Efficient experimental mathematics for combinatorics and number theory

Alin Bostan

Inria

Vienna Summer School of Mathematics

Weissensee, Austria

September 23–27, 2019

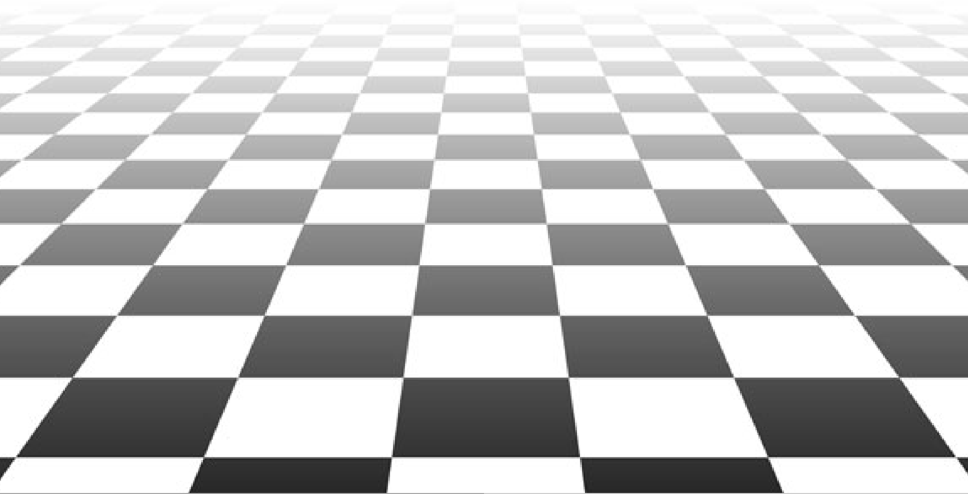
Overview

Lecture 1: Context, Motivation, Examples

Lecture 2: Exp. Math. for Combinatorics

Lecture 3: Inside the Exp. Math. Toolbox

Lecture 3: Inside the Exp. Math. Toolbox



BASIC TOOLS

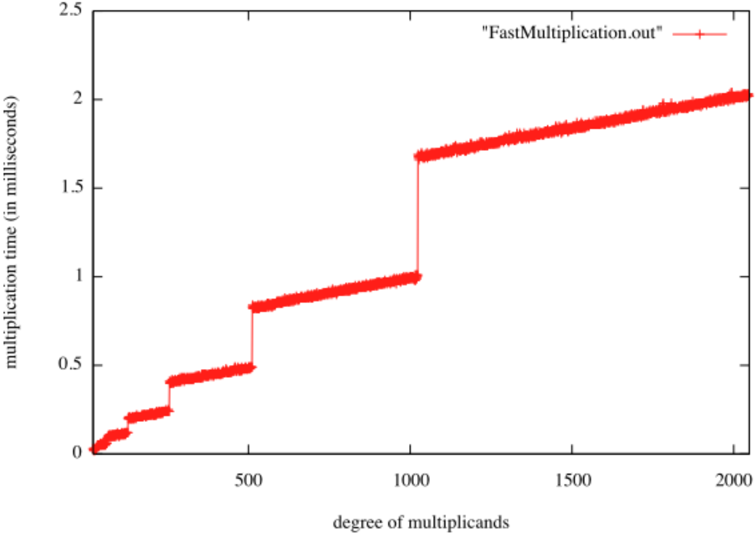
Fast elementary operations

Complexity yardsticks

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

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

Fast polynomial multiplication in practice



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

What can be computed in 1 second (in maple, on a laptop)

1. Integer numbers:
   - product of two integers with 30 000 000 digits
   - factorial of 1 300 000 (output: 7 000 000 digits)
   - factorization of an integer with 42 digits

2. Polynomials in $\mathbb{F}_p[x]$:
   - product of two polynomials of degree 650 000
   - gcd and resultant of two polynomials of degree 12 500
   - factorization of a polynomial of degree 170

3. Polynomials in $\mathbb{F}_p[x, y]$:
   - resultant of two polynomials of total degree 20 (output degree 400)
   - factorization of a polynomial of degree 160

4. Matrices:
   - product of two 850×850 matrices with coefficients in $\mathbb{F}_p$
   - determinant of a $1\,400 \times 1\,400$ matrix with coefficients in $\mathbb{F}_p$
   - characteristic polynomial of a 500×500 matrix with coefficients in $\mathbb{F}_p$
   - determinant of a 200×200 matrix with 32-bits integer entries.

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

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

Inverse DFT

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

- $V_\omega \cdot V_{\omega^{-1}} = n \cdot I_n$ $\rightarrow$ performing the inverse DFT in size n amounts to:
  - performing a DFT at
  $$\frac{1}{1}, \quad \frac{1}{\omega}, \quad \dots, \quad \frac{1}{\omega^{n-1}}$$
  - 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 — $N \leq 4n$
- compute DFT(f, N) and DFT(g, N) — $O(N \log(N))$
- multiply pointwise these values to get DFT(h, N) — $O(N)$
- recover h by inverse DFT — $O(N \log(N))$

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

▷ General case: Create artificial roots of unity $O(n \log(n) \log\log n) = \tilde{O}(n)$

▷ Similarly for integers: N-bit integers can be multiplied in $\tilde{O}(N)$ bit ops.

TOOLS FOR GENERATING DATA

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.

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

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

▷ 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.

```
> 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
```

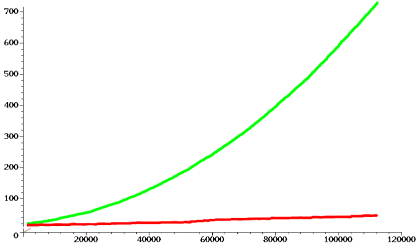
```
> tt:=time(): x:=pro(210000): time()-tt;
> tt:=time(): y:=evalf(exp(1), 1000000): time()-tt, evalf(x-y, 1000000);
```

3.730, 24.037, 0.

Application: record computation of π

[Chudnovsky-Chudnovsky 1987] fast convergence hypergeometric identity

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



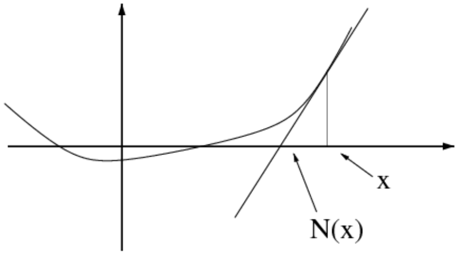
▷ Used in Maple & Mathematica: 1st order recurrence, yields 14 correct digits per iteration ⟶ 4 billion digits [Chudnovsky-Chudnovsky 1994]

▷ Current record: 31.4 trillion digits [Iwao 2019]

TOOLS FOR GENERATING DATA

2. Newton iteration

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



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

$$x_1 = 1.500000000000000000000000000000$$
$$x_2 = 1.416666666666666666666666666667$$
$$x_3 = 1.414215686274509803921568627451$$
$$x_4 = 1.414213562374689910626295578890$$
$$x_5 = 1.414213562373095048801689623503$$

Newton's tangent method: power series case

In order to solve $\varphi(x, g) = 0$ in $\mathbb{K}[[x]]$ 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 $\mathbb{K}[[x]]$ can be computed at precision N using $\tilde{O}(N)$ operations in $\mathbb{K}$

TOOLS FOR CONJECTURES

Hermite-Padé approximants

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.

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 $A \in \mathbb{K}[[x]]$ 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));
```

$$1 - y(x) + xy(x)^2$$

```
> listtodiffeq([1,1,2,5,14,42,132,429],y(x))[1];
```

$$\left\{-2y(x) + (2-4x)\frac{d}{dx}y(x) + x\frac{d^2}{dx^2}y(x), y(0) = 1, D(y)(0) = 1\right\}$$

Existence and naive computation

Theorem For any vector $\mathbf{F} = (f_1, \dots, f_n)^T \in \mathbb{K}[[x]]^n$ and for any n-tuple $\mathbf{d} = (d_1, \dots, d_n) \in \mathbb{N}^n$, 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 (Euclidean-like elimination) $O(\sigma^2)$
- Beckermann-Labahn algorithm (DAC) $\tilde{O}(\sigma) = O(\sigma \log^2 \sigma)$
- structured linear algebra algorithms for Toeplitz-like matrices $\tilde{O}(\sigma)$

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 $\tilde{O}(n^\omega d)$ ops. in $\mathbb{K}$.

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 $\mathbf{P}_1 \in \mathbb{K}[x]^{n\times n}$ s.t. $\mathbf{P}_1 \cdot \mathbf{F} = O(x^{\sigma/2})$, $\deg(\mathbf{P}_1) \approx \frac{d}{2}$
   2. compute "residue" $\mathbf{R}$ such that $\mathbf{P}_1 \cdot \mathbf{F} = x^{\sigma/2} \cdot \big(\mathbf{R} + O(x^{\sigma/2})\big)$
   3. recursively compute $\mathbf{P}_2 \in \mathbb{K}[x]^{n\times n}$ s.t. $\mathbf{P}_2 \cdot \mathbf{R} = O(x^{\sigma/2})$, $\deg(\mathbf{P}_2) \approx \frac{d}{2}$
   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 $\tilde{O}(d)$ ops. in $\mathbb{K}$.

An (innocent looking) combinatorial question

Let $\mathscr{S} = \{\uparrow, \leftarrow, \searrow\}$. An $\mathscr{S}$-walk is a path in $\mathbb{Z}^2$ using only steps from $\mathscr{S}$.
Show that, for any integer n, the following quantities are equal:

(i) number a_n of n-steps $\mathscr{S}$-walks confined to the upper half plane $\mathbb{Z} \times \mathbb{N}$ that start and finish at the origin $(0, 0)$ (*excursions*);

(ii) number b_n of n-steps $\mathscr{S}$-walks confined to the quarter plane $\mathbb{N}^2$ that start at the origin $(0, 0)$ and finish on the diagonal of $\mathbb{N}^2$ (*diagonal walks*).

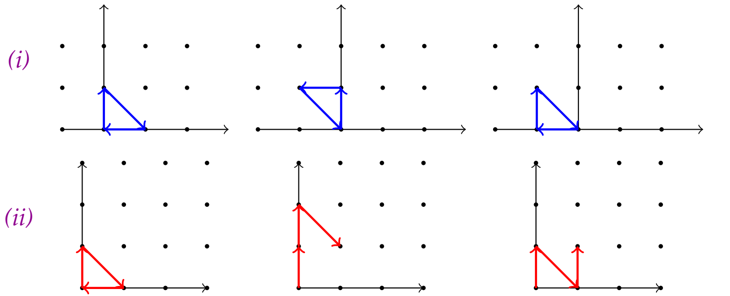
An (innocent looking) combinatorial question

Let $\mathscr{S} = \{\uparrow, \leftarrow, \searrow\}$. An $\mathscr{S}$-walk is a path in $\mathbb{Z}^2$ using only steps from $\mathscr{S}$. Show that, for any integer n, the following quantities are equal:

(i) number a_n of n-steps $\mathscr{S}$-walks confined to the upper half plane $\mathbb{Z} \times \mathbb{N}$ that start and finish at the origin $(0,0)$ (*excursions*);

(ii) number b_n of n-steps $\mathscr{S}$-walks confined to the quarter plane $\mathbb{N}^2$ that start at the origin $(0,0)$ and finish on the diagonal of $\mathbb{N}^2$ (*diagonal walks*).

For instance, for $n = 3$, this common value is $a_3 = b_3 = 3$:



A recurrence relation for $\{\uparrow, \leftarrow, \searrow\}$-walks in $\mathbb{Z} \times \mathbb{N}$

$h(n;i,j)$ = nb. of $\{\uparrow, \leftarrow, \searrow\}$-walks in $\mathbb{Z} \times \mathbb{N}$ of length n from $(0,0)$ to (i,j)
The numbers $h(n;i,j)$ satisfy

$$h(n;i,j) = \begin{cases} 0 & \text{if } j < 0 \text{ or } n < 0, \\ \mathbb{1}_{i=j=0} & \text{if } n = 0, \\ \sum\limits_{(i',j') \in \mathscr{S}} h(n-1; i-i', j-j') & \text{otherwise.} \end{cases}$$

```
> h:=proc(n,i,j)
  option remember;
    if j<0 or n<0 then 0
    elif n=0 then if i=0 and j=0 then 1 else 0 fi
    else h(n-1,i,j-1) + h(n-1,i+1,j) + h(n-1,i-1,j+1) fi
  end:

> A:=series(add(h(n,0,0)*t^n, n=0..12), t,12);
```

$$A = 1 + 3t^3 + 30t^6 + 420t^9 + O(t^{12})$$

A recurrence relation for $\{\uparrow, \leftarrow, \searrow\}$-walks in $\mathbb{N}^2$

$q(n;i,j)$ = nb. of $\{\uparrow, \leftarrow, \searrow\}$-walks in $\mathbb{N}^2$ of length n from $(0,0)$ to (i,j)
The numbers $q(n;i,j)$ satisfy

$$q(n;i,j) = \begin{cases} 0 & \text{if } i < 0 \text{ or } j < 0 \text{ or } n < 0, \\ \mathbb{1}_{i=j=0} & \text{if } n = 0, \\ \sum_{(i',j') \in \mathscr{S}} q(n-1; i-i', j-j') & \text{otherwise.} \end{cases}$$

```
> q:=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 q(n-1,i,j-1) + q(n-1,i+1,j) + q(n-1,i-1,j+1) fi
  end:

> B:=series(add(add(q(n,k,k), k=0..n)*t^n, n=0..12), t,12);
```

$$B = 1 + 3t^3 + 30t^6 + 420t^9 + O(t^{12})$$

Guessing the answer

```
> A:=series(add(h(n,0,0)*t^n, n=0..30), t, 25):
> recA:=seriestorec(A, a(n))[1];
```

$$(n+6)\,(n+3)\,u\,(n+3) - 27\,(n+2)\,(n+1)\,u\,(n) = 0$$

```
> an:=rsolve(recA, a(n)):
> sum(subs(n=3*n, op(2,an))*t^(3*n), n=0..infinity)
                                        assuming t>0 and t<1/9;
```

$${}_2F_1\left(\begin{matrix}1/3 \quad 2/3\\ 2\end{matrix}\,\middle|\, 27\,t^3\right)$$

Guessing the answer

```
> A:=series(add(h(n,0,0)*t^n, n=0..30), t, 25):
> recA:=seriestorec(A, a(n))[1];
```

$$(n+6)(n+3)\,u(n+3) - 27\,(n+2)(n+1)\,u(n) = 0$$

```
> an:=rsolve(recA, a(n)):
> sum(subs(n=3*n, op(2,an))*t^(3*n), n=0..infinity)
                                      assuming t>0 and t<1/9;
```

$$ {}_2F_1\left(\left.\begin{matrix} 1/3 \quad 2/3 \\ 2 \end{matrix}\right| 27\,t^3\right) $$

▷ Thus, differential guessing predicts

$$A(t) = B(t) = {}_2F_1\left(\left.\begin{matrix} 1/3 \quad 2/3 \\ 2 \end{matrix}\right| 27\,t^3\right) = \sum_{n=0}^{\infty} \frac{(3n)!}{n!^3}\,\frac{t^{3n}}{n+1}.$$

Guessing the answer

```
> A:=series(add(h(n,0,0)*t^n, n=0..30), t, 25):
> recA:=seriestorec(A, a(n))[1];
```

$$(n+6)(n+3)u(n+3) - 27(n+2)(n+1)u(n) = 0$$

```
> an:=rsolve(recA, a(n)):
> sum(subs(n=3*n, op(2,an))*t^(3*n), n=0..infinity)
                                    assuming t>0 and t<1/9;
```

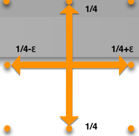
$${}_2F_1\left(\begin{matrix}1/3 \quad 2/3\\ 2\end{matrix}\,\middle|\, 27\,t^3\right)$$

▷ Thus, differential guessing predicts

$$A(t) = B(t) = {}_2F_1\left(\begin{matrix}1/3 \quad 2/3\\ 2\end{matrix}\,\middle|\, 27\,t^3\right) = \sum_{n=0}^{\infty} \frac{(3n)!}{n!^3}\,\frac{t^{3n}}{n+1}.$$

▷ This can be algorithmically proved using creative telescoping

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));
```

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

Example: guessing equations for $F_{\mathscr{S}}(t;x,0)$ and $F_{\mathscr{S}}(t;0,y)$

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

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

Example: guessing equations for $F_{\mathscr{S}}(t;x,0)$ and $F_{\mathscr{S}}(t;0,y)$

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

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

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

Example: guessing equations for $F_{\mathscr{S}}(t;x,0)$ and $F_{\mathscr{S}}(t;0,y)$

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

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

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

- Both tasks amount to linear algebra in size N over $\mathbb{Q}(x)$.
- In practice: use many modular Hermite-Padé approximations (via the Beckermann-Labahn algorithm) combined with (rational) evaluation-interpolation and rational number reconstruction.
- Fast (FFT-based) arithmetic in $\mathbb{F}_p[t]$ and $\mathbb{F}_p[t]\langle \frac{t}{\partial t} \rangle$.

Example: guessing equations for Kreweras' $K(t;x,0)$

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

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

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

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

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

Example: guessing equations for Gessel's $G(t;x,0)$ and $G(t;0,y)$

Using $N = 1200$ terms of $G(t;x,y)$, one can guess candidates

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

such that

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

Using $N = 1200$ terms of $G(t;x,y)$, one can guess candidates

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

such that

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

▷ 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!

Using $N = 1200$ terms of $G(t;x,y)$, one can guess candidates

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

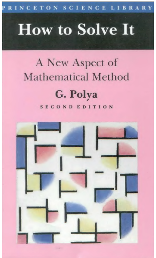
such that

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

▷ 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!

▷ [B., Kauers '09] actually first guessed differential equations†, then computed their p-curvatures to empirically certify them. This led them suspect the algebraicity of $G(t;x,0)$ and $G(t;0,y)$, using a conjecture of Grothendieck's (on differential equations modulo p) 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.

TOOLS FOR PROOFS

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 over a commutative ring R.

Basic observation

If $A = a_m x^m + \cdots + a_0$ and $B = b_n x^n + \cdots + b_0$, 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 $\operatorname{Res}(A, B) = 0$.

Example: the discriminant

The discriminant of A is the resultant of A and of its derivative A'.
E.g. for $A = ax^2 + bx + c$,

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

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

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

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

Main properties

- **Link with gcd** $\text{Res}(A,B) = 0$ 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:

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

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

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

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

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

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

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

$$\mathrm{Res}_x(A(x), t - B(x)) = \prod_{i} (t - B(\alpha_i)).$$

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

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

Two beautiful identities of Ramanujan's

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

▷ If $a = \pi/7$ and $x = e^{ia}$, then $x^7 = -1$ and $\cos(ka) = \frac{x^k + x^{-k}}{2}$

Two beautiful identities of Ramanujan's

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

▷ If $a = \pi/7$ and $x = e^{ia}$, then $x^7 = -1$ and $\cos(ka) = \frac{x^k + x^{-k}}{2}$

▷ Since $x \in \overline{\mathbb{Q}}$, any polynomial expression in the $\cos(ka)$ is in $\mathbb{Q}(x)$, thus in $\overline{\mathbb{Q}}$

Two beautiful identities of Ramanujan's

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

▷ If $a = \pi/7$ and $x = e^{ia}$, then $x^7 = -1$ and $\cos(ka) = \frac{x^k + x^{-k}}{2}$

▷ Since $x \in \overline{\mathbb{Q}}$, any polynomial expression in the $\cos(ka)$ is in $\mathbb{Q}(x)$, thus in $\overline{\mathbb{Q}}$

▷ In particular $v = F(x) = \frac{N(x)}{D(x)}$ is an algebraic number

```
> 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,%)):
```

$$\frac{2\,i\left(x^{16}+5\,x^{14}+12\,x^{12}+x^{11}+20\,x^{10}+3\,x^9+23\,x^8+3\,x^7+20\,x^6+x^5+12\,x^4+5\,x^2+1\right)}{x\left(x^2-1\right)\left(x^2+1\right)^2\left(x^4+x^2+1\right)^2}$$

Two beautiful identities of Ramanujan's

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

- ▷ If $a = \pi/7$ and $x = e^{ia}$, then $x^7 = -1$ and $\cos(ka) = \frac{x^k + x^{-k}}{2}$
- ▷ Since $x \in \overline{\mathbb{Q}}$, any polynomial expression in the $\cos(ka)$ is in $\mathbb{Q}(x)$, thus in $\overline{\mathbb{Q}}$
- ▷ In particular $v = F(x) = \frac{N(x)}{D(x)}$ is an algebraic number

```
> 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,%)):
```

$$\frac{2i\left(x^{16}+5x^{14}+12x^{12}+x^{11}+20x^{10}+3x^9+23x^8+3x^7+20x^6+x^5+12x^4+5x^2+1\right)}{x\,(x^2-1)\,(x^2+1)^2\,(x^4+x^2+1)^2}$$

- ▷ Get polynomial in $\mathbb{Q}[t]$ with root v: resultant $\mathrm{Res}_x(x^7+1, t\cdot D(x) - N(x))$

```
> factor(resultant(x^7+1,t*denom(F)-numer(F),x));
```

$$-1274\,i\left(t^2-28\right)^3$$

TOOLS FOR PROOFS

D-Finiteness

D-finite Series & Sequences

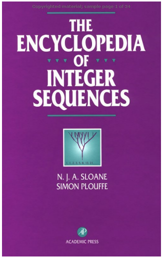
Definition: A power series $f(x) \in \mathbb{K}[[x]]$ is D-finite over $\mathbb{K}$ if its derivatives generate a finite-dimensional vector space over $\mathbb{K}(x)$.

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

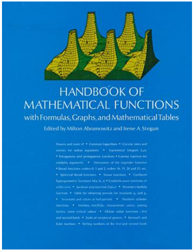
$$p_r(n)u_{n+r} + p_{r-1}(n)u_{n+r-1} + \cdots + p_0(n)u_n = 0, \qquad n \geq 0.$$

equation + init conditions = 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,...



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

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

Proof by 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

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

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

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

So, $f+g$ 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);
```

$$1 + O(x^4)$$

This proves $\sin(x)^2 + \cos(x)^2 = 1$. Why?

(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) $\implies \sin^2 + \cos^2 - 1$ 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 8 do
   fibonacci(n)^2-fibonacci(n+1)*fibonacci(n-1)+(-1)^n
od;
```

$$0, 0, 0, 0, 0, 0, 0, 0$$

Algebraic series are D-finite

Theorem [Abel 1827, Cockle 1860, Harley 1862] Algebraic series are D-finite, i.e., they satisfy linear differential equations with polynomial coefficients.

Algebraic series are D-finite

Theorem [Abel 1827, Cockle 1860, Harley 1862] Algebraic series are D-finite, thus, their coefficients satisfy linear recurrences with polynomial coefficients.

Theorem [Abel 1827, Cockle 1860, Harley 1862] Algebraic series are D-finite.

Proof: Let $f(t) \in \mathbb{Q}[[t]]$ such that $P(t, f(t)) = 0$, with $P \in \mathbb{Q}[t, T]$ irreducible.

Differentiate w.r.t. t:

$$P_t(t, f(t)) + f'(t) P_T(t, f(t)) = 0 \qquad \Longrightarrow \qquad f' = -\frac{P_t}{P_T}(t, f(t)).$$

Extended gcd: $\gcd(P, P_T) = 1 \implies UP + VP_T = 1$, for $U, V \in \mathbb{Q}(t)[T]$

$$\Longrightarrow \quad f' = -\Big(P_t V \bmod P\Big)(t, f) \in \mathsf{Vect}_{\mathbb{Q}(t)}\left(1, f, f^2, \ldots, f^{\deg_T(P)-1}\right).$$

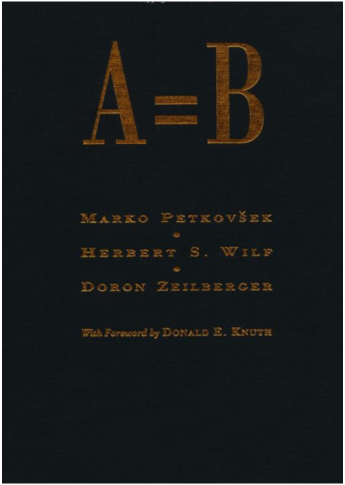
By induction, $f^{(\ell)} \in \mathsf{Vect}_{\mathbb{Q}(t)}\left(1, f, f^2, \ldots, f^{\deg_T(P)-1}\right)$, for all ℓ. □

▷ Implemented, e.g., in maple's package gfun — algeqtodiffeq, diffeqtorec
▷ Generalization: g D-finite, f algebraic $\to g \circ f$ D-finite — algebraicsubs

TOOLS FOR PROOFS

Creative Telescoping

General framework in computer algebra –initiated by Zeilberger in the ’90s– for proving identities on multiple integrals and sums with parameters.



Examples I: hypergeometric summation

- $\displaystyle\sum_{k\in\mathbb{Z}} (-1)^k \binom{a+b}{a+k}\binom{a+c}{c+k}\binom{b+c}{b+k} = \frac{(a+b+c)!}{a!b!c!}$ [Dixon 1891]

- $\displaystyle A_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$ satisfies the recurrence [Apéry 1978]:

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

(*Neither Cohen nor I had been able to prove this in the intervening two months* [Van der Poorten 1979])

- $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} \sum_{j=0}^{k} \binom{k}{j}^3$ [Strehl 1992]

Examples I: hypergeometric summation

- $$\sum_{k\in\mathbb{Z}} (-1)^k \binom{a+b}{a+k}\binom{a+c}{c+k}\binom{b+c}{b+k} = \frac{(a+b+c)!}{a!b!c!}$$ [Dixon 1891]

- $A_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$ satisfies the recurrence [Apéry 1978]:

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

(*The specific problem was mentioned to Don Zagier, who solved it with irritating speed* [Van der Poorten 1979])

- $$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} \sum_{j=0}^{k} \binom{k}{j}^3$$ [Strehl 1992]

Examples II: Integrals and Diagonals

- $\displaystyle\int_0^1 \frac{\cos(zu)}{\sqrt{1-u^2}}\,du = \int_1^{+\infty} \frac{\sin(zu)}{\sqrt{u^2-1}}\,du = \frac{\pi}{2} J_0(z);$

- $\displaystyle\int_0^{+\infty} x J_1(ax) I_1(ax) Y_0(x) K_0(x)\,dx = -\frac{\ln(1-a^4)}{2\pi a^2}$ [Glasser-Montaldi 1994];

- $\displaystyle\frac{1}{2\pi i} \oint \frac{(1+2xy+4y^2)\exp\left(\frac{4x^2y^2}{1+4y^2}\right)}{y^{n+1}(1+4y^2)^{\frac{3}{2}}}\,dy = \frac{H_n(x)}{\lfloor n/2 \rfloor!}$ [Doetsch 1930];

- $\displaystyle\operatorname{Diag} \frac{1}{(1-x-y)(1-z-u)-xyzu} = \sum_{n\geq 0} A_n t^n$ [Straub 2014].

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

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 $P(n, S_n)$ and $R(n, k, S_n, S_k)$ such that

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

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

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

Zeilberger's Algorithm [1990]

Input: a hypergeometric term $u_{n,k}$, i.e., $\frac{u_{n+1,k}}{u_{n,k}}$ and $\frac{u_{n,k+1}}{u_{n,k}}$ are in $\mathbb{Q}(n,k)$

Output:

- a linear recurrence, called telescoper, (P) satisfied by $F_n = \sum_k u_{n,k}$
- a certificate (Q), such that checking the result is easy from $P(n,S_n) \cdot u_{n,k} = \Delta_k Q \cdot u_{n,k}$.

```
> T := binomial(n,k);
> Zpair:=SumTools[Hypergeometric][Zeilberger](T,n,k,Sn):
> tel:=Zpair[1];
```

$$S_n - 2$$

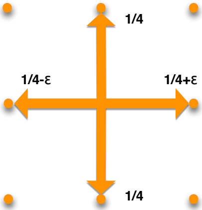
▷ This is a proof that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

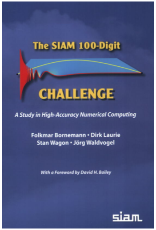
▷ Can check using the certificate:

```
> cert:=Zpair[2];
> iszero:=(subs(n=n+1,T) - 2*T) - (subs(k=k+1,cert) - cert);
> simplify(convert(%,GAMMA));
```

$$0$$

Example: Back to the SIAM flea





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

$$p_n = \sum_{k=0}^{n} U_{n,k} \quad = \text{probability of return to } (0,0) \text{ at step } 2n.$$

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

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

$$I(t) = \oint_\gamma H(t,x)\,dx = ?$$

IF one knows $P(t, \partial_t)$ and $R(t, x, \partial_t, \partial_x)$ such that

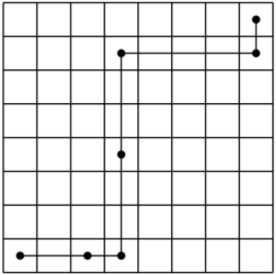
$$\left(P(t,\partial_t) + \partial_x R(t,x,\partial_t,\partial_x)\right) \cdot H(t,x) = 0,$$

then the integral “telescopes”, leading to

$$P(t,\partial_t) \cdot I(t) = 0.$$

Diagonal Rook paths

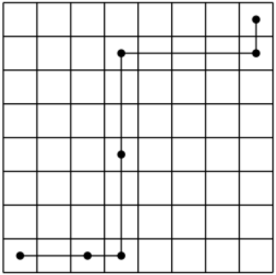
Question: A chess Rook can move any number of squares horizontally or vertically in one step. How many paths can a Rook take from the lower-left corner square to the upper-right corner square of an $N \times N$ chessboard? Assume that the Rook moves right or up at each step.



$$(r_n)_{n \geq 0} : \quad 1,\ 2,\ 14,\ 106,\ 838,\ 6802,\ 56190,\ 470010,\ \ldots$$

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.



$$(r_n)_{n \geq 0}: \quad 1,\ 2,\ 14,\ 106,\ 838,\ 6802,\ 56190,\ 470010,\ \ldots$$

Answer: r_N = Nth coefficient in the Taylor expansion of $\frac{1}{2}\left(1+\sqrt{\frac{1-x}{1-9x}}\right)$.

Generating function of the sequence

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

is

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

By creative telescoping, $\mathsf{Diag}(F)$ satisfies the differential equation

```
> F:=1/(1-x/(1-x)-y/(1-y)):
> G:=normal(1/x*subs(y=t/x,F)):
> Zeilberger(G, t, x, Dt)[1];
```

$$(9t^2 - 10t + 1)\partial_t^2 + (18t - 14)\partial_t$$

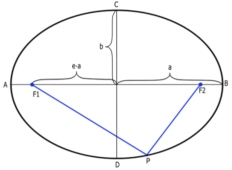
Answer: Generating series of diagonal Rook paths is $\frac{1}{2}\left(1 + \sqrt{\frac{1-t}{1-9t}}\right).$

Creative Telescoping for Multiple Integration

Example [Euler, 1733]: Perimeter of an ellipse of eccentricity e, semi-major axis 1

Example [Euler, 1733]: Perimeter of an ellipse of eccentricity e, semi-major axis 1

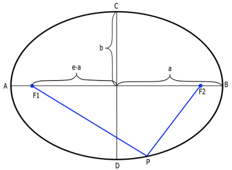
$$p(e) = 4\int_0^1 \sqrt{\frac{1-e^2u^2}{1-u^2}}\,\mathrm{d}u = 4\oint\!\!\oint \frac{\mathrm{d}u\mathrm{d}v}{1-\frac{1-e^2u^2}{(1-u^2)v^2}}$$



Principle: Find algorithmically

Example [Euler, 1733]: Perimeter of an ellipse of eccentricity e, semi-major axis 1

$$p(e) = 4\int_0^1 \sqrt{\frac{1-e^2u^2}{1-u^2}}\,\mathrm{d}u = 4\oint\!\!\oint \frac{\mathrm{d}u\mathrm{d}v}{1-\frac{1-e^2u^2}{(1-u^2)v^2}}$$



Principle: Find algorithmically

$$\left((e-e^3)\partial_e^2 + (1-e^2)\partial_e + e\right)\cdot\left(\frac{1}{1-\frac{1-e^2u^2}{(1-u^2)v^2}}\right) =$$

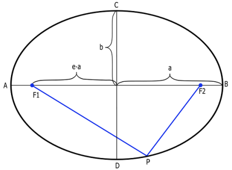
$$\partial_u\left(-\frac{e\left(-1-u+u^2+u^3\right)v^2\left(-3+2u+v^2+u^2\left(-2+3e^2-v^2\right)\right)}{\left(-1+v^2+u^2(e^2-v^2)\right)^2}\right)$$

$$+\,\partial_v\left(\frac{2e\left(-1+e^2\right)u\left(1+u^3\right)v^3}{\left(-1+v^2+u^2(e^2-v^2)\right)^2}\right)$$

▷ Conclusion: $p(e) = \frac{\pi}{2}\cdot {}_2F_1\left(\begin{matrix}-\frac{1}{2} & \frac{1}{2}\\ & 1\end{matrix}\,\middle|\, e^2\right) = 2\pi - \frac{\pi}{2}e^2 - \frac{3\pi}{32}e^4 - \cdots.$

Example [Euler, 1733]: Perimeter of an ellipse of eccentricity e, semi-major axis 1

$$p(e) = 4\int_0^1 \sqrt{\frac{1-e^2u^2}{1-u^2}}\mathrm{d}u = 4\oint\!\!\oint \frac{\mathrm{d}u\mathrm{d}v}{1-\frac{1-e^2u^2}{(1-u^2)v^2}}$$



Principle: Find algorithmically

$$\left((e-e^3)\partial_e^2 + (1-e^2)\partial_e + e\right)\cdot\left(\frac{1}{1-\frac{1-e^2u^2}{(1-u^2)v^2}}\right) =$$

$$\partial_u\left(-\frac{e\left(-1-u+u^2+u^3\right)v^2\left(-3+2u+v^2+u^2\left(-2+3e^2-v^2\right)\right)}{\left(-1+v^2+u^2(e^2-v^2)\right)^2}\right)$$

$$+\,\partial_v\left(\frac{2e\left(-1+e^2\right)u\left(1+u^3\right)v^3}{\left(-1+v^2+u^2(e^2-v^2)\right)^2}\right)$$

▷ Drawback: Size(certificate) $\gg$ Size(telescoper).

Algorithm for the integration of rational functions [B., Lairez, Salvy, 2013]

- **Input:** $R(e, \mathbf{x})$ a rational function in e and $\mathbf{x} = x_1, \ldots, x_n$.
- **Output:** A linear ODE $T(e, \partial_e) y = 0$ satisfied by $y(e) = \oint\!\!\oint R(e, \mathbf{x}) d\mathbf{x}$.
- **Complexity:** $\mathcal{O}(D^{8n+2})$, where $D = \deg R$.
- **Output size:** T has order $\leq D^n$ in ∂_e and degree $\leq D^{3n+2}$ in e.

▷ Avoids the (costly) computation of certificates, of size $\Omega(D^{n^2/2})$.

▷ Previous algorithms: complexity (at least) doubly exponential in n.

▷ Very efficient in practice.

Exercises

1. Explain why $\sum_n F_n t^n$ is rational, where $F_{n+2} = F_{n+1} + F_n, F_0 = 0, F_1 = 1$. Find a general statement.
2. Show that the series $\sum_n \binom{2n}{n} t^n$ and $\sum_n \binom{5n}{n} t^n$ are both algebraic.
3. Prove that the series
   - $\sqrt{1-4t} = 1 - 2\,t - 2\,t^2 - 4\,t^3 - 10\,t^4 - 28\,t^5 - \cdots$
   - $\sqrt[3]{1-9t} = 1 - 3\,t - 9\,t^2 - 45\,t^3 - 270\,t^4 - 1782\,t^5 - \cdots$

   have only integer coefficients. Try to generalize.
4. Prove that $\tan(t) = t + \frac{1}{3}t^3 + \frac{2}{15}t^5 + \frac{17}{315}t^7 + \frac{62}{2835}t^9 + \cdots$ is not D-finite.
5. Let $M_{n,k}$ be the number of $\{(1,1),(1,-1)\}$-walks in $\mathbb{N}^2$ of length n that start at $(0,0)$ and end at vertical altitude k. Let $M(x,y) = \sum_{n,k} M_{n,k} x^n y^k$.

   (a) Show that $(y - x(1+y^2)) \cdot M(x,y) = y - x \cdot M(x,0)$

   (b) Deduce that $M(x,y) = \dfrac{\sqrt{1-4x^2} + 2xy - 1}{2x(y - x(1+y^2))}$