{odd}}) < n/2$.

Then $f(\omega^j) = f_{\text{even}}(\omega^{2j}) + \omega^j f_{\text{odd}}(\omega^{2j})$, and $(\omega^{2j})_{0 \le j < n} = \frac{n}{2}$-roots of 1.

Complexity: $\quad \mathsf{F}(n) = 2 \cdot \mathsf{F}(n/2) + O(n) \quad \Longrightarrow \quad \mathsf{F}(n) = O(n \log n)$

# Inverse DFT

IDFT Problem: Given $n = 2^k$, $v_0, \ldots, v_{n-1} \in \mathbb{K}$ and $\omega \in \mathbb{K}$ a primitive $n$-th root of unity, compute $f \in \mathbb{K}[x]_{<n}$ such that $f(1) = v_0, \ldots, f(\omega^{n-1}) = v_{n-1}$

- $V_\omega \cdot V_{\omega^{-1}} = n \cdot I_n \;\; \rightarrow \;\;$ performing the inverse DFT in size $n$ amounts to:
  - performing a DFT at
$$\frac{1}{1}, \;\; \frac{1}{\omega}, \;\; \ldots, \;\; \frac{1}{\omega^{n-1}}$$
  - dividing the results by $n$.
- this new DFT is the same as before:
$$\frac{1}{\omega^i} = \omega^{n-i},$$
  so the outputs are just shuffled.

Consequence: the cost of the inverse DFT is $O(n \log(n))$

# FFT polynomial multiplication

Suppose the basefield $\mathbb{K}$ contains enough roots of unity

To multiply two polynomials $f, g$ in $\mathbb{K}[x]$, of degrees $< n$:

- find $N = 2^k$ such that $h = fg$ has degree less than $N$ $\quad N \leq 4n$
- compute DFT$(f, N)$ and DFT$(g, N)$ $\quad O(N \log(N))$
- multiply pointwise these values to get DFT$(h, N)$ $\quad O(N)$
- recover $h$ by inverse DFT $\quad O(N \log(N))$

Complexity: $O(N \log(N)) = O(n \log(n))$

General case: Create artificial roots of unity $\quad O(n \log(n) \log \log n)$

# HIGH PRECISION

## 2. Binary Splitting

# Example: fast factorial

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

Naive iterative way: unbalanced multiplicands $\tilde{O}(N^2)$

- 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 $\tilde{O}(N)$.

- Extends to matrix factorials $A(N)A(N-1)\cdots A(1)$ $\tilde{O}(N)$
  $\longrightarrow$ recurrences of arbitrary order.

# Application to recurrences

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 $\tilde{O}(N^2)$ bit ops.

Binary splitting: $U_n = (u_n, \ldots, u_{n+r-1})^T$ satisfies the 1st order recurrence

$$U_{n+1} = \frac{1}{p_r(n)} A(n) U_n \quad \text{with} \quad A(n) = \begin{bmatrix} & p_r(n) & & \\ & & \ddots & \\ & & & p_r(n) \\ -p_0(n) & -p_1(n) & \ldots & -p_{r-1}(n) \end{bmatrix}.$$

$\Longrightarrow u_N$ reads off the matrix factorial $A(N-1)\cdots A(0)$

[Chudnovsky-Chudnovsky, 1987]: Binary splitting strategy $\tilde{O}(N)$ bit ops.

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

[Brent 1976]

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

Recurrence $e_n - e_{n-1} = 1/n! \iff n(e_n - e_{n-1}) = e_{n-1} - e_{n-2}$ rewrites

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

- $e_N$ in $\tilde{O}(N)$ bit operations [Brent 1976]
- generalizes to the evaluation of any D-finite series at an algebraic number [Chudnovsky-Chudnovsky 1987] $\tilde{O}(N)$ bit ops.

# Implementation in gfun

[Mezzarobba, S. 2010]

```
> rec:={n*(e(n) - e(n-1)) = e(n-1) - e(n-2), e(0)=1, e(1)=2};
> pro:=rectoproc(rec,e(n));
```

```
pro := proc(n::nonnegint)
local i1, loc0, loc1, loc2, tmp2, tmp1, i2;
    if n <= 22 then
        loc0 := 1;
        loc1 := 2;
        if n = 0 then return loc0
        else for i1 to n - 1 do
                loc2 := (-loc0 + loc1 + loc1*(i1 + 1))/(i1 + 1); loc0 := loc1; loc1 := loc2
            end do
        end if; loc1
    else
        tmp1 := `gfun/rectoproc/binsplit`([
            'ndmatrix'(Matrix([[0, i2 + 2], [-1, i2 + 3]]), i2 + 2), i2, 0, n,
            matrix_ring(ad, pr, ze, ndmatrix(Matrix(2, 2, [[...],[...]],
            datatype = anything, storage = empty, shape = [identity]), 1)),
            expected_entry_size], Vector(2, [...], datatype = anything));
        tmp1 := subs({e(0) = 1, e(1) = 2}, tmp1);  tmp1
    end if
end proc
```

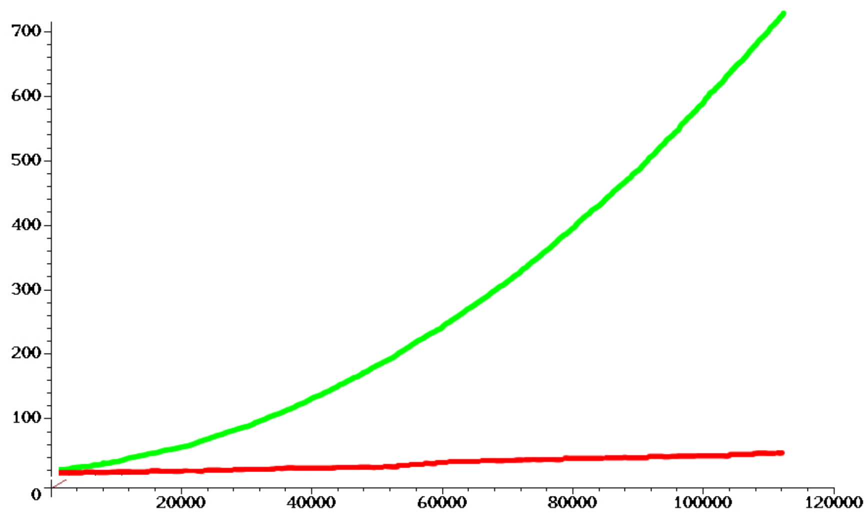
```
> tt:=time(): x:=pro(50000): time()-tt, evalf(x-exp(1), 200000);
```

1.827, 0.

# Application: record computation of $\pi$

[Chudnovsky-Chudnovsky 1987] fast convergence hypergeometric identity

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



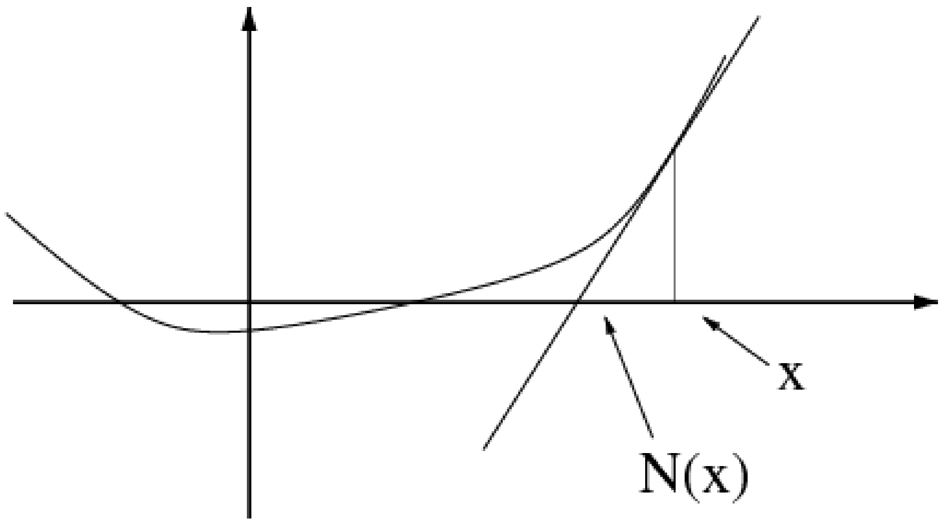

- Used in Maple & Mathematica: 1st order recurrence, yields 14 correct digits per iteration $\longrightarrow$ 4 billion digits [Chudnovsky-Chudnovsky 1994]
- Current record on a PC: 10000 billion digits [Kondo & Yee 2011]

# HIGH PRECISION

## 3. Newton Iteration

# Newton's tangent method: real case

[Newton, 1671]




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

$$x_1 = 1.50000000000000000000000000000000$$

$$x_2 = 1.41666666666666666666666666666667$$

$$x_3 = 1.41421568627450980392156862745098$$

$$x_4 = 1.41421356237468991062629557889013$$

$$x_5 = 1.41421356237309504880168962350253$$

# Newton's tangent method: power series case

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

$$x_1 = 1 - \frac{1}{2}t$$

$$x_2 = 1 - \frac{1}{2}t - \frac{1}{8}t^2 - \frac{1}{16}t^3 - \frac{1}{32}t^4 - \frac{1}{64}t^5 - \frac{1}{128}t^6 - \frac{1}{256}t^7 - \frac{1}{512}t^8 - \frac{1}{1024}t^9 + \cdots$$

$$x_3 = 1 - \frac{1}{2}t - \frac{1}{8}t^2 - \frac{1}{16}t^3 - \frac{5}{128}t^4 - \frac{7}{256}t^5 - \frac{21}{1024}t^6 - \frac{33}{2048}t^7 - \frac{107}{8192}t^8 - \frac{177}{16384}t$$

# Newton's tangent method: power series case

In order to solve $\varphi(x, g) = 0$ in $\mathbb{K}[[x]]$ (where $\varphi \in \mathbb{K}[[x, y]]$, $\varphi(0, 0) = 0$ and $\varphi_y(0, 0) \neq 0$), iterate

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

$$g - g_{\kappa+1} = g - g_\kappa + \frac{\varphi(g) + (g_\kappa - g)\varphi_y(g) + O((g - g_\kappa)^2)}{\varphi_y(g) + O(g - g_\kappa)} = O((g - g_\kappa)^2).$$

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

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

# Division, logarithm and exponential of power series

[Sieveking1972, Kung1974, Brent1975]

To compute the reciprocal of $f \in \mathbb{K}[[x]]$ with $f(0) \neq 0$, choose $\varphi(g) = 1/g - f$:

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

Complexity: $\mathsf{C}(N) = \mathsf{C}(N/2) + O(\mathsf{M}(N)) \implies \mathsf{C}(N) = O(\mathsf{M}(N))$

Corollary: division of power series at precision $N$ in $O(\mathsf{M}(N))$

# Division, logarithm and exponential of power series
[Sieveking1972, Kung1974, Brent1975]

To compute the reciprocal of $f \in \mathbb{K}[[x]]$, choose $\varphi(g) = 1/g - f$:

$$g_0 = 1/f_0 \quad \text{and} \quad g_{\kappa+1} = g_\kappa + g_\kappa(1 - f g_\kappa) \quad \bmod x^{2^{\kappa+1}} \qquad \text{for } \kappa \geq 0.$$

Complexity: $\mathsf{C}(N) = \mathsf{C}(N/2) + O(\mathsf{M}(N)) \qquad \Longrightarrow \qquad \mathsf{C}(N) = O(\mathsf{M}(N))$

Corollary: division of power series at precision $N$ in $O(\mathsf{M}(N))$

Corollary: Logarithm $\log(f) = -\sum_{i \geq 1} \frac{(1-f)^i}{i}$ of $f \in 1 + x\mathbb{K}[[x]]$ in $O(\mathsf{M}(N))$:

- compute the Taylor expansion of $h = f'/f$ modulo $x^{N-1}$ — $O(\mathsf{M}(N))$
- take the antiderivative of $h$ — $O(N)$

# Division, logarithm and exponential of power series

[Sieveking1972, Kung1974, Brent1975]

To compute the reciprocal of $f \in \mathbb{K}[[x]]$, choose $\varphi(g) = 1/g - f$:

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

Complexity: $\mathsf{C}(N) = \mathsf{C}(N/2) + O(\mathsf{M}(N)) \quad \Longrightarrow \quad \mathsf{C}(N) = O(\mathsf{M}(N))$

Corollary: division of power series at precision $N$ in $O(\mathsf{M}(N))$

Corollary: Logarithm $\log(f) = -\sum_{i \geq 1} \frac{(1-f)^i}{i}$ of $f \in 1 + x\mathbb{K}[[x]]$ in $O(\mathsf{M}(N))$:

- compute the Taylor expansion of $h = f'/f$ modulo $x^{N-1}$ $\quad O(\mathsf{M}(N))$
- take the antiderivative of $h$ $\quad O(N)$

Corollary: Exponential $\exp(f) = \sum_{i \geq 0} \frac{f^i}{i!}$ of $f \in x\mathbb{K}[[x]]$. Use $\phi(g) = \log(g) - f$:

$$g_0 = 1 \quad \text{and} \quad g_{\kappa+1} = g_\kappa - g_\kappa\left(\log(g_\kappa) - f\right) \quad \bmod x^{2^{\kappa+1}} \qquad \text{for } \kappa \geq 0.$$

Complexity: $\mathsf{C}(N) = \mathsf{C}(N/2) + O(\mathsf{M}(N)) \quad \Longrightarrow \quad \mathsf{C}(N) = O(\mathsf{M}(N))$

# Application: Euclidean division for polynomials

[Strassen, 1973]

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

Naive algorithm: $O(N^2)$

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

Let $N = \deg(F)$ and $n = \deg(G)$. Then $\deg(Q) = N - n$, $\deg(R) < n$ and

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

Algorithm:

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

# Application: conversion coefficients $\leftrightarrow$ power sums

[Schönhage, 1982]

Any polynomial $F = x^n + a_1 x^{n-1} + \cdots + a_n$ in $\mathbb{K}[x]$ 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):

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

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

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

# Application: special bivariate resultants

[B-Flajolet-S-Schost, 2006]

Composed products and sums: manipulation of algebraic numbers

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

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

Linear algebra: $\chi_{xy}, \chi_{x+y}$ in $\mathbb{K}[x,y]/(F(x), G(y))$ $O(\mathsf{MM}(N))$

Resultants: $\mathrm{Res}_y\left(F(y), y^{\deg(G)} G(x/y)\right)$, $\mathrm{Res}_y\left(F(y), G(x-y)\right)$ $O(N^{1.5})$

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

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

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

Corollary: Fast polynomial shift $P(x+a) = P(x) \oplus (x+a)$ $O(\mathsf{M}(\deg(P)))$

# Newton iteration on power series: operators and systems

In order to solve an equation $\phi(Y) = 0$, with $\phi : (\mathbb{K}[[x]])^r \to (\mathbb{K}[[x]])^r$,

1. Linearize: $\phi(Y_\kappa - U) = \phi(Y_\kappa) - D\phi|_{Y_\kappa} \cdot U + O(U^2)$,
   where $D\phi|_Y$ is the differential of $\phi$ at $Y$.
2. Iterate: $Y_{\kappa+1} = Y_\kappa - U_{\kappa+1}$, where $U_{\kappa+1}$ is found by
3. Solve linear equation: $D\phi|_{Y_k} \cdot U = \phi(Y_\kappa)$ with $\operatorname{val} U > 0$.

Then, the sequence $Y_\kappa$ converges quadratically to the solution $Y$.

# Application: inversion of power series matrices

[Schulz, 1933]

To compute the inverse $Z$ of a matrix of power series $Y \in \mathcal{M}_r(\mathbb{K}[[x]])$:

- Choose the map $\phi : Z \mapsto I - YZ$ with differential $D\phi|_Y : U \mapsto -YU$
- Equation for $U$: $-YU = I - YZ_\kappa \mod x^{2^{\kappa+1}}$
- Solution: $U = -Y^{-1}(I - YZ_\kappa) = -Z_\kappa (I - YZ_\kappa) \bmod x^{2^{\kappa+1}}$

This yields the following Newton-type iteration for $Y^{-1}$

$$Z_{\kappa+1} = Z_\kappa + Z_\kappa(I_r - YZ_\kappa) \mod x^{2^{\kappa+1}}$$

Complexity:

$\mathsf{C}_{\mathrm{inv}}(N) = \mathsf{C}_{\mathrm{inv}}(N/2) + O(\mathsf{MM}(r, N)) \quad \Longrightarrow \quad \mathsf{C}_{\mathrm{inv}}(N) = O(\mathsf{MM}(r, N))$

# Application: non-linear systems

In order to solve a system $Y = H(Y) = \phi(Y) + Y$, with $H : (\mathbb{K}[[x]])^r \to (\mathbb{K}[[x]])^r$, such that $I_r - \partial H/\partial Y$ is invertible at 0.

1. Linearize: $\phi(Y_\kappa - U) - \phi(Y_\kappa) = U - \partial H/\partial Y(Y_\kappa) \cdot U + O(U^2)$.
2. Iterate $Y_{\kappa+1} = Y_\kappa - U_{\kappa+1}$, where $U_{\kappa+1}$ is found by
3. Solve linear equation: $(I_r - \partial H/\partial Y(Y_\kappa)) \cdot U = H(Y_\kappa) - Y_\kappa$ with $\operatorname{val} U > 0$.

This yields the following Newton-type iteration:

$$\begin{cases} Z_{\kappa+1} & = Z_\kappa + Z_\kappa(I_r - (I_r - \partial H/\partial Y(Y_\kappa))Z_\kappa) \mod x^{2^{\kappa+1}} \\ Y_{\kappa+1} & = Y_\kappa - Z_{\kappa+1}(H(Y_\kappa) - Y_\kappa) \mod x^{2^{\kappa+1}} \end{cases}$$

computing simultaneously a matrix and a vector.

# Example: Mappings

```
> mappings:={M=Set(Cycle(Tree)),Tree=Prod(Z,Set(Tree))}:
> combstruct[gfeqns](mappings,labeled,x);
```

$$\left[M(x) = \frac{1}{1 - \mathit{Tree}(x)}, \quad \mathit{Tree}(x) = x\exp(\mathit{Tree}(x))\right]$$

```
> countmappings:=SeriesNewtonIteration(mappings,labelled,x):
> countmappings(10);
```

$$\Big[M = 1 + x + 2\,x^2 + \frac{9}{2}x^3 + \frac{32}{3}x^4 + \frac{625}{24}x^5 + \frac{324}{5}x^6 + \frac{117649}{720}x^7 + \frac{131072}{315}x^8 + \frac{4782969}{4480}x^9 + O\left(x^{10}\right),$$

$$\mathit{Tree} = x + x^2 + \frac{3}{2}x^3 + \frac{8}{3}x^4 + \frac{125}{24}x^5 + \frac{54}{5}x^6 + \frac{16807}{720}x^7 + \frac{16384}{315}x^8 + \frac{531441}{4480}x^9 + O\left(x^{10}\right)\Big]$$

Code Pivoteau-S-Soria, should end up in `combstruct`

# Application: quasi-exponential of power series matrices

[B-Chyzak-Ollivier-Salvy-Schost-Sedoglavic 2007]

To compute the solution $Y \in \mathcal{M}_r(\mathbb{K}[[x]])$ of the system $Y' = AY$

- choose the map $\phi : Y \mapsto Y' - AY$, with differential $\phi$.
- the equation for $U$ is $\quad U' - AU = Y'_\kappa - AY_\kappa \mod x^{2^{\kappa+1}}$
- the method of variation of constants yields the solution
  $U = Y_\kappa V_\kappa \bmod x^{2^{\kappa+1}}$, $\;Y'_\kappa - AY_\kappa = Y_\kappa V'_\kappa \bmod x^{2^{\kappa+1}}$

This yields the following Newton-type iteration for $Y$:

$$Y_{\kappa+1} = Y_\kappa - Y_\kappa \int Y_\kappa^{-1} \left(Y'_\kappa - AY_\kappa\right) \mod x^{2^{\kappa+1}}$$

Complexity:

$\mathsf{C}_{\mathrm{solve}}(N) = \mathsf{C}_{\mathrm{solve}}(N/2) + O(\mathsf{MM}(r,N)) \quad \Longrightarrow \quad \mathsf{C}_{\mathrm{solve}}(N) = O(\mathsf{MM}(r,N))$

# TOOLS FOR CONJECTURES

## 1. Hermite-Padé Approximants

# Definition

Definition: Given a column vector $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ 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 $\mathbf{P} = (P_1, \ldots, P_n) \in \mathbb{K}[x]^n$, $(\mathbf{P} \neq 0)$, 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 $i$.

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

- Very useful concept in number theory (transcendence theory):
  - [Hermite, 1873]: $e$ is transcendent.
  - [Lindemann, 1882]: $\pi$ is transcendent, and so does $e^\alpha$ for any $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$.
  - [Beukers, 1981]: reformulate Apéry's proof that $\zeta(3) = \sum_n \frac{1}{n^3}$ is irrational.
  - [Rivoal, 2000]: there exist an infinite number 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 $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ such that

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

By 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 $A \in \mathbb{K}[[x]]$ seriestoalgeq, listtoalgeq
- differential approximants = Hermite-Padé approximants for $f_\ell = A^{(\ell-1)}$, where $A \in \mathbb{K}[[x]]$ 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 $\mathbf{F} = (f_1, \ldots, f_n)^T \in \mathbb{K}[[x]]^n$ and for any $n$-tuple $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$, there exists a Hermite-Padé approximant 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 $\sigma = \sum_i (d_i + 1) - 1$ equations and $\sigma + 1$ unknowns.

Corollary Computation in $O(\mathsf{MM}(\sigma)) = O(\sigma^\theta)$, for $2 \leq \theta \leq 3$.

- There are better algorithms:
  - The linear system is structured (Sylvester-like / quasi-Toeplitz)
  - Derksen's algorithm (Gaussian-like elimination) $O(\sigma^2)$
  - Beckermann-Labahn's algorithm (DAC) $\tilde{O}(\sigma) = O(\sigma \log^2 \sigma)$

# Quasi-optimal computation

Theorem [Beckermann-Labahn, 1994] One can compute a Hermite-Padé approximant of type $(d, \ldots, d)$ for $\mathbf{F} = (f_1, \ldots, f_n)$ in $O(\mathsf{MM}(n, d) \log(nd))$.

Ideas:

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

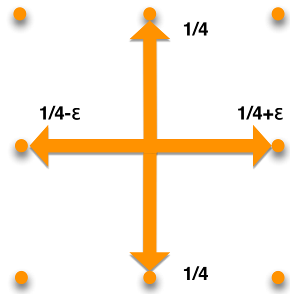
Algorithm:

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

▶ The precise choices of degrees is a delicate issue

▶ Gcd, extended gcd, Padé approximants in $O(\mathsf{M}(n) \log n)$

# Example: Flea from SIAM 100-Digit Challenge




```
> proba:=proc(i,j,n,c)
option remember;
  if abs(i)+abs(j)>n then 0
  elif n=0 then 1
  else
      expand(proba(i-1,j,n-1,c)*(1/4+c)+proba(i+1,j,n-1,c)*(1/4-c)
      +proba(i,j+1,n-1,c)*1/4+proba(i,j-1,n-1,c)*1/4)
  fi
end:
> seq(proba(0,0,k,c),k=0..6);
```

$$1, 0, \frac{1}{4} - 2c^2, 0, \frac{9}{64} - \frac{9}{4}c^2 + 6c^4, 0, \frac{25}{256} - \frac{75}{32}c^2 + 15c^4 - 20c^6$$

```
> gfun:-listtodiffeq([seq(proba(0,0,2*k,c),k=0..20)],y(x));
```

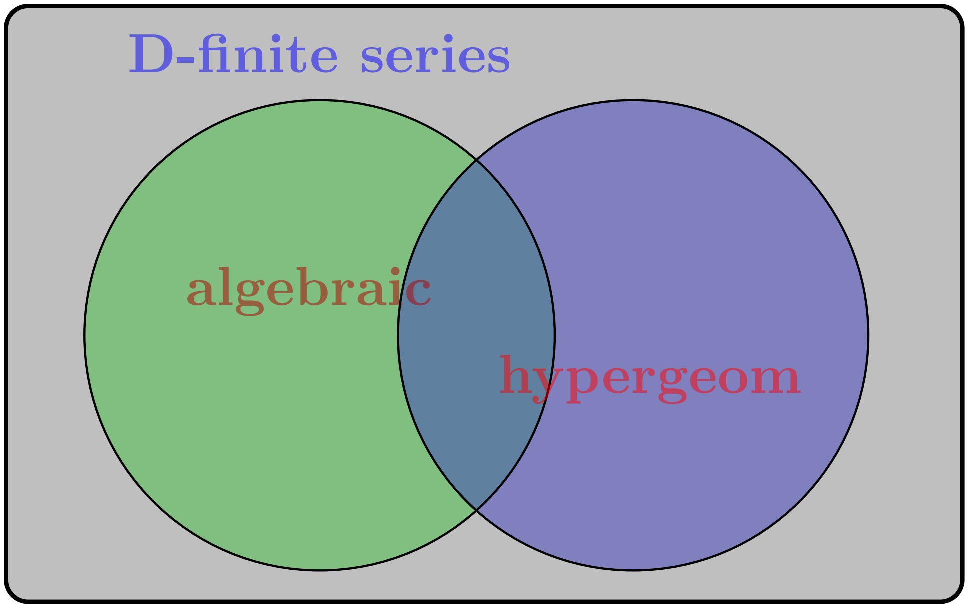
$$[\{ \left(-1+8\,c^2+48\,xc^4\right) y\left(x\right)+\left(4-8\,x+64\,xc^2+192\,x^2c^4\right) \frac{d}{dx}y\left(x\right) + \left(4\,x+64\,x^3c^4-4\,x^2+32\,x^2c^2\right) \frac{d^2}{dx^2}y\left(x\right), y\left(0\right)=1, \mathrm{D}\left(y\right)\left(0\right)=1/4-2\,c^2\}, ogf]$$

Next steps: `dsolve` (+ help) and evaluation at $x = 1$.

# TOOLS FOR CONJECTURES

## 2. $p$-Curvature of Differential Operators

# Important classes of power series




Algebraic: $S(x) \in \mathbb{K}[[x]]$ root of a polynomial $P \in \mathbb{K}[x, y]$.

D-finite: $S(x) \in \mathbb{K}[[x]]$ satisfying a linear differential equation with polynomial (or rational function) coefficients $c_r(x)S^{(r)}(x) + \cdots + c_0(x)S(x) = 0$.

Hypergeometric: $S(x) = \sum_n s_n x^n$ such that $\frac{s_{n+1}}{s_n} \in \mathbb{K}(n)$. E.g.

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

# Linear differential operators

Definition: If $\mathbb{K}$ is a field, $\mathbb{K}\langle x, \partial; \partial x = x\partial + 1\rangle$, or simply $\mathbb{K}(x)\langle\partial\rangle$, denotes the associative algebra of linear differential operators with coefficients in $\mathbb{K}(x)$.

$\mathbb{K}[x]\langle\partial\rangle$ is called the (rational) Weyl algebra. It is the algebraic formalization of the notion of linear differential equation with rational function coefficients:

$$a_r(x)y^{(r)}(x) + \cdots + a_1(x)y'(x) + a_0(x)y(x) = 0$$

$$\Longleftrightarrow$$

$$L(y) = 0, \quad \text{where} \quad L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

The commutation rule $\partial x = x\partial + 1$ formalizes Leibniz's rule $(fg)' = f'g + fg'$.

▶ Implementation in the `DEtools` package: `diffop2de, de2diffop, mult`

```
DEtools[mult](Dx,x,[Dx,x]);
                                    x Dx + 1
```

# Weyl algebra is Euclidean

Theorem [Libri 1833, Brassinne 1864, Wedderburn 1932, Ore 1932]
$\mathbb{K}(x)\langle\partial\rangle$ is a non-commutative (left and right) Euclidean domain: for any $A, B \in \mathbb{K}(x)\langle\partial\rangle$, there exist unique operators $Q, R \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$A = QB + R, \qquad \text{and} \quad \deg_\partial(R) < \deg_\partial(B).$$

This is called the Euclidean right division of $A$ by $B$.

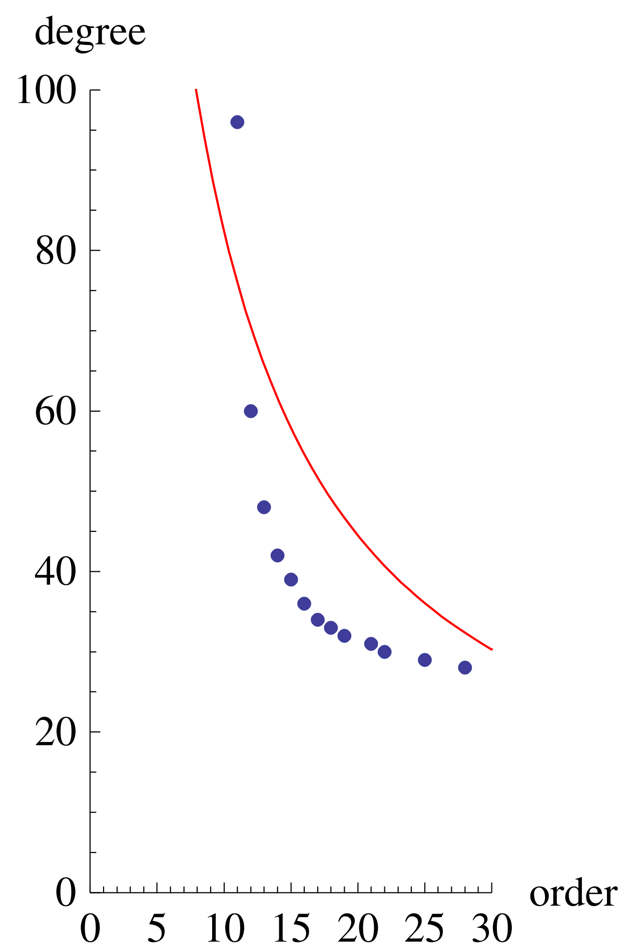
Moreover, any $A, B \in \mathbb{K}(x)\langle\partial\rangle$ admit a greatest common right divisor (GCRD) and a least common left multiple (LCLM). They can be computed by a non-commutative version of the extended Euclidean algorithm.

- `rightdivision, GCRD, LCLM` from the `DEtools` package

```
> rightdivision(Dx^10,Dx^2-x,[Dx,x])[2];
                            3                   2    5
                     (20 x  + 80) Dx + 100 x  + x
```

proves that $\mathrm{Ai}^{(10)}(x) = (20x^3 + 80)\mathrm{Ai}'(x) + (100x^2 + x^5)\mathrm{Ai}(x)$

# Application to differential guessing




1000 terms of a series are enough to guess candidate differential equations below the red curve. GCRD of candidates could jump above the red curve.

# The Grothendieck–Katz $p$-curvatures conjecture

**Q**: when does a differential equation possess a basis of algebraic solutions?

E.g. for the Gauss hypergeometric equation $x(1-x)\partial^2 + (\gamma - (\alpha+\beta+1)x)\partial - \alpha\beta x$, Schwarz's list (1873) classifies algebraic ${}_2F_1$'s in terms of $\alpha, \beta, \gamma$

Conjecture [Grothendieck, 1960's, unpublished; Katz, 1972]
Let $A \in \mathbb{Q}(x)^{n\times n}$. The system (S) : $y' = Ay$ has a full set of algebraic solutions if and only if, for almost all prime numbers $p$, the system ($\mathsf{S}_p$) defined by reduction of (S) modulo $p$ has a full set of algebraic solutions over $\mathbb{F}_p(x)$.

Definition: The $p$-curvature of (S) is the matrix $A_p$, where

$$A_0 = I_n, \quad \text{and} \quad A_{\ell+1} = A_\ell' + A_\ell A \quad \text{for} \quad \ell \geq 0.$$

Theorem [Cartier, 1957]
The sufficient condition of the G.-K. Conjecture is equivalent to $A_p = 0 \bmod p$.

- For each $p$, this can be checked algorithmically.

# Grothendieck's conjecture

**Q**: when does a differential equation possess a basis of algebraic solutions?

For a scalar differential equation, the G.-K. Conjecture can be reformulated:

Grothendieck's Conjecture: Suppose $L \in \mathbb{K}(x)\langle\partial\rangle$ is irreducible. The equation (E) : $L(y) = 0$ has a basis of algebraic solutions if and only if, for almost all prime numbers $p$, the operator $L$ right-divides $\partial^p$ modulo $p$.

- For each $p$, this can be checked algorithmically.

- Conjecture is proved for Picard-Fuchs equations [Katz 1972] (in particular, for diagonals [Christol 1984]), for ${}_nF_{n-1}$ equations [Beukers & Heckman 1989].

# Grothendieck's conjecture for combinatorics

Suppose that we have guessed a linear differential equation $L(f) = 0$ (by differential Hermite-Padé approximation) for some power series $f \in \mathbb{Q}[[x]]$, and that we want to recognize whether $f$ is algebraic or not.

Recipe 1: try algebraic guessing.

Recipe 2: For several primes $p$, compute $p$-curvatures mod $p$, and check whether they are zero; equivalently, test if $\partial^p \bmod L = 0 \pmod{p}$.

▶ For many power series coming from counting problems (diagonals, constant terms, integrals of algebraic functions, ...) Grothendieck's conjecture is true.

# Grothendieck's conjecture at work

Chebychev in his work on the distribution of primes numbers used the following fact

$$u_n := \frac{(30n)!n!}{(15n)!(10n)!(6n)!} \in \mathbb{Z}, \qquad n = 0, 1, 2, \ldots$$

This is not immediately obvious (for example, this ratio of factorials is not a product of multinomial coefficients) but it is not hard to prove. The only proof I know proceeds by checking that the valuations $v_p(u_n)$ are non-negative for every prime $p$; an interpretation of $u_n$ as counting natural objects or being dimensions of natural vector spaces is far from clear.

As it turns out, the generating function

$$u := \sum_{\nu \geq 1} u_n \lambda^n$$

is algebraic over $\mathbb{Q}(\lambda)$; i.e. there is a polynomial $F \in \mathbb{Z}[x, y]$ such that

$$F(\lambda, u(\lambda)) = 0.$$

However, we are not likely to see this polynomial explicitly any time soon as its degree is $483, 840$ (!)

(excerpt from Rodriguez-Villegas's "Integral ratios of factorials")

- Algebraicity of $u$ can be however guessed using any prior knowledge, by computing $p$-curvatures of the (minimal) order-8 operator $L$ s.t. $L(u) = 0$
- For $p < 300$, they are all zero, except when $p \in \{11, 13, 17, 19, 23\}$

# $G$-series and global nilpotence

Definition: 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) $\exists\, C > 0$, $\operatorname{lcm}(b_0, \ldots, b_n) \leq C^n$.

Basic examples: (1) algebraic functions [Eisenstein 1852]
(2) $-\log(1-x) = \sum_{n\geq 1} x^n/n$ ([Chebyshev 1852] $\operatorname{lcm}(1, 2, \ldots, n) \leq 4^n$)
(3) ${}_2F_1\left(\begin{matrix}\alpha\ \ \beta\\ \gamma\end{matrix}\,\middle|\, x\right)$, $\alpha, \beta, \gamma \in \mathbb{Q}$
(4) OGF of any $P$-recursive, integer-valued, exponentially bounded, sequence

Theorem [Chudnovsky 1985] The minimal-order linear differential operator annihilating a $G$-series is globally nilpotent: for almost all prime numbers $p$, it right-divides $\partial^{p\mu}$ modulo $p$, for some $\mu \leq \deg_\partial L$.
(this condition is equivalent to the nilpotence mod $p$ of the $p$-curvature matrix)

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

# Global nilpotence for combinatorics

Suppose we have guessed (by differential approximation) a linear differential equation $L(f) = 0$ for a power series $f \in \mathbb{Q}[[x]]$ which is a $G$-series (typically, the OGF of a $P$-recursive, integer-valued, exponentially bounded, sequence).

A way to empirically certify that $L$ is very plausible:

Recipe: compute $p$-curvatures mod $p$, and check whether they are nilpotent; equivalently, test if $\partial^{pr} \bmod L = 0 \pmod{p}$, where $r = \deg_\partial L$

Example:

```
> L:=x^2*(64*x^4+40*x^3-30*x^2-5*x+1)*Dx^3+
      x*(576*x^4+200*x^3-252*x^2-33*x+5)*Dx^2+
       4*(1+288*x^4+22*x^3-117*x^2-12*x)*Dx+384*x^3-12-144*x-72*x^2:
> p:=7; for j to 3 do N:=rightdivision(Dx^(3*p),L,[Dx,x])[2] mod p;
        p:=nextprime(p); print(p, N); od:

                                11, 0
                                13, 0
                                17, 0
```

# Overview

Today

1. Introduction
2. High Precision Approximations
   – Fast multiplication, binary splitting, Newton iteration
3. Tools for Conjectures
   – Hermite-Padé approximants, $p$-curvature

Tomorrow morning

4. Tools for Proofs
   – Symbolic method, resultants, D-finiteness, creative telescoping

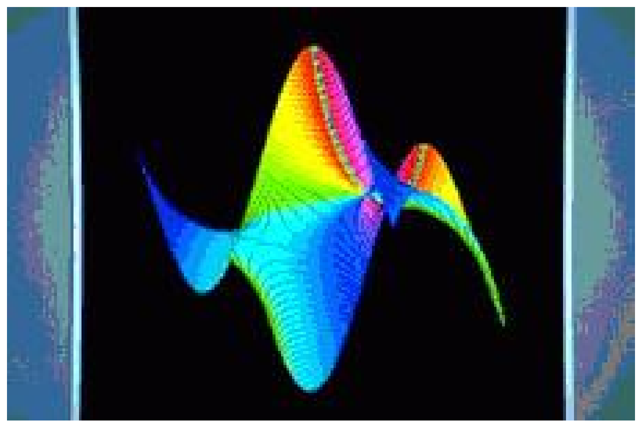
Tomorrow night

– Exercises with Maple

# Computer algebra for Combinatorics

Part II

Alin Bostan & Bruno Salvy



Algorithms Project, INRIA

ALEA 2012

# Overview

### Yesterday

1. Introduction
2. High Precision Approximations
   – Fast multiplication, binary splitting, Newton iteration
3. Tools for Conjectures
   – Hermite-Padé approximants, $p$-curvature

### This Morning

4. Tools for Proofs
   – Symbolic method, resultants, D-finiteness, creative telescoping

### Tonight

– Exercises with Maple

# TOOLS FOR PROOFS

## 1. Symbolic Method

# Language

Context-free grammars (UNION, PROD, SEQUENCE), plus SET, CYCLE.
Origins: [Pólya37, Joyal81,...]
Labelled and unlabelled universes.

Examples:

| | |
|---|---|
| Binary trees | B=UNION(Z,PROD(B,B)) |
| Mappings | M=SET(CYCLE(Tree)), |
| | Tree=PROD(Z,SET(Tree)) |
| Permutations | P=SET(CYCLE(Z)) |
| Children rounds | R=SET(PROD(Z,CYCLE(Z))) |
| Integer partitions | P=SET(SEQUENCE(Z)) |
| Set partitions | P=SET(SET(Z,card>0)) |
| Irreducible polynomials mod $p$ | P=SET(Irred), P=SEQUENCE(Coeff). |

Aim: a complete library for enumeration, random generation, generating functions of structures "defined" like this (`combstruct`).

# Generating Function Dictionary

Definition: Exponential and Ordinary Generating Functions of a class $\mathcal{A}$:

$$A(x) = \sum_{n \geq 0} A_n \frac{x^n}{n!}, \quad \tilde{A}(x) = \sum_{n \geq 0} \tilde{A}_n x^n,$$

where $A_n$ (resp. $\tilde{A}_n$) is the number of labeled (resp. unlabeled) elements of size $n$ in $\mathcal{A}$.

| structure | EGF | OGF |
|---|---|---|
| $\textsc{Union}(\mathcal{A}, \mathcal{B})$ | $A(x) + B(x)$ | $\tilde{A}(x) + \tilde{B}(x)$ |
| $\textsc{Prod}(\mathcal{A}, \mathcal{B})$ | $A(x) \times B(x)$ | $\tilde{A}(x) \times \tilde{B}(x)$ |
| $\textsc{Seq}(\mathcal{C})$ | $\frac{1}{1-C(x)}$ | $\frac{1}{1-\tilde{C}(x)}$ |
| $\textsc{Cyc}(\mathcal{C})$ | $\log \frac{1}{1-C(x)}$ | $\sum_{k \geq 1} \frac{\phi(k)}{k} \log \frac{1}{1-\tilde{C}(x^k)}$ |
| $\textsc{Set}(\mathcal{C})$ | $\exp(C(x))$ | $\exp(\tilde{C}(x) + \frac{1}{2}\tilde{C}(x^2) + \frac{1}{3}\tilde{C}(x^3) + \cdots)$ |

Proof. [Labeled product]

$$\sum_{\gamma=(\alpha,\beta)\in\textsc{Prod}(\mathcal{A},\mathcal{B})} \frac{x^{|\gamma|}}{|\gamma|!} = \sum_{\alpha\in\mathcal{A}} \sum_{\beta\in\mathcal{B}} \underbrace{\binom{|\gamma|}{|\alpha|}}_{\text{relabeling}} \frac{x^{|\alpha|+|\beta|}}{|\gamma|!}$$

$$= \sum_{\alpha} \frac{x^{|\alpha|}}{|\alpha|!} \times \sum_{\beta} \frac{x^{|\beta|}}{|\beta|!}.$$

Proof. [Unlabeled set]

$$\begin{aligned}
\sum_{c \in \textsc{Set}(\mathcal{C})} x^{|c|} &= \prod_{c \in \mathcal{C}} (1 + x^{|c|} + x^{2|c|} + \cdots) \\
&= \exp \log \prod \cdots \\
&= \exp\left(\sum_{c \in \mathcal{C}} \log \frac{1}{1 - x^{|c|}}\right) \\
&= \exp\left(\sum_{c \in \mathcal{C}} \sum_{k>0} \frac{x^{k|c|}}{k}\right) \\
&= \exp\left(\sum_{k>0} \frac{1}{k} \sum_{c \in \mathcal{C}} x^{k|c|}\right) \\
&= \exp(\tilde{C}(x) + \frac{1}{2}\tilde{C}(x^2) + \cdots).
\end{aligned}$$

# Examples

| | | |
|---|---|---|
| Binary trees | B=Union(Z,Prod(B,B)) | $B(x) = x + B^2(x)$ |
| Mappings | M=Set(Cycle(Tree)) | $M(x) = \exp\left(\log \frac{1}{1-T(x)}\right)$ |
| | Tree=Prod(Z,Set(Tree)) | $T(x) = x \exp(T(x))$ |
| Permutations | P=Set(Cycle(Z)) | $P(x) = \exp(\log \frac{1}{1-x})$ |
| Children rounds | R=Set(Prod(Z,Cycle(Z))) | $R(x) = (1-x)^{-x}$ |
| Integer partitions | P=Set(Sequence(Z)) | $P(x) = \exp(\frac{x}{1-x} + \frac{x^2/2}{1-x^2} + \cdots)$ |
| Set partitions | P=Set(Set(Z,card>0)) | $P(x) = \exp(e^x - 1)$ |
| Irreducible pols | P=Set(Irred) | $P(x) = \exp(I(x) + \frac{1}{2}I(x^2) + \cdots$ |
| mod $p$ | P=Sequence(Coeff) | $= \frac{1}{1-px}$ |

# Examples

| | | |
|---|---|---|
| Binary trees | B=Union(Z,Prod(B,B)) | $B(x) = x + B^2(x)$ |
| Mappings | M=Set(Cycle(Tree)) | $M(x) = \exp\left(\log \frac{1}{1-T(x)}\right)$ |
| | Tree=Prod(Z,Set(Tree)) | $T(x) = x\exp(T(x))$ |
| Permutations | P=Set(Cycle(Z)) | $P(x) = \exp(\log \frac{1}{1-x})$ |
| Children rounds | R=Set(Prod(Z,Cycle(Z))) | $R(x) = (1-x)^{-x}$ |
| Integer partitions | P=Set(Sequence(Z)) | $P(x) = \exp(\frac{x}{1-x} + \frac{x^2/2}{1-x^2} + \cdots)$ |
| Set partitions | P=Set(Set(Z,card>0)) | $P(x) = \exp(e^x - 1)$ |
| Irreducible pols | P=Set(Irred) | $P(x) = \exp(I(x) + \frac{1}{2}I(x^2) + \cdots$ |
| mod $p$ | P=Sequence(Coeff) | $= \frac{1}{1-px}$ |

```
> mappings:={M=Set(Cycle(Tree)),Tree=Prod(Z,Set(Tree))}:
> combstruct[gfeqns](mappings,labeled,x);
```

$$\left[M(x) = \frac{1}{1 - \mathit{Tree}(x)}, \quad \mathit{Tree}(x) = x\exp(\mathit{Tree}(x))\right]$$

# Constructible Classes [Flajolet-Sedgewick]

Definition. Well-founded system: $\mathcal{Y} = \mathcal{H}(\mathcal{Z}, \mathcal{Y})$ such that $Y_{n+1} = H(x, Y_n)$ with $Y_0 = 0$ converges to a (vector of) power series (with no 0 coordinate).

# Constructible Classes [Flajolet-Sedgewick]

Definition. Well-founded system: $\mathcal{Y} = \mathcal{H}(\mathcal{Z}, \mathcal{Y})$ such that $Y_{n+1} = H(x, Y_n)$ with $Y_0 = 0$ converges to a (vector of) power series (with no 0 coordinate).

Definition. Constructible classes: Constructed from $\{1, \mathcal{Z}, \mathcal{Y}_1, \mathcal{Y}_2, \dots\}$ (with $|\mathcal{Z}| = 1$ and $|\mathcal{Y}_i| = 0$) by compositions with

- Union, Prod, Sequence, Set, Cycle (with cardinality restricted to intervals);
- the solution of well-founded systems $\mathcal{Y} = \mathcal{H}(\mathcal{Z}, \mathcal{Y})$ where the coordinates of $\mathcal{H}$ are constructible.

# Constructible Classes [Flajolet-Sedgewick]

Definition. Well-founded system: $\mathcal{Y} = \mathcal{H}(\mathcal{Z}, \mathcal{Y})$ such that $Y_{n+1} = H(x, Y_n)$ with $Y_0 = 0$ converges to a (vector of) power series (with no 0 coordinate).

Definition. Constructible classes: Constructed from $\{1, \mathcal{Z}, \mathcal{Y}_1, \mathcal{Y}_2, \dots\}$ (with $|\mathcal{Z}| = 1$ and $|\mathcal{Y}_i| = 0$) by compositions with

- Union, Prod, Sequence, Set, Cycle (with cardinality restricted to intervals);
- the solution of well-founded systems $\mathcal{Y} = \mathcal{H}(\mathcal{Z}, \mathcal{Y})$ where the coordinates of $\mathcal{H}$ are constructible.

Theorem [Pivoteau-S.-Soria] Enumeration of all constructible classes with precision $N$ in $O(\mathsf{M}(N))$ coefficient operations.

Idea: Newton's iteration ($\rightarrow$ yesterday's slides).

Soon to be in `combstruct[count]`

# Example: Mappings

```
> mappings:={M=Set(Cycle(Tree)),Tree=Prod(Z,Set(Tree))}:
> combstruct[gfeqns](mappings,labeled,x);
```

$$\left[M(x) = \frac{1}{1 - \mathit{Tree}(x)}, \quad \mathit{Tree}(x) = x \exp(\mathit{Tree}(x))\right]$$

```
> countmappings:=SeriesNewtonIteration(mappings,labelled,x):
> countmappings(10);
```

$$\left[M = 1 + x + 2\,x^2 + \frac{9}{2}x^3 + \frac{32}{3}x^4 + \frac{625}{24}x^5 + \frac{324}{5}x^6 + \frac{117649}{720}x^7 + \frac{131072}{315}x^8 + \frac{4782969}{4480}x^9 + O\left(x^{10}\right), \mathit{Tree} = x + x^2 + \frac{3}{2}x^3 + \frac{8}{3}x^4 + \frac{125}{24}x^5 + \frac{54}{5}x^6 + \frac{16807}{720}x^7 + \frac{16384}{315}x^8 + \frac{531441}{4480}x^9 + O\left(x^{10}\right)\right]$$

Code Pivoteau-S-Soria, should end up in `combstruct`

# Multivariate Generating Functions

Same translation rules:

```
> maps2:={M=Set(Cycle(Prod(U,Tree))),Tree=Prod(Z,Set(Tree)),U=Epsilon}:
> combstruct[gfsolve](maps2,labeled,z,[[u,U]]);
```

$$\left\{ M(z,u) = \frac{1}{1+uW(-z)}, \mathit{Tree}(z,u) = -W(-z), U(z,u) = u, Z(z,u) = z \right\}$$

This computes

$$M(z,u) = \sum_{n,k} c_{n,k} u^k \frac{z^n}{n!},$$

$c_{n,k}$ = number of mappings with $n$ points, $k$ of which are in cycles.

# Multivariate Generating Functions

Same translation rules:

```
> maps2:={M=Set(Cycle(Prod(U,Tree))),Tree=Prod(Z,Set(Tree)),U=Epsilon}:
> combstruct[gfsolve](maps2,labeled,z,[[u,U]]);
```

$$\left\{M(z,u) = \frac{1}{1+uW(-z)}, \mathit{Tree}(z,u) = -W(-z), U(z,u) = u, Z(z,u) = z\right\}$$

```
> gf:=subs(%,M(z,u)):
```

Some automatic asymptotics (avg number of points in cycles):

```
> map(simplify,equivalent(eval(gf,u=1),z,n));
```

$$1/2\,\frac{\sqrt{2}n^{-1/2}\mathrm{e}^n}{\sqrt{\pi}} + O\left(\mathrm{e}^n n^{-3/2}\right)$$

```
> map(simplify,equivalent(eval(diff(gf,u),u=1),z,n));
```

$$1/2\,\mathrm{e}^n + O\left(\mathrm{e}^n n^{-1/2}\right)$$

```
> asympt(%/%%,n);
```

$$1/2\,\sqrt{2}\sqrt{\pi}n^{1/2} + O\left(1\right)$$

# Also in `combstruct`

- `gfeqns`: generating function equations;
- `gfseries`: generating function expansions;
- `count`: number of objects of a given size;
- `draw`: uniform random generation;
- `agfeqns`, `agfseries`, `agfmomentsolve`: extensions to attribute grammars (see [Delest-Fédou92, Delest-Duchon99, Mishna2003] and examples in help pages).

# TOOLS FOR PROOFS

## 2. Resultants

# Definition

The Sylvester matrix of $A = a_m x^m + \cdots + a_0 \in \mathbb{K}[x]$, $(a_m \neq 0)$, and of $B = b_n x^n + \cdots + b_0 \in \mathbb{K}[x]$, $(b_n \neq 0)$, is the square matrix of size $m+n$

$$\mathsf{Syl}(A,B) = \begin{bmatrix} a_m & a_{m-1} & \dots & a_0 & & & & \\ & a_m & a_{m-1} & \dots & a_0 & & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & a_m & a_{m-1} & \dots & a_0 & \\ b_n & b_{n-1} & \dots & b_0 & & & & \\ & b_n & b_{n-1} & \dots & b_0 & & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & b_n & b_{n-1} & \dots & b_0 & \end{bmatrix}$$

The resultant $\mathsf{Res}(A,B)$ of $A$ and $B$ is the determinant of $\mathsf{Syl}(A,B)$.

- Definition extends to polynomials with coefficients in a commutative ring $\mathsf{R}$.

# Basic observation

If $\quad A = a_m x^m + \cdots + a_0 \quad$ and $\quad B = b_n x^n + \cdots + b_0, \quad$ then

$$\begin{bmatrix} a_m & a_{m-1} & \dots & a_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & a_m & a_{m-1} & \dots & a_0 \\ b_n & b_{n-1} & \dots & b_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & b_n & b_{n-1} & \dots & b_0 \end{bmatrix} \times \begin{bmatrix} \alpha^{m+n-1} \\ \vdots \\ \alpha \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha^{n-1} A(\alpha) \\ \vdots \\ A(\alpha) \\ \alpha^{m-1} B(\alpha) \\ \vdots \\ B(\alpha) \end{bmatrix}$$

Corollary: If $A(\alpha) = B(\alpha) = 0$, then $\mathsf{Res}\,(A, B) = 0$.

# Example: the discriminant

The discriminant of $A$ is the resultant of $A$ and of its derivative $A'$.

E.g. for $A = ax^2 + bx + c$,

$$\mathsf{Disc}(A) = \mathsf{Res}\,(A, A') = \det \begin{bmatrix} a & b & c \\ 2a & b & \\ & 2a & b \end{bmatrix} = -a(b^2 - 4ac).$$

E.g. for $A = ax^3 + bx + c$,

$$\mathsf{Disc}(A) = \mathsf{Res}\,(A, A') = \det \begin{bmatrix} a & 0 & b & c & \\ & a & 0 & b & c \\ 3a & 0 & b & & \\ & 3a & 0 & b & \\ & & 3a & 0 & b \end{bmatrix} = a^2(4b^3 + 27ac^2).$$

▶ The discriminant vanishes when $A$ and $A'$ have a common root, that is when $A$ has a multiple root.

# Main properties

- Link with gcd $\quad \mathsf{Res}\,(A,B)=0$ if and only if $\gcd(A,B)$ is non-constant.

- Elimination property

  There exist $U,V\in\mathbb{K}[x]$ not both zero, with $\deg(U)<n$, $\deg(V)<m$ and such that the following Bézout identity holds:

$$\mathsf{Res}\,(A,B)=UA+VB \quad \text{in} \;\; \mathbb{K}\cap(A,B).$$

- Poisson formula

  If $A=a(x-\alpha_1)\cdots(x-\alpha_m)$ and $B=b(x-\beta_1)\cdots(x-\beta_n)$, then

$$\mathsf{Res}\,(A,B) \; = \; a^n b^m \prod_{i,j}(\alpha_i-\beta_j) \; = \; a^n \prod_{1\le i\le m} B(\alpha_i).$$

- Bézout-Hadamard bound

  If $A,B\in\mathbb{K}[x,y]$, then $\mathsf{Res}_y(A,B)$ is a polynomial in $\mathbb{K}[x]$ of degree

$$\le \deg_x(A)\deg_y(B)+\deg_x(B)\deg_y(A).$$

# Application: computation with algebraic numbers

Let $A = \prod_i (x - \alpha_i)$ and $B = \prod_j (x - \beta_j)$ be polynomials of $\mathbb{K}[x]$. Then

$$\mathsf{Res}_x(A(x), B(t-x)) = \prod_{i,j} (t - (\alpha_i + \beta_j)),$$

$$\mathsf{Res}_x(A(x), B(t+x)) = \prod_{i,j} (t - (\beta_j - \alpha_i)),$$

$$\mathsf{Res}_x(A(x), x^{\deg B} B(t/x)) = \prod_{i,j} (t - \alpha_i \beta_j),$$

$$\mathsf{Res}_x(A(x), t - B(x)) = \prod_i (t - B(\alpha_i)).$$

In particular, the set of algebraic numbers is a field.

Proof: Poisson's formula. E.g., first one: $\prod_i B(t - \alpha_i) = \prod_{i,j} (t - \alpha_i - \beta_j)$.

- The same formulas apply mutatis mutandis to algebraic power series.

# Two beautiful identities of Ramanujan's

$$\frac{\sin\frac{2\pi}{7}}{\sin^2\frac{3\pi}{7}} - \frac{\sin\frac{\pi}{7}}{\sin^2\frac{2\pi}{7}} + \frac{\sin\frac{3\pi}{7}}{\sin^2\frac{\pi}{7}} = 2\sqrt{7}.$$

- Using $\sin(k\pi/7) = \frac{1}{2i}(x^k - x^{-k})$, where $x = \exp(i\pi/7)$, left-hand sum is a rational function $N(x)/D(x)$, so it is a root of $\mathrm{Res}_X(X^7+1,\, t\cdot D(X) - N(X))$

```
> f:=sin(2*a)/sin(3*a)^2-sin(a)/sin(2*a)^2+sin(3*a)/sin(a)^2:
> expand(convert(f,exp)):
> F:=normal(subs(exp(I*a)=x,%)):
> factor(resultant(x^7+1,numer(t-F),x)):
```

$$-1274\, I\, (t^2 - 28)^3$$

- A slightly more complicated one:

$$\sqrt[3]{\cos\frac{2\pi}{7}} + \sqrt[3]{\cos\frac{4\pi}{7}} + \sqrt[3]{\cos\frac{8\pi}{7}} = \sqrt[3]{\frac{5-3\sqrt[3]{7}}{2}}.$$

# Rothstein-Trager resultant

Let $A, B \in \mathbb{K}[x]$ with $\deg(A) < \deg(B)$ and squarefree monic denominator $B$. The rational function $F = A/B$ has simple poles only.

If $F = \sum_i \frac{\gamma_i}{x - \beta_i}$, then the residue $\gamma_i$ of $F$ at the pole $\beta_i$ equals $\gamma_i = \frac{A(\beta_i)}{B'(\beta_i)}$.

Theorem. The residues $\gamma_i$ of $F$ are roots of the Rothstein-Trager resultant

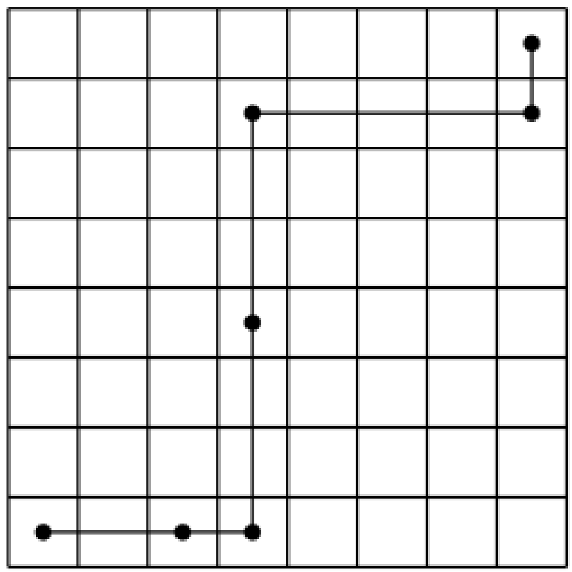
$$R(t) = \mathsf{Res}_x\big(B(x),\ A(x) - t \cdot B'(x)\big).$$

Proof. Poisson formula again: $R(t) = \prod_i \Big(A(\beta_i) - t \cdot B'(\beta_i)\Big)$.

- This special resultant is useful for symbolic integration of rational functions.

# Application: diagonal Rook paths

Question: A chess Rook can move any number of squares horizontally or vertically in one step. How many paths can a Rook take from the lower-left corner square to the upper-right corner square of an $N \times N$ chessboard? Assume that the Rook moves right or up at each step.



$$1,\ 2,\ 14,\ 106,\ 838,\ 6802,\ 56190,\ 470010,\ \ldots$$

# Application: diagonal Rook paths

$$1,\ 2,\ 14,\ 106,\ 838,\ 6802,\ 56190,\ 470010,\ \ldots$$

$$\mathsf{Diag}(F) = [s^0]\, F(s, x/s) = \frac{1}{2i\pi} \oint F(s, x/s)\, \frac{ds}{s}, \quad \text{where} \quad F = \frac{1}{1 - \frac{s}{1-s} - \frac{t}{1-t}}.$$

By the residue theorem, $\mathsf{Diag}(F)$ is a sum of roots of the Rothstein-Trager resultant

```
> F:=1/(1-s/(1-s)-t/(1-t)):
> G:=normal(1/s*subs(t=x/s,F)):
> factor(resultant(denom(G),numer(G)-t*diff(denom(G),s),s));
```

```
       2                                 2              2
      x  (-1 + 2 t) (x - 1) (-x + 36 t  x + 1 - 4 t )
```

Answer: Generating series of diagonal Rook paths is $\frac{1}{2}\left(1+\sqrt{\frac{1-x}{1-9x}}\right)$.

# Application: certified algebraic guessing

Guess + Bound = Proof

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x, y]$ of degree at most $d$ in $x$ and at most $n$ in $y$.

If $\displaystyle\sum_{i=0}^{n} Q_i(x) A^i(x) = O(x^{2dn+1})$ and $\deg Q_i \leq d$, then $\displaystyle\sum_{i=0}^{n} Q_i(x) A^i(x) = 0$.

# Application: certified algebraic guessing

Guess + Bound = Proof

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most $d$ in $x$ and at most $n$ in $y$.

If $\displaystyle\sum_{i=0}^{n} Q_i(x)A^i(x) = O(x^{2dn+1})$ and $\deg Q_i \le d$, then $\displaystyle\sum_{i=0}^{n} Q_i(x)A^i(x) = 0$.

Proof: Let $P \in \mathbb{K}[x,y]$ be an irreducible polynomial such that

$$P(x, A(x)) = 0, \text{ and } \deg_x(P) \le d, \ \deg_y(P) \le n.$$

# Application: certified algebraic guessing

Guess + Bound = Proof

Theorem. Suppose $A \in \mathbb{K}[[x]]$ is an algebraic series, and that it is a root of a (unknown) polynomial in $\mathbb{K}[x,y]$ of degree at most $d$ in $x$ and at most $n$ in $y$.

If $\displaystyle\sum_{i=0}^{n} Q_i(x)A^i(x) = O(x^{2dn+1})$ and $\deg Q_i \leq d$, then $\displaystyle\sum_{i=0}^{n} Q_i(x)A^i(x) = 0$.

Proof: Let $P \in \mathbb{K}[x,y]$ be an irreducible polynomial such that

$$P(x, A(x)) = 0, \text{ and } \deg_x(P) \leq d, \ \deg_y(P) \leq n.$$

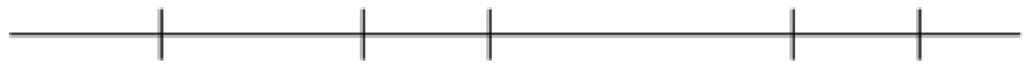
- By Hadamard, $R(x) = \mathrm{Res}_y(P,Q) \in \mathbb{K}[x]$ has degree at most $2dn$.
- By elimination, $R(x) = UP + VQ$ for $U, V \in \mathbb{K}[x,y]$ with $\deg_y(V) < n$.
- Evaluation at $y = A(x)$ yields

$$R(x) = U(x, A(x))\underbrace{P(x, A(x))}_{0} + V(x, A(x))\underbrace{Q(x, A(x))}_{O(x^{2dn+1})} = O(x^{2dn+1}).$$

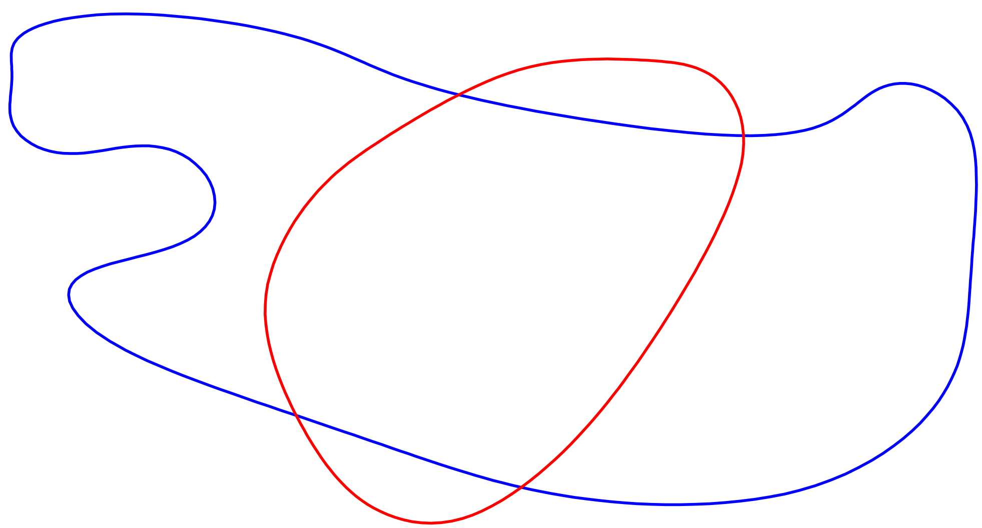
- Thus $R = 0$, that is $\gcd(P,Q) \neq 1$, and thus $P \mid Q$, and $A$ is a root of $Q$.

# Systems of two equations and two unknowns

Geometrically, roots of a polynomial $f \in \mathbb{Q}[x]$ correspond to points on a line.



Roots of polynomials $A \in \mathbb{Q}[x, y]$ correspond to plane curves $A = 0$.

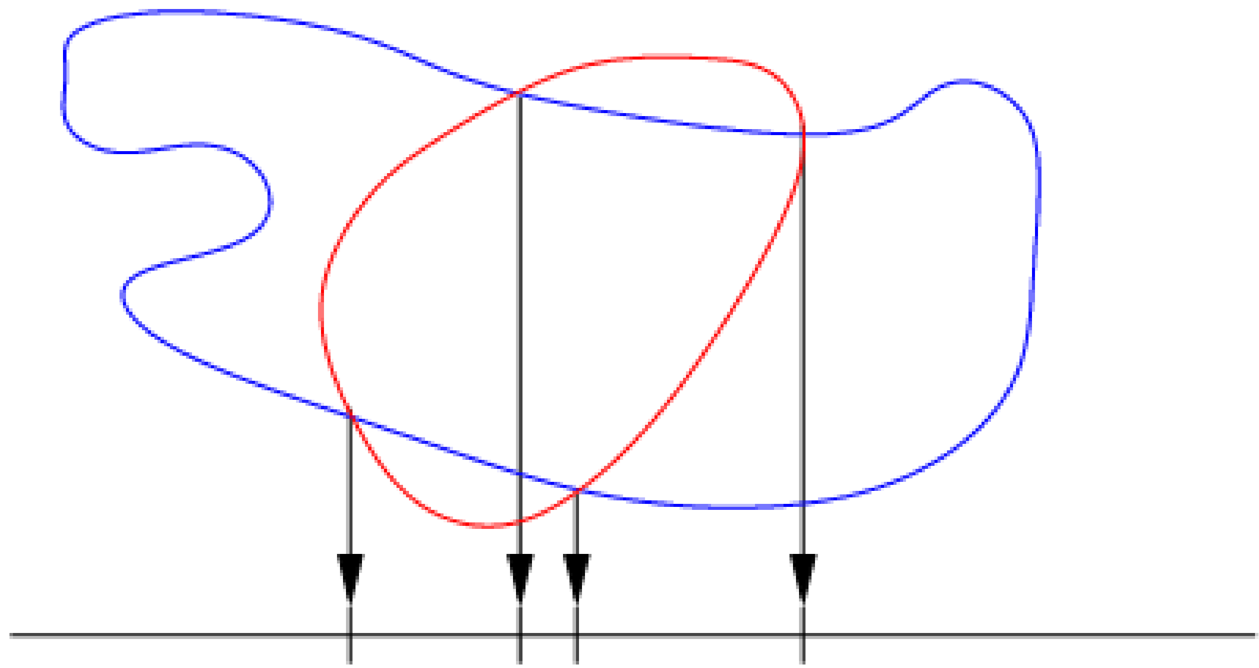


Let now $A$ and $B$ be in $\mathbb{Q}[x, y]$. Then:

- either the curves $A = 0$ and $B = 0$ have a common component,
- or they intersect in a finite number of points.

# Application: Resultants compute projections

Theorem. Let $A = a_m y^m + \cdots$ and $B = b_n y^n + \cdots$ be polynomials in $\mathbb{Q}[x][y]$. The roots of $\mathsf{Res}_y(A,B) \in \mathbb{Q}[x]$ are either the abscissas of points in the intersection $A = B = 0$, or common roots of $a_m$ and $b_n$.



Proof. Elimination property: $\mathsf{Res}\,(A,B) = UA + VB$, for $U, V \in \mathbb{Q}[x,y]$.

Thus $A(\alpha,\beta) = B(\alpha,\beta) = 0$ implies $\mathsf{Res}_y(A,B)(\alpha) = 0$

# Application: implicitization of parametric curves

Task: Given a rational parametrization of a curve

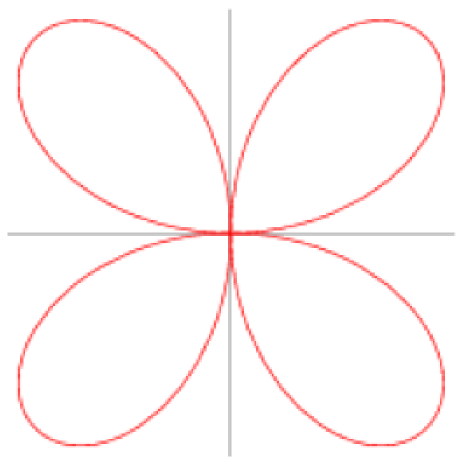
$$x = A(t), \quad y = B(t), \qquad A, B \in \mathbb{K}(t),$$

compute a non-trivial polynomial in $x$ and $y$ vanishing on the curve.

Recipe: take the resultant in $t$ of numerators of $x - A(t)$ and $y - B(t)$.

Example: for the four-leaved clover (a.k.a. quadrifolium) given by

$$x = \frac{4t(1-t^2)^2}{(1+t^2)^3}, \quad y = \frac{8t^2(1-t^2)}{(1+t^2)^3},$$



$$\mathrm{Res}_t((1+t^2)^3x - 4t(1-t^2)^2, (1+t^2)^3y - 8t^2(1-t^2)) = 2^{24}\left((x^2+y^2)^3 - 4x^2y^2\right).$$

# TOOLS FOR PROOFS

## 3. D-Finiteness

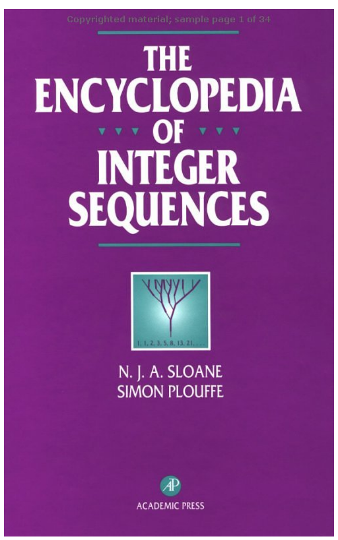
# D-finite Series & Sequences

**Definition**: A power series $f(x) \in \mathbb{K}[[x]]$ is **D-finite** over $\mathbb{K}$ when its derivatives generate a finite-dimensional vector space over $\mathbb{K}(x)$.

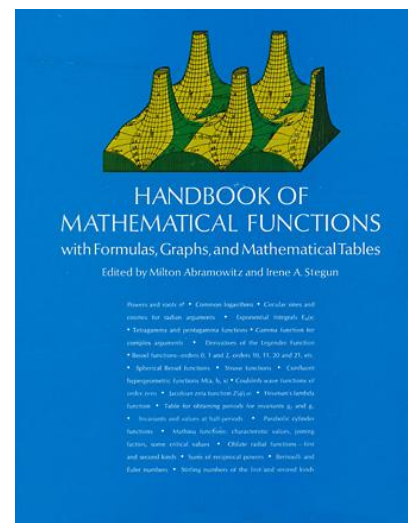
A sequence $u_n$ is **D-finite** (or **P-recursive**) over $\mathbb{K}$ when its shifts $(u_n, u_{n+1}, \dots)$ generate a finite-dimensional vector space over $\mathbb{K}(n)$.

$$\boxed{\text{equation} + \text{init conditions} = \text{data structure}}$$

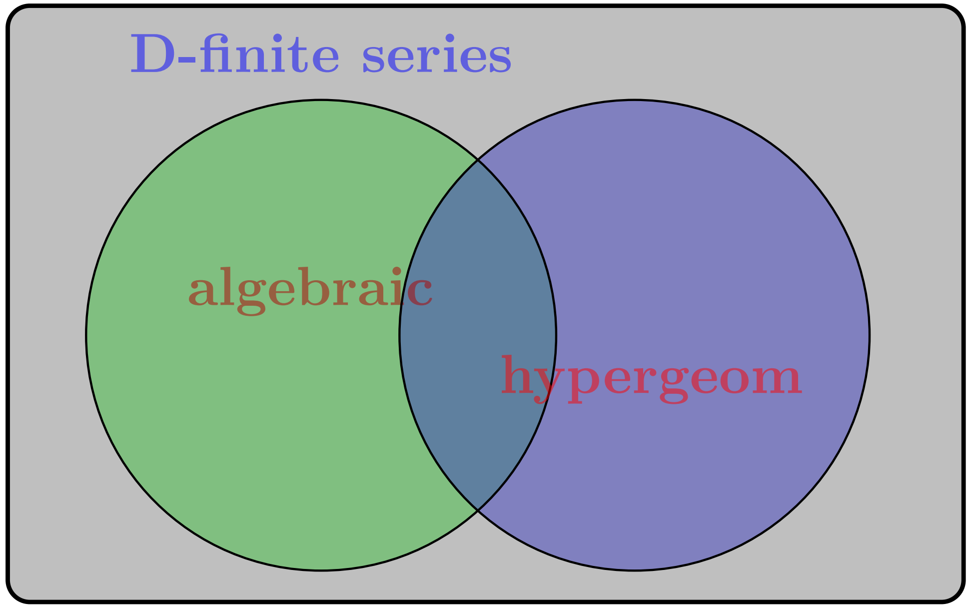
About 25% of Sloane's encyclopedia, 60% of Abramowitz & Stegun




Examples: exp, log, sin, cos, sinh, cosh, arccos, arccosh, arcsin, arcsinh, arctan, arctanh, arccot, arccoth, arccsc, arccsch, arcsec, arcsech, ${}_pF_q$ (includes Bessel $J$, $Y$, $I$ and $K$, Airy Ai and Bi and polylogarithms), Struve, Weber and Anger functions, the large class of algebraic functions,...



# Important classes of power series




Algebraic: $S(x) \in \mathbb{K}[[x]]$ root of a polynomial $P \in \mathbb{K}[x, y]$.

D-finite: $S(x) \in \mathbb{K}[[x]]$ satisfying a linear differential equation with polynomial (or rational function) coefficients $c_r(x)S^{(r)}(x) + \cdots + c_0(x)S(x) = 0$.

Hypergeometric: $S(x) = \sum_n s_n x^n$ such that $\frac{s_{n+1}}{s_n} \in \mathbb{K}(n)$. E.g.

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

# Link D-finite $\leftrightarrow$ P-recursive

Theorem: A power series $f \in \mathbb{K}[[x]]$ is D-finite if and only if the sequence $f_n$ of its coefficients is P-recursive

Proof (idea): $x\partial \leftrightarrow n$ and $x^{-1} \leftrightarrow S_n$ give a ring isomorphism between

$$\mathbb{K}[x, x^{-1}, \partial] \quad \text{and} \quad \mathbb{K}[S_n, S_n^{-1}, n].$$

Snobbish way of saying that the equality $f = \sum_{n \geq 0} f_n x^n$ implies

$$[x^n]\, x f'(x) = n f_n, \quad \text{and} \quad [x^n]\, x^{-1} f(x) = f_{n+1}.$$

▶ Both conversions implemented in gfun: diffeqtorec and rectodiffeq

▶ Differential operators of order $r$ and degree $d$ give rise to recurrences of order $d + r$ and coefficients of degree $r$

# Closure properties

Th. D-finite series in $\mathbb{K}[[x]]$ form a $\mathbb{K}$-algebra closed under Hadamard product. P-recursive sequences over $\mathbb{K}$ form an algebra closed under Cauchy product.

Proof: Linear algebra:

If $a_r(x)f^{(r)}(x)+\cdots+a_0(x)f(x)=0, \quad b_s(x)g^{(s)}(x)+\cdots+b_0(x)g(x)=0$, then

$$f^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f,\, f',\dots,f^{(r-1)}\right), \quad g^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(g,\, g',\dots,g^{(s-1)}\right),$$

$$\text{so that} \quad (f+g)^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f,\, f',\dots,f^{(r-1)},\, g,\, g',\dots,g^{(s-1)}\right),$$

$$\text{and} \quad (fg)^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(f^{(i)}g^{(j)}, \quad i<r,\, j<s\right).$$

Thus $f+g$ satisfies LDE of order $\leq (r+s)$ and $fg$ satisfies LDE of order $\leq (rs)$.

Corollary: D-finite series can be multiplied mod $x^N$ in linear time $O(N)$.

▶ Implemented in gfun: diffeq+diffeq, diffeq*diffeq, hadamardproduct, rec+rec, rec*rec, cauchyproduct

# Proof of Identities

```
> series(sin(x)^2+cos(x)^2,x,4);
```

```
                          4
                 1 + O( x )
```

Why is this a proof?

(1) sin and cos satisfy a 2nd order LDE: $y'' + y = 0$;

(2) their squares (and their sum) satisfy a 3rd order LDE;

(3) the constant 1 satisfies a 1st order LDE: $y' = 0$;

(4) $\Longrightarrow \sin^2 + \cos^2 - 1$ satisfies a LDE of order at most 4;

(5) Since it is not singular at 0, Cauchy's theorem concludes.

- Cassini's identity (same idea): $F_n^2 - F_{n+1}F_{n-1} = (-1)^{n+1}$

```
> for n to 5 do
>    fibonacci(n)^2-fibonacci(n+1)*fibonacci(n-1)+(-1)^n
> od;
```

# Algebraic series are D-finite

Theorem [Abel 1827, Cockle 1860, Harley 1862] Any algebraic series is D-finite.

Proof: Let $f(x) \in \mathbb{K}[[x]]$ such that $P(x, f(x)) = 0$, with $P \in \mathbb{K}[x, y]$ irreducible.

Differentiate w.r.t. $x$:

$$P_x(x, f(x)) + f'(x) P_y(x, f(x)) = 0 \qquad \Longrightarrow \qquad f' = -\frac{P_x}{P_y}(x, f).$$

Bézout relation: $\quad \gcd(P, P_y) = 1 \quad \Longrightarrow \quad UP + VP_y = 1, \quad$ for $U, V \in \mathbb{K}(x)[y]$

$$\Longrightarrow \quad f' = -\Big(P_x V \bmod P\Big)(x, f) \ \in \ \mathsf{Vect}_{\mathbb{K}(x)}\left(1, f, f^2, \ldots, f^{\deg_y(P)-1}\right).$$

By induction, $f^{(\ell)} \in \mathsf{Vect}_{\mathbb{K}(x)}\left(1, f, f^2, \ldots, f^{\deg_y(P)-1}\right)$, for all $\ell$. $\square$

- Implemented in gfun: algeqtodiffeq
- Generalization: $g$ D-finite, $f$ algebraic $\rightarrow g \circ f$ D-finite algebraicsubs

# An Olympiad Problem

Question: Let $(a_n)$ be the sequence with $a_0 = a_1 = 1$ satisfying the recurrence

$$(n+3)a_{n+1} = (2n+3)a_n + 3na_{n-1}.$$

Show that all $a_n$ is an integer for all $n$.

Computer-aided solution: Let's compute the first 10 terms of the sequence:

```
> rec:=(n+3)*a(n+1)-(2*n+3)*a(n)-3*n*a(n-1): ini:=a(0)=1,a(1)=1:
> pro:=gfun:-rectoproc({rec,ini}, a(n), list);
> pro(10);
```

```
[1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188]
```

gfun's seriestoalgeq command allows to guess that GF is algebraic:

```
> pol:=gfun:-listtoalgeq(%,y(x))[1];
```

```
                              2    2
1 + (x - 1) y(x) + x  y(x)
```

Thus it is very likely that $y = \sum_{n \geq 0} a_n x^n$ verifies $1 + (x-1)y + x^2 y^2 = 0$.

By coefficient extraction, $(a_n)$ conjecturally verifies the non-linear recurrence

$$a_{n+2} = a_{n+1} + \sum_{k=0}^{n} a_k \cdot a_{n-k}. \tag{1}$$

Clearly (1) implies $a_n \in \mathbb{N}$. To prove (1), we proceed the other way around: we start with $P(x,y) = 1 + (x-1)y + x^2y^2$, and show that it admits a power series solution whose coefficients satisfy the same linear recurrence as $(a_n)$:

```
> deq:=gfun:-algeqtodiffeq(pol,y(x)):
> recb:=gfun:-diffeqtorec(deq,y(x),b(n));
```

```
recb := {(3 + 3 n) b(n) + (2 n + 5) b(n + 1) + (-4 - n) b(n + 2),
                                            b(0) = 1, b(1) = 1}
```

► In fact, $a_n$ is equal to

$$a_n = \sum_{k=0}^{n} \binom{n}{2k}\binom{2k}{k} - \sum_{k=0}^{n} \binom{n}{2k}\binom{2k}{k+1},$$

(which clearly implies $a_n \in \mathbb{Z}$), but how to find algorithmically such a formula?

# Gessel's walks are algebraic

Let's prove that the series counting Gessel walks of prescribed length

$$G(1,1,x) = \frac{1}{2x} \cdot {}_2F_1\left(\begin{matrix} -1/12 & 1/4 \\ & 2/3 \end{matrix} \,\middle|\, -\frac{64x(4x+1)^2}{(4x-1)^4}\right) - \frac{1}{2x}.$$

is algebraic.

Proof principle: Guess a polynomial $P(x,y)$ in $\mathbb{Q}[x,y]$, then prove that $P$ admits the power series $G(1,1,x) = \sum_{n=0}^{\infty} g_n x^n$ as a root.

1. Such a $P$ can be guessed from the first 100 terms of $G(1,1,x)$.

```
> G:=(hypergeom([-1/12,1/4],[2/3],-64*x*(4*x+1)^2/(4*x-1)^4)-1)/x/2:
> seriestoalgeq(series(G,x,100),y(x)):
> P:=subs(y(x)=y,%[1]):
```

2. Implicit function theorem: $\exists!$ root $r(x) \in \mathbb{Q}[[x]]$ of $P$.

```
> map(eval,[P,diff(P,y)], {x=0,y=1});
                              [0, 1]
```

3. D-finiteness: $r(x)=\sum_{n=0}^{\infty} r_n x^n$ being algebraic, it is D-finite, and so is $(r_n)$:

```
> deqP:=algeqtodiffeq(P,y(x)): recP:=diffeqtorec(deqP,y(x),r(n));
                                          2                            2
recP:= {(256 + 448 n + 192 n ) r(n) - (240 + 208 n + 48 n ) r(n+1) -
                 2                      2
(100+68n+12n ) r(n+2) + (44+23n+3n ) r(n+3), r(0)=1, r(1)=2, r(2)=7}
```

4. D-finiteness: $G(1,1,x)$ being the composition of a D-finite by an algebraic, it is D-finite, and so is $(g_n)$:

```
> deqG:=holexprtodiffeq(G,y(x)): recG:=diffeqtorec(deqG,y(x),g(n));
                                          2                            2
recG:= {(256 + 448 n + 192 n ) g(n) - (240 + 208 n + 48 n ) g(n+1) -
                 2                      2
(100+68n+12n ) g(n+2) + (44+23n+3n ) g(n+3), g(0)=1, g(1)=2, g(2)=7}
```

5. Conclusion: $(r_n)$ and $(g_n)$ are equal, since they satisfy the same recurrence and the same initial values. Thus $G(1,1,x)$ coincides with the algebraic series $r(x)$, so it is algebraic. $\square$

# TOOLS FOR PROOFS

## 4. Creative Telescoping

# Examples I: hypergeometric summation

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

- $A_n=\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}^2$ satisfies the recurrence [Apéry78]:

$$(n+1)^3A_{n+1}=(34n^3+51n^2+27n+5)A_n-n^3A_{n-1}.$$

(*Neither Cohen nor I had been able to prove this in the intervening two months* [Van der Poorten]).

- $$\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}^2=\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}\sum_{j=0}^{k}\binom{n}{k}^3 \qquad \text{[Strehl92]}$$

# Examples II: Integrals

- $$\int_0^1 \frac{\cos(zu)}{\sqrt{1-u^2}}\,du = \int_1^{+\infty} \frac{\sin(zu)}{\sqrt{u^2-1}}\,du = \frac{\pi}{2} J_0(z);$$
- $$\int_0^{+\infty} x J_1(ax) I_1(ax) Y_0(x) K_0(x)\,dx = -\frac{\ln(1-a^4)}{2\pi a^2} \quad \text{[Glasser-Montaldi94];}$$
- $$\frac{1}{2\pi i} \oint \frac{(1+2xy+4y^2)\exp\left(\frac{4x^2y^2}{1+4y^2}\right)}{y^{n+1}(1+4y^2)^{\frac{3}{2}}}\,dy = \frac{H_n(x)}{\lfloor n/2 \rfloor !} \quad \text{[Doetsch30].}$$

# Examples III: Diagonals

Definition If $f(x_1,\ldots,x_k) = \displaystyle\sum_{i_1,i_2,\ldots,i_k\geq 0} c_{i_1,\ldots,i_k} x_1^{i_1}\cdots x_k^{i_k} \in \mathbb{K}[[x_1,\ldots,x_k]]$, then its diagonal is $\mathrm{Diag}(f) = \displaystyle\sum_{n\geq 0} c_{n,\ldots,n} x^n \in \mathbb{K}[[x]]$.

# Examples III: Diagonals

Definition If $f(x_1,\ldots,x_k) = \sum_{i_1,i_2,\ldots,i_k\geq 0} c_{i_1,\ldots,i_k} x_1^{i_1}\cdots x_k^{i_k} \in \mathbb{K}[[x_1,\ldots,x_k]]$, then its diagonal is $\operatorname{Diag}(f) = \sum_{n\geq 0} c_{n,\ldots,n} x^n \in \mathbb{K}[[x]]$.

- Diagonal $k$-D rook paths: $\operatorname{Diag} \dfrac{1}{1-\frac{x_1}{1-x_1}-\cdots-\frac{x_k}{1-x_k}}$;
- Hadamard product: $F(x)\odot G(x) = \sum_n f_n g_n x^n = \operatorname{Diag}(F(x)G(y))$;
- Algebraic series [Furstenberg67]: if $P(x,S(x))=0$ and $P_y(0,0)\neq 0$ then

$$S(x) = \operatorname{Diag}\left(y^2\frac{P_y(xy,y)}{P(xy,y)}\right).$$

- Apéry's sequence [Dwork80]:

$$\sum_{n\geq 0} A_n z^n = \operatorname{Diag}\frac{1}{(1-x_1)((1-x_2)(1-x_3)(1-x_4)(1-x_5)-x_1x_2x_3)}.$$

# Examples III: Diagonals

Definition If $f(x_1,\dots,x_k)=\sum_{i_1,i_2,\dots,i_k\geq 0} c_{i_1,\dots,i_k} x_1^{i_1}\cdots x_k^{i_k}\in\mathbb{K}[[x_1,\dots,x_k]]$, then its diagonal is $\operatorname{Diag}(f)=\sum_{n\geq 0} c_{n,\dots,n}x^n\in\mathbb{K}[[x]]$.

- Diagonal $k$-D rook paths: $\operatorname{Diag}\dfrac{1}{1-\frac{x_1}{1-x_1}-\cdots-\frac{x_k}{1-x_k}}$;
- Hadamard product: $F(x)\odot G(x)=\sum_n f_n g_n x^n=\operatorname{Diag}(F(x)G(y))$;
- Algebraic series [Furstenberg67]: if $P(x,S(x))=0$ and $P_y(0,0)\neq 0$ then

$$S(x)=\operatorname{Diag}\left(y^2\frac{P_y(xy,y)}{P(xy,y)}\right).$$

- Apéry's sequence [Dwork80]:

$$\sum A_n z^n=\operatorname{Diag}\frac{1}{(1-x_1)((1-x_2)(1-x_3)(1-x_4)(1-x_5)-x_1x_2x_3)}.$$

Theorem [Lipshitz88] The diagonal of a rational (or algebraic, or even D-finite) series is D-finite.

# Summation by Creative Telescoping

$$I_n := \sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

**IF** one knows Pascal's triangle:

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} = 2\binom{n}{k} + \binom{n}{k-1} - \binom{n}{k},$$

then summing over $k$ gives

$$I_{n+1} = 2I_n.$$

The initial condition $I_0 = 1$ concludes the proof.

# Creative Telescoping for Sums

$$F_n = \sum_k u_{n,k} =?$$

**IF** one knows $A(n, S_n)$ and $B(n, k, S_n, S_k)$ s.t.

$$(A(n, S_n) + \Delta_k B(n, k, S_n, S_k)) \cdot u_{n,k} = 0$$

(where $\Delta_k$ is the difference operator, $\Delta_k \cdot v_{n,k} = v_{n,k+1} - v_{n,k}$), then the sum "telescopes", leading to

$$A(n, S_n) \cdot F_n = 0.$$

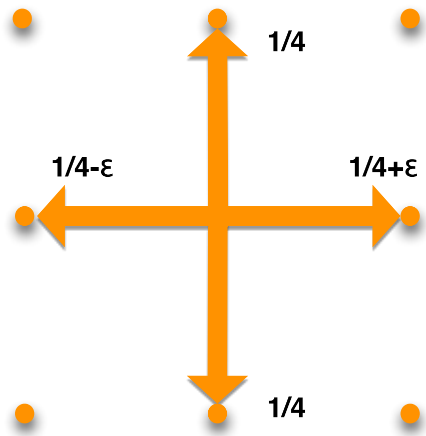
# Zeilberger's Algorithm [1990]

Input: a hypergeometric term $u_{n,k}$, i.e., $u_{n+1,k}/u_{n,k}$ and $u_{n,k+1}/u_{n,k}$ rational functions in $n$ and $k$;

Output:

- a linear recurrence ($A$) satisfied by $F_n = \sum_k u_{n,k}$
- a certificate ($B$), s.t. checking the result is easy from $A(n, S_n) \cdot u_{n,k} = \Delta_k B \cdot u_{n,k}$.

# Example: SIAM flea




$$U_{n,k} := \binom{2n}{2k}\binom{2k}{k}\binom{2n-2k}{n-k}\left(\frac{1}{4}+c\right)^k\left(\frac{1}{4}-c\right)^k\frac{1}{4^{2n-2k}}.$$

```
> SumTools[Hypergeometric][Zeilberger](U,n,k,Sn);
```

$$[(4\,n^2+16\,n+16)\,Sn^2+(-4\,n^2+32\,c^2n^2+96\,c^2n-12\,n+72\,c^2-9)\,Sn$$
$$+128\,c^4n+64\,c^4n^2+48\,c^4, \ldots\text{(BIG certificate)}\ldots]$$

# Creative Telescoping for Integrals

$$I(x) = \int_{\Omega} u(x,y)\,dy = ?$$

**IF** one knows $A(x,\partial_x)$ and $B(x,y,\partial_x,\partial_y)$ s.t.

$$(A(x,\partial_x) + \partial_y B(x,y,\partial_x,\partial_y)) \cdot u(x,y) = 0,$$

then the integral "telescopes", leading to

$$A(x,\partial_x) \cdot I(x) = 0.$$

# Special Case: Diagonals

Analytically,

$$\operatorname{Diag}(F(x,y)) = \frac{1}{2\pi i}\oint F\left(\frac{x}{y}, y\right)\frac{dy}{y}.$$

On power series,

$$(A(x,\partial_x) + \partial_y B)\cdot \underbrace{\frac{1}{y}F\left(\frac{x}{y}, y\right)}_{U} = 0 \Longrightarrow A(x,\partial_x)\cdot \operatorname{Diag} F = 0.$$

# Special Case: Diagonals

Analytically,

$$\mathrm{Diag}(F(x,y)) = \frac{1}{2\pi i} \oint F\left(\frac{x}{y}, y\right) \frac{dy}{y}.$$

On power series,

$$(A(x,\partial_x) + \partial_y B) \cdot \underbrace{\frac{1}{y} F\left(\frac{x}{y}, y\right)}_{U} = 0 \Longrightarrow A(x,\partial_x) \cdot \mathrm{Diag}\, F = 0.$$

Proof:

1. $[y^{-1}]U = \mathrm{Diag}(f)$;
2. $0 = [y^{-1}]A \cdot U + [y^{-1}]\partial_y B \cdot U = A \cdot [y^{-1}]U.$

# Special Case: Diagonals

Analytically,

$$\mathrm{Diag}(F(x,y)) = \frac{1}{2\pi i}\oint F\left(\frac{x}{y}, y\right)\frac{dy}{y}.$$

On power series,

$$(A(x,\partial_x) + \partial_y B)\cdot \underbrace{\frac{1}{y}F\left(\frac{x}{y}, y\right)}_{U} = 0 \Longrightarrow A(x,\partial_x)\cdot \mathrm{Diag}\,F = 0.$$

Proof:

1. $[y^{-1}]U = \mathrm{Diag}(f)$;
2. $[y^{-1}]A\cdot U + [y^{-1}]\partial_y B\cdot U = A\cdot[y^{-1}]U$.

Extends to more variables: $\mathrm{Diag}\,F(x,y,z)$ obtained from $[y^{-1}z^{-1}]U$, $U = \frac{1}{yz}F\left(\frac{x}{y}, \frac{y}{z}, z\right)$, **if** one finds

$$(A(x,\partial_x) + \partial_y B(x,y,z,\partial_x,\partial_y,\partial_z) + \partial_z C(x,y,z,\partial_x,\partial_y,\partial_z))\cdot U = 0.$$

Provided by Chyzak's algorithm

# Example: 3D rook paths [B-Chyzak-Hoeij-Pech 2011]

Proof of a recurrence conjectured by [Erickson *et alii* 2010]

```
> F:=subs(y=y/z,x=x/y,1/(1-x/(1-x)-y/(1-y)-z/(1-z)))/y/z:
> A,B,C:=op(op(Mgfun:-creative_telescoping(F,x::diff,[y::diff,z::diff]))):
> A;
```

$$\left(2304\,x^3 - 3204\,x^2 - 432\,x + 296\right) \frac{d}{dx}\_F\left(x\right) + \left(4608\,x^4 - 6372\,x^3 + 813\,x^2 + 514\,x - 4\right) \frac{d^2}{dx^2}\_F\left(x\right) + \left(1152\,x^5 - 1746\,x^4 + 475\,x^3 + 121\,x^2 - 2\,x\right) \frac{d^3}{dx^3}\_F\left(x\right)$$

# More and more general creative telescoping

- Multivariate D-finite series wrt mixed differential, shift, $q$-shift,... [Chyzak-S 1998, Chyzak 2000]
- Symmetric functions [Chyzak-Mishna-S 2005]
- Beyond D-finiteness [Chyzak-Kauers-S 2009]

(Some) implementations available in `Mgfun`

**THE END**

**(Except for the exercises!)**