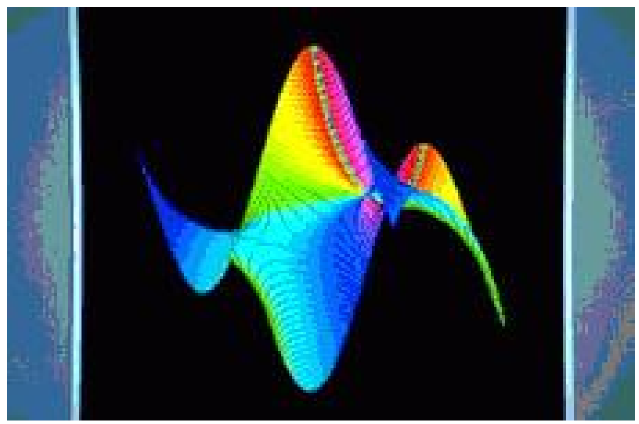
Computer algebra for Combinatorics

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);
```

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

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);
```

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

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

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]]);
```

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

```
> 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);
```

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

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 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

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

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 $\mathsf{Res}\,(A,B)=0$ 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

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

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

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

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

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

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

- 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 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)):
                                  2       3
                    -1274 I (t  - 28)
```

- 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 γ_i of F at the pole β_i equals $\gamma_i = \frac{A(\beta_i)}{B'(\beta_i)}$.

Theorem. The residues γ_i of F are roots of the Rothstein-Trager resultant

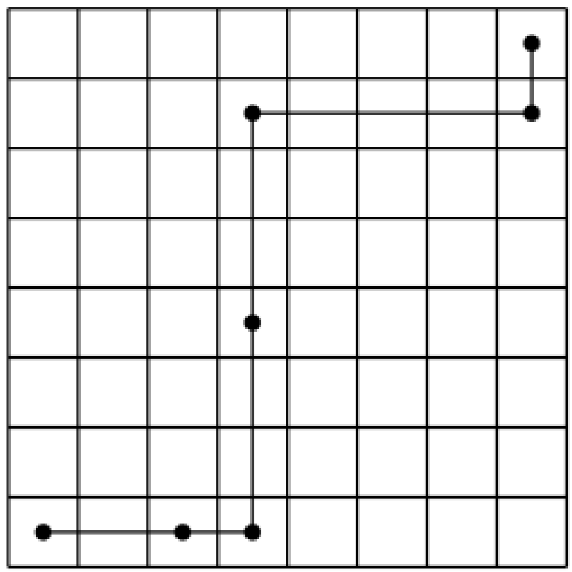
$$R(t) = \mathsf{Res}_x\big(B(x),\ A(x) - t \cdot B'(x)\big).$$

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 $\deg Q_i \leq d$, 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

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

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

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

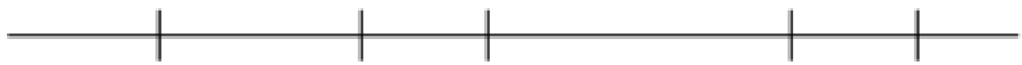
- By Hadamard, $R(x) = \mathrm{Res}_y(P, Q) \in \mathbb{K}[x]$ has degree at most $2dn$.
- By elimination, $R(x) = UP + VQ$ for $U, V \in \mathbb{K}[x, y]$ with $\deg_y(V) < n$.
- Evaluation at $y = A(x)$ yields

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

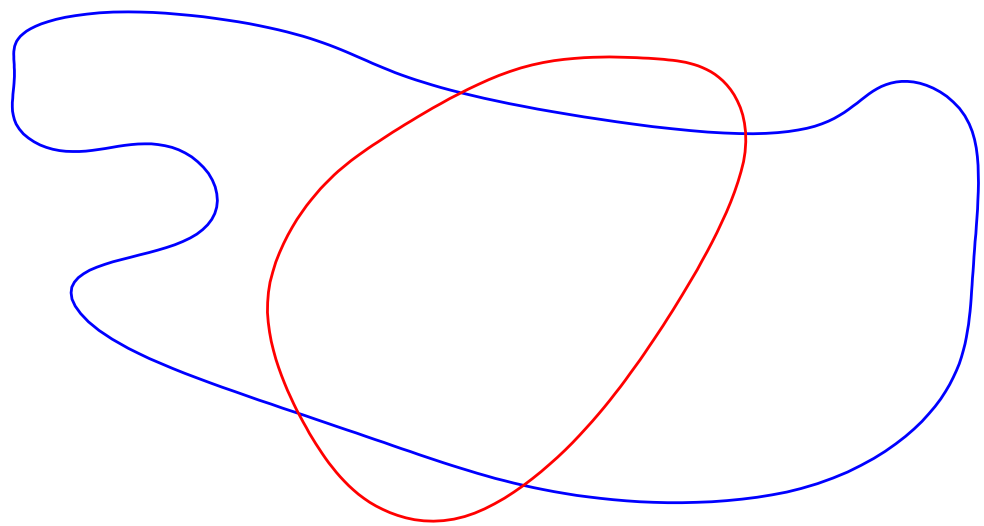
- Thus $R = 0$, that is $\gcd(P, Q) \neq 1$, and thus $P \mid Q$, and A is a root of Q.

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 $A = 0$.

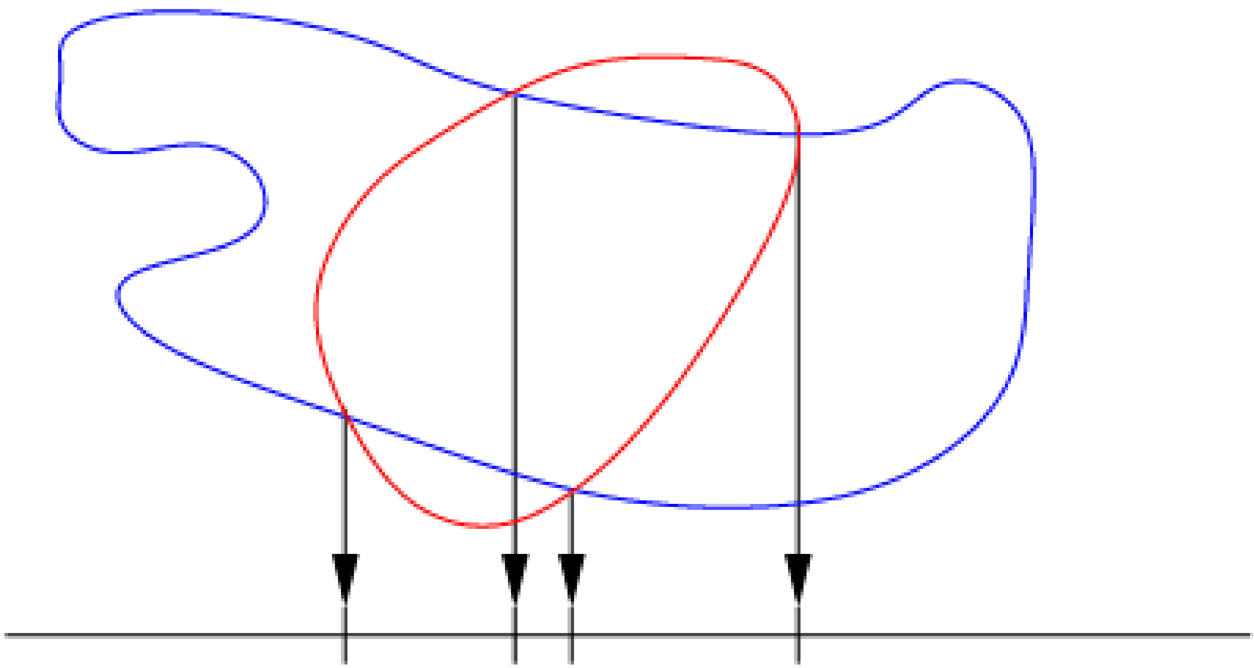


Let now A and B be in $\mathbb{Q}[x, y]$. Then:

- 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 $\mathrm{Res}_y(A, B) \in \mathbb{Q}[x]$ are either the abscissas of points in the intersection $A = B = 0$, or common roots of a_m and b_n.



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

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

Application: implicitization of parametric curves

Task: Given a rational parametrization of a curve

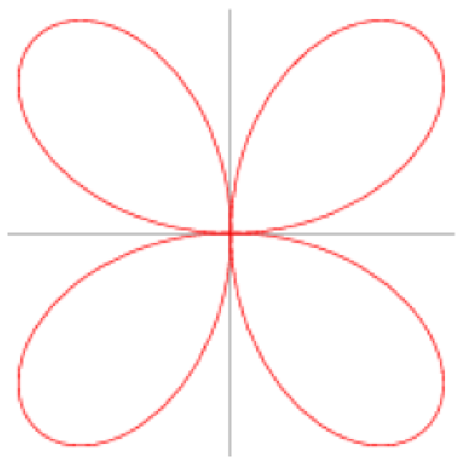
$$x = A(t), \quad y = B(t), \qquad A, B \in \mathbb{K}(t),$$

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

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



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

TOOLS FOR PROOFS

3. D-Finiteness

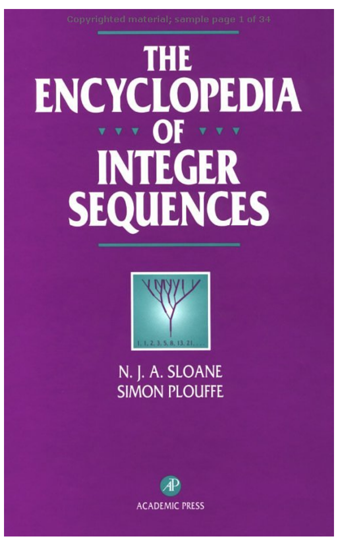
D-finite Series & Sequences

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 $\mathbb{K}(x)$.

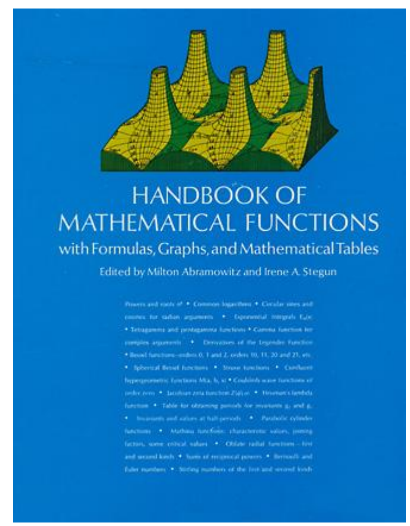
A sequence u_n is **D-finite** (or **P-recursive**) over $\mathbb{K}$ when its shifts $(u_n, u_{n+1}, \dots)$ generate a finite-dimensional vector space over $\mathbb{K}(n)$.

equation + init conditions = data structure

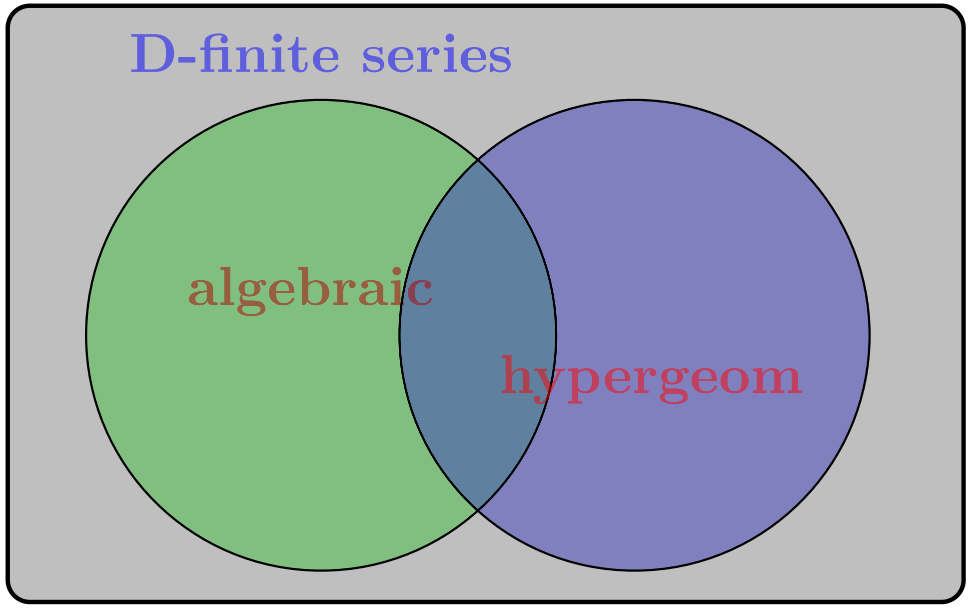
About 25% of Sloane's encyclopedia, 60% of Abramowitz & Stegun



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,...



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

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

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

- Implemented in gfun: algeqtodiffeq
- Generalization: g D-finite, f algebraic $\to g \circ f$ 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 $1 + (x-1)y + x^2y^2 = 0$. 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

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

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. □

TOOLS FOR PROOFS

4. Creative Telescoping

Examples I: hypergeometric summation

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

- $\displaystyle A_n=\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}^2$ 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]).

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

Examples II: Integrals

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

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 $\mathrm{Diag}(f) = \sum_{n \geq 0} c_{n, \dots, n} x^n \in \mathbb{K}[[x]]$.

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]:

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

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]:

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

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 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

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

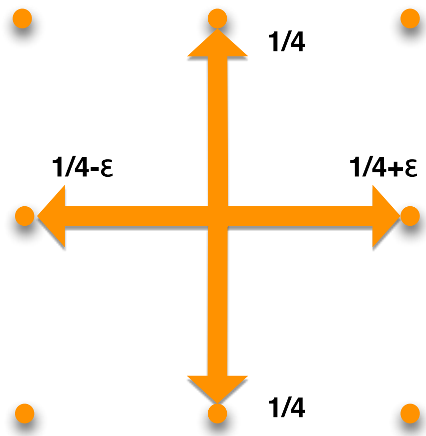
Zeilberger's Algorithm [1990]

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,

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

On power series,

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

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,

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

Proof:

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

Special Case: Diagonals

Analytically,

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

On power series,

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

Proof:

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

Extends to more variables: $\operatorname{Diag} F(x,y,z)$ 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;
```

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

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!)