Algebraicity and transcendence of power series: combinatorial and computational aspects

Alin Bostan

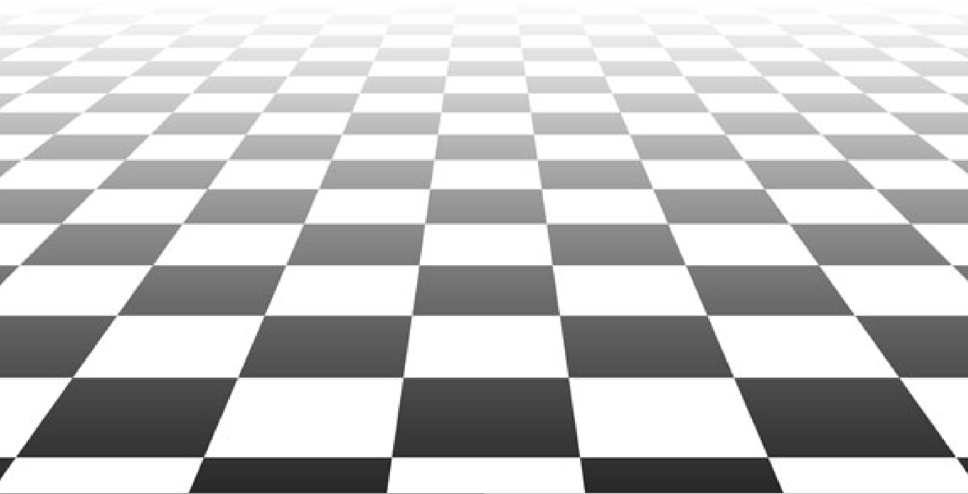
Inria informatics mathematics

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

Overview

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

Part II: Properties and Criteria (1)



In contrast with the "hard" theory of arithmetic transcendence, it is usually "easy" to establish transcendence of functions.

[Flajolet, Sedgewick, 2009]

- A power series f in $\mathbb{Q}[[t]]$ is called *algebraic* if it is a root of some algebraic equation $P(t, f(t)) = 0$, where $P(x, y) \in \mathbb{Z}[x, y] \setminus \{0\}$.
- A power series that is not algebraic is called *transcendental*.

▷ Task: Given a power series, either in explicit or in implicit form, determine whether it is algebraic or transcendental.

Properties

Almost all power series are transcendental

Almost anything is non-holonomic unless it is holonomic by design. (This naïve remark cannot of course be universally true and there are surprises, e.g., some sequences may eventually admit algebraic or holonomic descriptions for rather deep reasons.)

[Flajolet, Gerhold, Salvy, 2005]

Theorem [Pólya, 1918], [Steinhaus, 1930], [Boerner, 1938]
"Almost all power series are transcendental":

There is a natural topology on the space of all power series with radius of convergence 1 such that the set of transcendental power series is open and dense in this topological space.

Establishing transcendence of values at an algebraic point constitutes in principle the most straightforward transcendence criterion for functions, although it is almost invariably the most difficult to apply.

[Flajolet, 1987]

Theorem Let $f \in \mathbb{Q}[[t]]$

1. If f is algebraic and $a \in \overline{\mathbb{Q}}$, then $f(a) \in \overline{\mathbb{Q}}$
2. If f is algebraic and if p is a prime number such that $f_p = f \bmod p$ is well-defined in $\mathbb{F}_p[[t]]$, then f_p is algebraic over $\mathbb{F}_p(t)$

Two easy criteria

Establishing transcendence of values at an algebraic point constitutes in principle the most straightforward transcendence criterion for functions, although it is almost invariably the most difficult to apply.

[Flajolet, 1987]

Criteria Let $f \in \mathbb{Q}[[t]]$

1. If $a \in \overline{\mathbb{Q}}$ such that $f(a) \notin \overline{\mathbb{Q}}$, then f is transcendental
2. If p is a prime number such that $f_p = f \bmod p$ is well-defined in $\mathbb{F}_p[[t]]$ and f_p is not algebraic over $\mathbb{F}_p(t)$, then f is transcendental

Main properties of algebraic series

- Algebraic properties
  - Algebraic series form an algebra
  - Algebraic series are D-finite
  - Algebraic series are diagonals of bivariate rational functions
- Arithmetic properties
  - Algebraic series have almost integer coefficients
  - The coefficient sequence mod p of an algebraic series is p-automatic
  - Algebraic irrational series are badly approximated by rational series
  - Resolvents of algebraic series have zero p-curvature
- Analytic properties
  - The coefficient sequence of an algebraic series has small gaps
  - The coefficient sequence of an algebraic series has "nice" asymptotics
  - Resolvents of algebraic series are Fuchsian

Resulting transcendence criteria

- If a series is not D-finite
- If a series does not have almost integer coefficients
- If the coefficient sequence mod p of a series is not p-automatic
- If an irrational series can be too well approximated by rational series
- If the resolvent of a D-finite series has a non-zero p-curvature
- If the coefficient sequence of a series has large gaps
- If the coefficient sequence of a series has “ugly” asymptotics
- If the resolvent of a D-finite series is not Fuchsian

then the series is transcendental

Algebraic properties

Very quick refresh on resultants

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

Very quick refresh on resultants

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

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

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

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

- **Bézout-Hadamard bound**
  If $A, B \in \mathbb{Q}[x, y]$, then $\mathrm{Res}_y(A, B)$ is a polynomial in $\mathbb{Q}[x]$ of degree

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

Algebraic series form an algebra

Theorem

Let $P, Q \in \mathbb{Q}[t, T] \setminus \{0\}$ be annihilating polynomials for $f, g \in \mathbb{Q}[[t]]$. Then:

- $f + g$ is algebraic, root of $\mathsf{Res}_z(P(t,z), Q(t, T-z))$
- fg is algebraic, root of $\mathsf{Res}_z(P(t,z), z^{\deg_T Q} Q(t, T/z))$
- $1/f$ is algebraic (if $f(0) \neq 0$), root of $T^{\deg_T P} P(t, 1/T))$
- $f \circ g$ is algebraic (if $g(0) = 0$), root of $\mathsf{Res}_z(P(t,z), Q(z,T))$
- f' is algebraic, root of $\mathsf{Res}_z(P(t,z), P_t(t,z) + TP_T(t,z))$ $\qquad P_t := \frac{\partial P}{\partial t}$

Algebraic series form an algebra

Theorem

Let $P, Q \in \mathbb{Q}[t,T] \setminus \{0\}$ be annihilating polynomials for $f, g \in \mathbb{Q}[[t]]$. Then:

- $f+g$ is algebraic, root of $\mathrm{Res}_z(P(t,z), Q(t,T-z))$
- fg is algebraic, root of $\mathrm{Res}_z(P(t,z), z^{\deg_T Q} Q(t,T/z))$
- $1/f$ is algebraic (if $f(0) \neq 0$), root of $T^{\deg_T P} P(t,1/T))$
- $f \circ g$ is algebraic (if $g(0) = 0$), root of $\mathrm{Res}_z(P(t,z), Q(z,T))$
- f' is algebraic, root of $\mathrm{Res}_z(P(t,z), P_t(t,z) + TP_T(t,z))$ $\qquad P_t := \frac{\partial P}{\partial t}$

Proof: Let $R(t,T)$ denote the first resultant. By the elimination property:

$$R(t,T) = U(t,z,T) \cdot P(t,z) + V(t,z,T) \cdot Q(t,T-z).$$

for some $U, V \in \mathbb{Q}[t,z,T]$.

Evaluating this equality at $(z,T) = (f(t), f(t)+g(t))$ gives $R(t, f+g) = 0$.

For f', the result follows from $P_t(t, f(t)) + f'(t) \cdot P_T(t, f(t)) = 0$. $\square$

Theorem

Let $P, Q \in \mathbb{Q}[t,T] \setminus \{0\}$ be annihilating polynomials for $f, g \in \mathbb{Q}[[t]]$. Then:

- $f + g$ is algebraic, root of $\mathsf{Res}_z(P(t,z), Q(t, T-z))$
- fg is algebraic, root of $\mathsf{Res}_z(P(t,z), z^{\deg_T Q} Q(t, T/z))$
- $1/f$ is algebraic (if $f(0) \neq 0$), root of $T^{\deg_T P} P(t, 1/T))$
- $f \circ g$ is algebraic (if $g(0) = 0$), root of $\mathsf{Res}_z(P(t,z), Q(z,T))$
- f' is algebraic, root of $\mathsf{Res}_z(P(t,z), P_t(t,z) + TP_T(t,z))$ $\qquad P_t := \frac{\partial P}{\partial t}$

Proof: Let $R(t,T)$ denote the first resultant. By the elimination property:

$$R(t,T) = U(t,z,T) \cdot P(t,z) + V(t,z,T) \cdot Q(t, T-z).$$

for some $U, V \in \mathbb{Q}[t,z,T]$.

Evaluating this equality at $(z,T) = (f(t), f(t)+g(t))$ gives $R(t, f+g) = 0$.

For f', the result follows from $P_t(t, f(t)) + f'(t) \cdot P_T(t, f(t)) = 0$. $\square$

$\triangleright$ More efficient algorithms $\longrightarrow$ Friday

Bonus: Hadamard products

Theorem [Jungen, 1931]
The Hadamard product of an algebraic and a rational series is algebraic.
The Hadamard product of two algebraic series is not necessarily algebraic:

$$\frac{1}{\sqrt{1-t}} \odot \frac{1}{\sqrt{1-t}} = {}_2F_1\left(\left.\begin{matrix}\frac{1}{2} \quad \frac{1}{2}\\ 1\end{matrix}\right| t\right).$$

Proof: Partial fraction decomposition + distributivity of Hadamard product +

$$f \odot \frac{1}{(1-t)^{\kappa+1}} = \frac{1}{\kappa!}\Big(t^{\kappa} f(t)\Big)^{(\kappa)} \quad \iff \quad t^n \cdot \binom{n+k}{n} = \frac{1}{\kappa!}\Big(t^{\kappa+n}\Big)^{(\kappa)} \quad \text{for all } n$$

Theorem [Bézivin, 1986]
If an algebraic $f \in \mathbb{Q}[[t]]$ has algebraic Hadamard inverse, then f is rational.

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

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

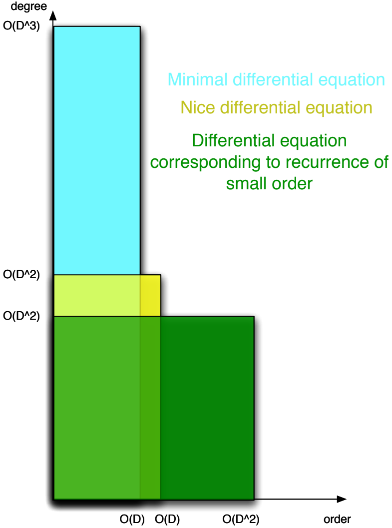
By induction, $f^{(\ell)} \in \mathrm{Vect}_{\mathbb{Q}(t)}\left(1, f, f^2, \ldots, f^{\deg_T(P)-1}\right)$, for all ℓ. $\square$

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

$$f \in \mathbb{Q}[[t]], \quad P(t, f(t)) = 0 \text{ with } \deg P = D$$

Question: sizes (order & coefficients degree) of differential equations for f?

Answer [B., Chyzak, Lecerf, Salvy, Schost, 2007]:

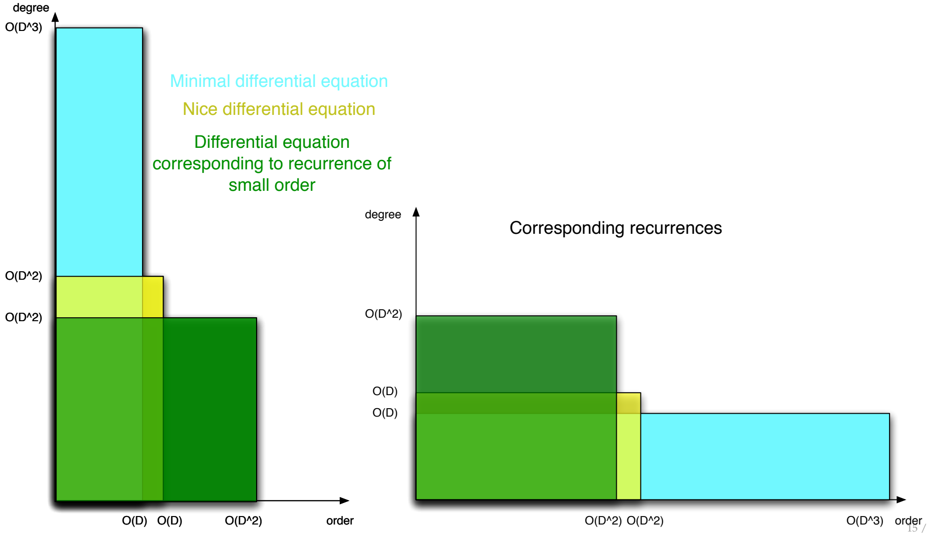


Bonus: sizes of differential equations for algebraic series

$$f \in \mathbb{Q}[[t]], \quad P(t, f(t)) = 0 \text{ with } \deg P = D$$

Question: sizes (order & coefficients degree) of differential equations for f?

Answer [B., Chyzak, Lecerf, Salvy, Schost, 2007]:

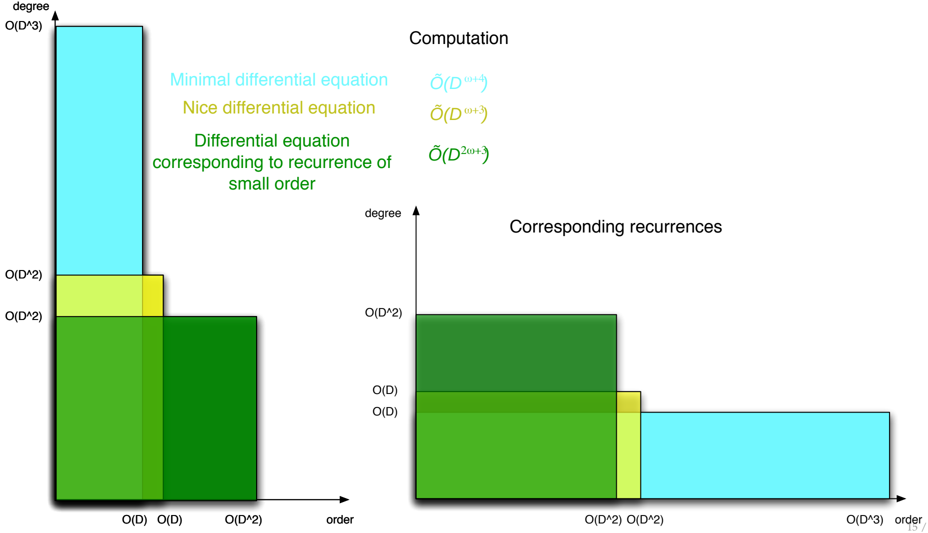


Bonus: sizes of differential equations for algebraic series

$$f \in \mathbb{Q}[[t]], \quad P(t, f(t)) = 0 \text{ with } \deg P = D$$

Question: sizes (order & coefficients degree) of differential equations for f?

Answer [B., Chyzak, Lecerf, Salvy, Schost, 2007]:

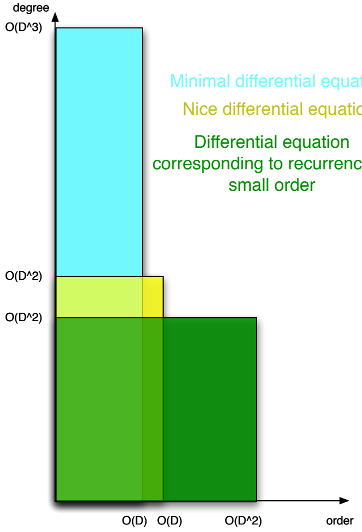


Bonus: sizes of differential equations for algebraic series

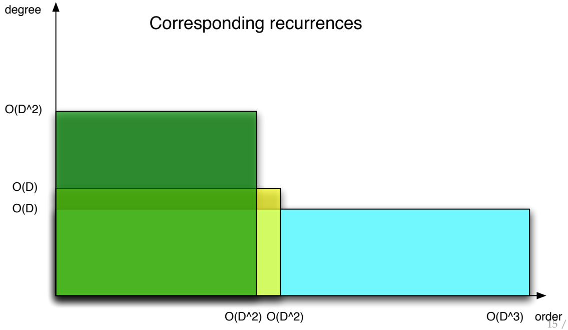
$$f \in \mathbb{Q}[[t]], \quad P(t, f(t)) = 0 \text{ with } \deg P = D$$

Question: sizes (order & coefficients degree) of differential equations for f?

Answer [B., Chyzak, Lecerf, Salvy, Schost, 2007]:



	Computation	Unrolling the recurrence
Minimal differential equation	$\tilde{O}(D^{\omega+4})$	$\tilde{O}(D^2 M(D) N)$
Nice differential equation	$\tilde{O}(D^{\omega+3})$	$\tilde{O}(D M(D) N)$
Differential equation corresponding to recurrence of small order	$\tilde{O}(D^{2\omega+3})$	$\tilde{O}(M(D^3) N)$



Pólya's theorem

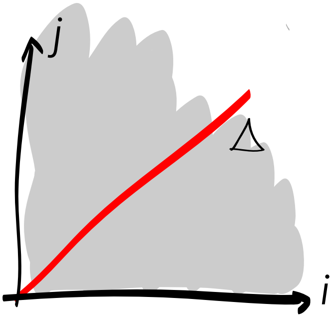
Definition

If F is a formal power series

$$F = \sum_{i_1,\dots,i_n \geq 0} a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

its diagonal is

$$\mathrm{Diag}(F) \stackrel{def}{=} \sum_i a_{i,\dots,i} t^i.$$



Theorem (Pólya, 1922)

Diagonals of bivariate rational functions are algebraic.

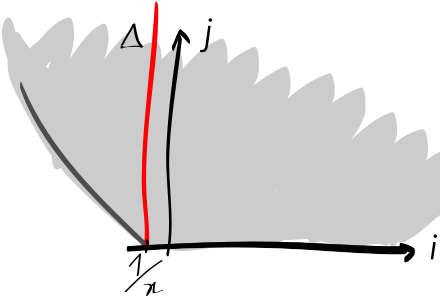
Definition

If F is a formal power series

$$F = \sum_{i_1,\dots,i_n \geq 0} a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

its diagonal is

$$\mathrm{Diag}(F) \stackrel{def}{=} \sum_i a_{i,\dots,i} t^i.$$



Theorem (Pólya, 1922)

Diagonals of bivariate rational functions are algebraic.

Proof:

$$\mathrm{Diag}\,(F) = [x^{-1}] \frac{1}{x} F\left(x, \frac{t}{x}\right) = \frac{1}{2\pi i} \oint_{|x|=\epsilon} F\left(x, \frac{t}{x}\right) \frac{dx}{x}$$

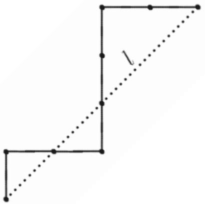
and evaluating the integral by residues concludes (residues are algebraic!)

Example: Dyck walks

$$\mathfrak{S} = \{(1,1),(1,-1)\}$$

Let B_n be the number of Dyck bridges (i.e. $\mathfrak{S}$-walks in $\mathbb{Z}^2$ starting at $(0,0)$ and ending on the horizontal axis), of length n

Rotating a Dyck bridge



counterclockwise by $\pi/4$

B_n = number of $\{(1,0),(0,1)\}$-walks in $\mathbb{Z}^2$ from $(0,0)$ to (n,n)

$$\Longrightarrow \qquad B(t) = \sum_{n\geq 0} B_n t^n = \operatorname{Diag}\left(\frac{1}{1-x-y}\right)$$

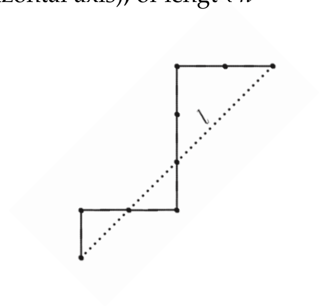
$$B(t) = \frac{1}{2\pi i}\oint_{|x|=\epsilon} \frac{dx}{x-x^2-t} = \left.\frac{1}{1-2x}\right|_{x=\frac{1-\sqrt{1-4t}}{2}} = \frac{1}{\sqrt{1-4t}}$$

Example: Dyck walks

$$\mathfrak{S} = \{(1,1),(1,-1)\}$$

Let B_n be the number of Dyck bridges (i.e. $\mathfrak{S}$-walks in $\mathbb{Z}^2$ starting at $(0,0)$ and ending on the horizontal axis), of length n

Rotating a Dyck bridge



counterclockwise by $\pi/4$

B_n = number of $\{(1,0),(0,1)\}$-walks in $\mathbb{Z}^2$ from $(0,0)$ to (n,n) $= \binom{2n}{n}$

$$\Longrightarrow \qquad B(t) = \sum_{n\geq 0} B_n t^n = \operatorname{Diag}\left(\frac{1}{1-x-y}\right)$$

$$B(t) = \frac{1}{2\pi i}\oint_{|x|=\epsilon} \frac{dx}{x-x^2-t} = \frac{1}{\sqrt{1-4t}} = \sum_{n\geq 0}\binom{2n}{n} t^n$$

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

If $F = \sum_i \frac{\gamma_i}{t - \beta_i}$, 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

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

Proof. By the elimination property, there exist $U, V \in \mathbb{Q}[x, t]$ such that

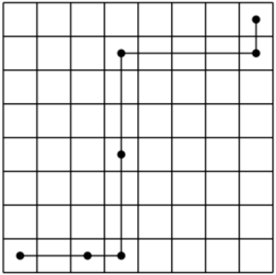
$$R(x) = U(x,t)B(t) + V(x,t)\big(A(t) - xB'(t)\big).$$

Evaluating at $(t, x) = (\beta_i, \gamma_i)$ yields $R(\gamma_i) = 0$. □

▷ This resultant is useful for symbolic integration of rational functions.
▷ [Bronstein 1992] generalized this result to multiple poles.

Example: 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, ...

Example: diagonal Rook paths

Generating function of the sequence

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

is

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

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

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

$$t^2(1-t)(2y-1)(36ty^2 - 4y^2 + 1 - t)$$

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

The Pólya-Furstenberg theorem

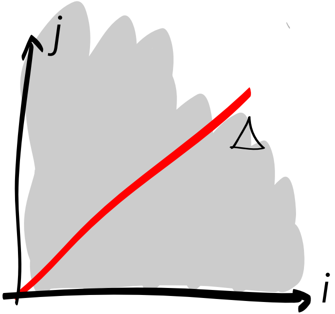
Definition

If F is a formal power series

$$F = \sum_{i_1,\dots,i_n \geq 0} a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

its diagonal is

$$\mathrm{Diag}(F) \stackrel{def}{=} \sum_i a_{i,\dots,i} t^i.$$



Theorem ([Pólya, 1922], [Furstenberg, 1967])

Diagonals of bivariate rational functions are algebraic and the converse is also true

▷ Key point If $f(0) = 0$ and $P \in \mathbb{Z}[x,y]$ with $P(t, f(t)) = 0$, $P_y(0,0) \neq 0$, then

$$f(t) = \mathrm{Diag}\left(y^2 \frac{P_y(xy,y)}{P(xy,y)}\right)$$

The Pólya-Furstenberg theorem

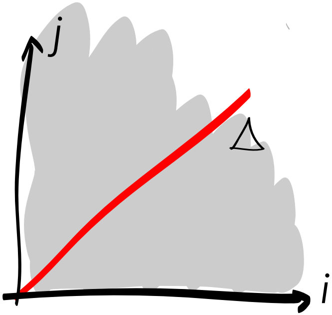
Definition

If F is a formal power series

$$F = \sum_{i_1,\dots,i_n \geq 0} a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

its diagonal is

$$\mathrm{Diag}(F) \stackrel{def}{=} \sum_i a_{i,\dots,i} t^i.$$



Theorem ([Pólya, 1922], [Furstenberg, 1967])

Diagonals of bivariate rational functions are algebraic and the converse is also true

▷ This is false for more than 2 variables. E.g.

$$\mathrm{Diag}\left(\frac{1}{1-x-y-z}\right) = \sum_{n\geq 0} \binom{3n}{n,n,n} t^n = {}_2F_1\left(\left.\begin{matrix}\frac{1}{3} & \frac{2}{3} \\ & 1\end{matrix}\right| 27t\right) \quad \text{is transcendental}$$

The Pólya-Furstenberg theorem

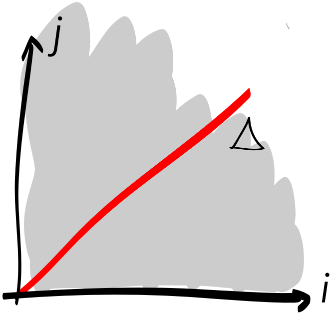
Definition

If F is a formal power series

$$F = \sum_{i_1,\dots,i_n \geq 0} a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

its diagonal is

$$\mathrm{Diag}(F) \stackrel{def}{=} \sum_i a_{i,\dots,i} t^i.$$



Theorem ([Pólya, 1922], [Furstenberg, 1967])

Diagonals of bivariate rational functions are algebraic and thus D-finite

- ▷ Algebraic equation has exponential size [B., Dumont, Salvy, 2015]
- ▷ Differential equation has polynomial size [B., Chen, Chyzak, Li, 2010]

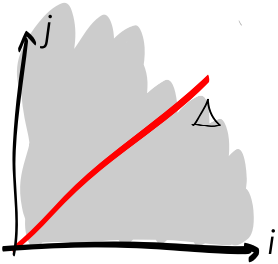
Definition

If F is a formal power series

$$F = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

its diagonal is

$$\mathrm{Diag}(F) \stackrel{def}{=} \sum_i a_{i,\ldots,i} t^i.$$



Theorem ([Lipshitz, 1988])

Diagonals of multivariate rational functions are D-finite.

Example: Diagonal Rook paths on a 3D chessboard

Question [Erickson, 2010]
How many ways can a Rook move from $(0,0,0)$ to (N,N,N), where each step is a positive integer multiple of $(1,0,0)$, $(0,1,0)$, or $(0,0,1)$?

$$1, 6, 222, 9918, 486924, 25267236, 1359631776, 75059524392, \ldots$$

Answer [B., Chyzak, van Hoeij, Pech, 2011]: GF of 3D diagonal Rook paths is

$$G(t) = 1 + 6 \cdot \int_0^t \frac{{}_2F_1\left(\begin{matrix} 1/3 & 2/3 \\ & 2 \end{matrix} \,\middle|\, \frac{27x(2-3x)}{(1-4x)^3}\right)}{(1-4x)(1-64x)}\, dx$$

It is a transcendental power series.

▷ More examples of this type $\longrightarrow$ Friday

Thanks for your attention!