MPRI C-2-22 — Lecture 3

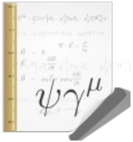
Differentially Finite Power Series

Marc Mezzarobba

October 14, 2024

Another M2 internship

- Long-term goal: Automatic implementation of special functions



compiler $\longrightarrow$

$$\begin{cases} p_r f^{(r)} + \cdots + p_0 f = 0 \\ f(0), \ldots, f^{(r-1)} \end{cases}$$

$[a, b] \subseteq \mathbb{R}$

$\varepsilon > 0$

```
double fun(double x);
```

$\forall x \in [a, b] \cap \texttt{double},$

$$\left| \frac{\texttt{fun}(x) - f(x)}{f(x)} \right| \leqslant \varepsilon$$

- This project: Bessel functions
- Floating-point arithmetic + symbolic computation + programming
- Talk to me if interested

Exercises from last week

Exercise 1

Let $T(n)$ be the complexity of multiplication of $n \times n$ lower triangular matrices with entries in $\mathbb{K}$. Show that one can multiply arbitrary $n \times n$ matrices in $\mathcal{M}_n(\mathbb{K})$ using $O(T(n))$ arithmetic operations in $\mathbb{K}$.

Solution.

For $n = 3\,k$:

- $n \times n$ matrices can be multiplied using $O(1)$ multiplications of blocks of size $k \times k$
- $k \times k$ matrices can be multiplied in $T(n)$ ops using the formula

$$\begin{pmatrix} \cdot & & \\ \cdot & \cdot & \\ \cdot & A & \cdot \end{pmatrix} \begin{pmatrix} \cdot & & \\ B & \cdot & \\ \cdot & \cdot & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & & \\ \cdot & \cdot & \\ A\,B & \cdot & \cdot \end{pmatrix}.$$

General case ($n \geqslant 12$): embed the $n \times n$ matrix product in a product of matrices of size $4\,\lceil n/4 \rceil$, reducing to 4^3 products in size $\lceil n/4 \rceil \leqslant n/3$.

Exercise 2

Let θ be a feasible exponent for matrix multiplication in $\mathbb{K}^{n\times n}$,
and $P \in \mathbb{K}[x]$ with $\deg P < n$.

a) Find an algorithm for the simultaneous evaluation of P at $\lceil \sqrt{n} \rceil$ elements of $\mathbb{K}$ using $O(n^{\theta/2})$ operations in $\mathbb{K}$.

b) If Q is another polynomial in $\mathbb{K}[x]$ of degree $< n$, show how to compute the first n coefficients of $P \circ Q := P(Q(x))$ using $O(n^{(\theta+1)/2})$ operations in $\mathbb{K}$.

Hint: Write $P(x)$ as $\sum_i P_i(x)\,(x^d)^i$ where d is well chosen and the P_i have degree $< d$.

Exercise 2 – Solution

a) Set $d = \lceil \sqrt{n} \rceil$ and $P(x) = P_0(x) + P_1(x) \cdot x^d + \cdots + P_{d-1}(x)\, x^{d(d-1)}$
$= p_0 + p_1 x + \cdots + p_{d^2-1} x^{d^2-1}$ (with $p_k = 0$ for $k \geqslant n$).

Then

$$\begin{pmatrix} p_0 & \cdots & p_{d-1} \\ p_d & & p_{2d-2} \\ \vdots & & \\ p_{(d-1)d} & \cdots & p_{d^2-1} \end{pmatrix} \begin{pmatrix} 1 & \cdots & 1 \\ a_0 & & a_{d-1} \\ \vdots & & \vdots \\ a_0^{d-1} & \cdots & a_{d-1}^{d-1} \end{pmatrix} = \begin{pmatrix} P_0(a_0) & \cdots & P_0(a_{d-1}) \\ P_1(a_0) & & P_1(a_{d-1}) \\ \vdots & & \vdots \\ P_{d-1}(a_0) & \cdots & P_{d-1}(a_{d-1}) \end{pmatrix}.$$

Algorithm:

- Compute the a_j^i and a_j^{di} for $0 \leqslant i, j < d$ — $O(d^2)$ ops
- Perform the matrix product — $O(d^\theta)$ ops
- Recover $P(a_j)$ from the $P_i(a_j)$ for $0 \leqslant j < d$ — $O(d^2)$ ops

Total $O(d^\theta) = O(n^{\theta/2})$, vs. $O(n^{3/2})$ naively.

(Next lecture: $O(M(n))$ for n evaluation points.)

Exercice 2 — Wait: why?

Let θ be a feasible exponent for matrix mult. in $\mathbb{K}^{n\times n}$, and $P \in \mathbb{K}[x]$ with $\deg P < n$.

b) If Q is another polynomial in $\mathbb{K}[x]$ of degree $< n$, show how to compute the first n coefficients of $P \circ Q := P(Q(x))$ using $O(n^{(\theta+1)/2})$ operations in $\mathbb{K}$.

Preliminary questions:

- How fast can we compute $P \circ Q$ in full (semi-naively)? $O(n\,M(n^2))$
- Is there any hope of doing better? $\text{size} = \Omega(n^2)$
- Why are we interested in the first n coefficients?

$$e.g., \quad \left.\begin{aligned} f(x) &= a_0 + a_1 x + \cdots + O(x^n) \\ g(x) &= b_1 x + b_2 x^2 + \cdots + O(x^n) \end{aligned}\right\} \Longrightarrow f(g(x)) = c_0 + c_1 x + \cdots + O(x^n)$$

- How fast can we compute them (semi-naively)? $O(n \cdot M(n))$

Exercise 2 – Solution

b) Write $P = P_0 + P_1 x^d + \cdots + P_{d-1} x^{d-1}$ as before, so that

$$\begin{aligned} P \circ Q &= P_0 \circ Q + (P_1 \circ Q) \cdot Q^d + \cdots + (P_{d-1} \circ Q) \cdot Q^{d(d-1)} \\ &= \quad (p_0 + p_1 \quad Q + \cdots + p \quad {}_{d-1} Q^{d-1}) \\ &\quad + (p_d + p_{d+1} Q + \cdots + p_{2d-1} Q^{d-1}) \quad Q^d \\ &\quad + \cdots \\ &\quad + (p_{(d-1)d} + p_{\square} Q + \cdots + p_{d^2-1} Q^{d-1}) \quad Q^{d(d-1)}. \end{aligned}$$

- First n coefficients in all cofactors of $Q^{d \cdot i}$ simultaneously:

$$\begin{pmatrix} P_0 \circ Q \\ \vdots \\ P_{d-1} \circ Q \end{pmatrix} \bmod x^n = \underbrace{\begin{pmatrix} p_0 & \cdots & p_{d-1} \\ \vdots & & \vdots \\ p_{(d-1)d} & \cdots & p_{d^2-1} \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & 0 \\ [Q]_0 & [Q]_1 & & [Q]_{n-1} \\ \vdots & \vdots & & \vdots \\ [Q^{d-1}]_0 & [Q^{d-1}]_1 & \cdots & [Q^{d-1}]_{n-1} \end{pmatrix}}_{d \times d \text{ by } d \times n \text{, cost } O(\frac{n}{d} d^\theta) = O(n^{(\theta+1)/2})} \begin{pmatrix} 1 \\ x \\ \vdots \\ x^{n-1} \end{pmatrix}.$$

- Powers of Q and $Q^d \bmod x^n$, final recombination: $O(d\, M(n)) = O(n^{3/2})$ ops.

Teaser: Fast composition (Lecture 6)

Power Series Composition in Near-Linear Time

Yasunori Kinoshita * Baitian Li †

Abstract

We present an algebraic algorithm that computes the composition of two power series in softly linear time complexity. The previous best algorithms are $\mathrm{O}(n^{1+o(1)})$ non-algebraic algorithm by Kedlaya and Umans (FOCS 2008) and an $\mathrm{O}(n^{1.43})$ algebraic algorithm by Neiger, Salvy, Schost and Villard (JACM 2023).

Our algorithm builds upon the recent Graeffe iteration approach to manipulate rational power series introduced by Bostan and Mori (SOSA 2021).

1 Introduction

Let $\mathbb{A}$ be a commutative ring and let $f(x), g(x)$ be polynomials in $\mathbb{A}[x]$ of degrees less than m and n, respectively. The problem of *power series composition* is to compute the coefficients of $f(g(x)) \bmod x^n$. The terminology stems from the idea that $g(x)$ can be seen as a

0 Rational Series
C-Finite Sequences

Formal power series

Definition. The **ring of formal power series** in the variable x over the ring $\mathbb{A}$ is the set of formal objects of the form

$$\sum_{n=0}^{\infty} a_n x^n$$

equipped with the operations $+$ and $\times$ implied by the notation.

Notation: $f(x) = g(x) + O(x^\sigma)$ when the terms of order $< \sigma$ of f, g coincide.

Variants.

- Formal Laurent series $\mathbb{A}((x))$ — $\sum_{n=N_0}^{\infty} a_n x^n$ for some $N_0 \in \mathbb{Z}$

  Note: $\mathbb{A}((x))$ is a field when $\mathbb{A}$ is a field. Also note the difference with Laurent series in complex analysis.

- Formal Puiseux series $\mathbb{A}((x^{1/*}))$ — $\sum_{n=N_0}^{\infty} a_n x^{n/d}$ for some $d \in \mathbb{N} \setminus \{0\}$ and $N_0 \in \mathbb{Z}$

  Note: $\mathbb{A}((x^{1/*}))$ is an (algebraically closed) field if $\mathbb{A}$ is an (algebraically closed) field.

Rational series, recurrences with constant coefficients

Definition. A formal power (or Laurent) series over a field $\mathbb{K}$ is called **rational** when it is the series expansion at 0 of an element of $\mathbb{K}(x)$.

Example. $\dfrac{1}{1+x-x^2} = 1 + x + 2x^2 + 3x^3 + 5x^4 + \cdots$

Definition. A sequence $(u_n) \in \mathbb{K}^{\mathbb{N}}$ is called **C-finite** when it satifies a linear recurrence

$$\forall n \in \mathbb{N}, \quad 1\, u_{n+s} + c_{s-1} u_{n+s-1} + \cdots + c_0 u_n = 0 \qquad \text{with } c_i \in \mathbb{K}.$$

(Equivalently: for $n \geqslant$ some N.)

$s =$ **order** of the recurrence

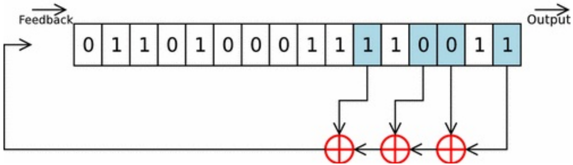
Example. $F_{n+2} = F_{n+1} + F_n$

Theorem. A power series is rational if and only if its coefficient sequence is C-finite.

By any other name…

Linear Feedback Shift Registers (LFSR)

Circuits, cryptography…

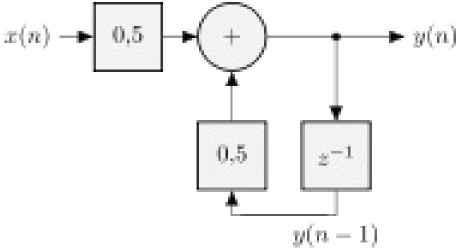


Matt Crypto, Wikimedia Commons, public domain

$$u_{n+16} = u_{n+5} + u_{n+3} + u_{n+2} + u_n \text{ (over } \mathbb{F}_2)$$

Infinite Impulse Response (IIR) filters

Signal processing, control



Przemekbary, Wikimedia Commons, cc-by-4.0-intl

$$y_n = 0.5\, y_{n-1} + x_n \text{ (over } \mathbb{R})$$

inhomogeneous

The characteristic polynomial of a recurrence

$$u_{n+s}+c_{s-1}u_{n+s-1}+\cdots+c_0u_n=0 \qquad \text{(Rec)}$$

Definition. The **characteristic polynomial** of the recurrence (Rec) is the polynomial

$$\chi(X)=X^s+c_{s-1}X^{s-1}+\cdots+c_0\,.$$

- Generating series: $\sum_{n=0}^{\infty} u_n x^n = \frac{p(x)}{1+c_{s-1}X+\cdots+c_0X^s}$ for some $p\in\mathbb{K}[x]$

  ($1+c_{s-1}X+\cdots+c_0X^s$ is called the **reciprocal polynomial** of χ.)

- Closed form solution: $u_n=\sum_{\chi(\alpha)=0} p_\alpha(n)\,\alpha^n$ where $p_\alpha\in\mathbb{K}[n]_{<\mathrm{mult}(\alpha,\chi)}$.

Algorithms

Proposition.

1. One can compute the **first N terms** of a rational series in $O(N)$ operations.
2. One can compute the **nth term** of a rational series in $O(\log n)$ operations.

Proof. Compute the associated recurrence and the first s terms by any means. Then

1. Set $u_s := -(c_{s-1}u_{s-1} + \cdots + c_0 u_0)$, then $u_{s+1} := -(c_{s-1}u_s + \cdots + c_0 u_1)$, etc.
2. Write the recurrence in matrix form:

$$\begin{pmatrix} u_{n+1} \\ u_{n+2} \\ \vdots \\ u_{n+s} \end{pmatrix} = \underbrace{\begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ -c_0 & -c_1 & \cdots & -c_{s-1} \end{pmatrix}}_{A} \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+s-1} \end{pmatrix}$$

Compute A^{n-s} by binary powering. Apply it to $(u_0, \ldots, u_{s-1})^T$. □

Faster algorithms for large s in Lecture 6.

An exercise for next time

Let $f(x) = (1 + x + x^2)^n \in \mathbb{Z}[x]$.

Give an algorithm that computes the parity of all coefficients of f in $O(M(n))$ **bit** operations.

1 Differentially Finite Series
P-Finite Sequences

Definition

$\mathbb{K}$ – effective field of characteristic zero

Definition. A power series $f \in \mathbb{K}[[x]]$ is **differentially finite** when the vector space

$$\operatorname{span}_{\mathbb{K}(x)}(f, f', f'', \dots) \subseteq \mathbb{K}((x))$$

generated by its iterated derivatives has finite dimension over $\mathbb{K}(x)$.

In other words: f satisfies a linear homogeneous differential equation

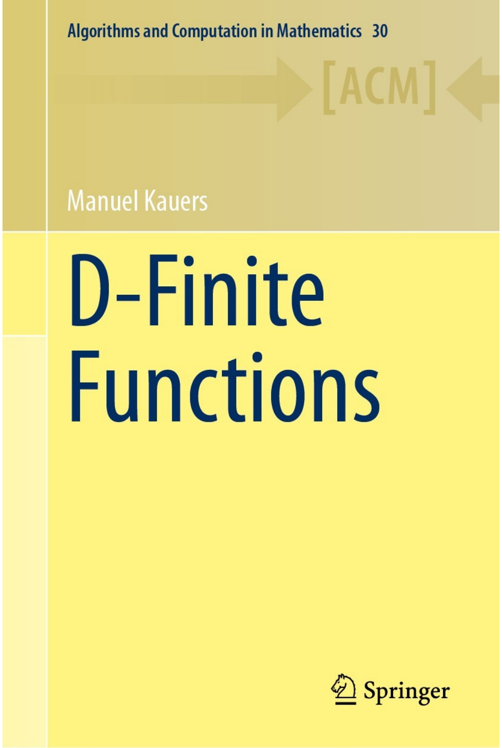
$$a_r(x)\, f^{(r)}(x) + \cdots + a_1(x)\, f'(x) + a_0(x)\, f(x) = 0 \qquad (a_r \neq 0)$$

with coefficients in $\mathbb{K}[x]$.

Differentially finite series are also called D-finite or holonomic.

Implementations

- Maple: `gfun`, `Mgfun`
- Mathematica: `HolonomicFunctions`, `Guess`, …
- SageMath: `ore_algebra`



Remark: Series vs. functions

Definition. For $U \subseteq \mathbb{C}$, a meromorphic function $f\colon U \to \mathbb{C}$ is called differentially finite when the vector space

$$\operatorname{span}_{\mathbb{C}(x)}(f, f', f'', \dots)$$

generated by its iterated derivatives has finite dimension over $\mathbb{C}(x)$.

Theorem ("Cauchy's theorem"). Suppose $a_r(0) \neq 0$ in the equation

$$a_r(x)\, f^{(r)}(x) + \cdots + a_1(x)\, f'(x) + a_0(x)\, f(x) = 0, \qquad a_0, \dots, a_r \in \mathbb{C}[x]. \qquad \text{(DiffEq)}$$

Then there exists a neighborhood $U \subseteq \mathbb{C}$ of 0 such that, for any $(v_0, \dots, v_{r-1}) \in \mathbb{C}^{r-1}$, (DiffEq) has a unique analytic solution with $f^{(i)}(0) = v_i$ for $i = 0, \dots, r-1$.

Proposition. A function that is analytic at 0 is D-finite if and only if its series expansion is D-finite.

Which of these series (functions) are D-finite?

- $f(x) = \exp(x) = 1 + x + 2\,x^2 + 6\,x^3 + \cdots$ — $f' - f = 0$ ✓
- $f(x) = x^2 + 5\,x^3 + x^{12}$ — $f^{(13)} = 0$ ✓
- $f(x) = \sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^4 + \cdots$ — $\dfrac{f'(x)}{f(x)} = \dfrac{1}{2\,(1+x)}$ ✓
- $f(x) = \tan(x) = 1 + \frac{1}{3}x^3 + \cdots$ — poles ✗
- $f(x) = \arctan(x) = 1 - \frac{1}{3}x^3 + \cdots$ — $(1+x^2)\,f'(x) = 1$ ✓
- $f(x) = \sum_{k=0}^{\infty} k!\,x^k$ — $x^2\,f''(x) + (3\,x - 1)\,f'(x) + f(x) = 0$... but see next slides ✓
- $f(x) = \sum_{k=0}^{\infty} 2^{k!}\,x^k$ — next slides ✗
- $f(x) = \dfrac{\sin(x) + \exp(x)^2}{\sqrt[5]{x^7+1}} = 1 + 3\,x + 2\,x^2 + \frac{7}{6}x^3 + \cdots$ — later ✓

P-finite sequences

Definition. A sequence $(u_n)_{n\in\mathbb{N}}$ is called **P-finite** (or **P-recursive**, or holonomic) if it satisfies a linear homogeneous recurrence relation

$$b_s(n)\,u_{n+s}+\cdots+b_1(n)\,u_{n+1}+b_0(n)\,u_n=0, \quad b_s\neq 0, \tag{Rec}$$

with coefficients in $\mathbb{K}[n]$.

Equivalently: when (Rec) holds for sufficiently large $n\in\mathbb{N}$.

Also, informally: when its shifts $(u_n)_{n\in\mathbb{N}}, (u_{n+1})_{n\in\mathbb{N}}, (u_{n+2})_{n\in\mathbb{N}}, \ldots$ generate a finite-dimensional vector space over $\mathbb{K}(n)$. (But some care is needed to make sense of this definition!)

Examples.

$n!$ $\qquad\qquad (n+1)!=(n+1)\,n!$

$C_n=\frac{1}{n+1}\binom{2n}{n}$ $\qquad\qquad (n+2)\,C_{n+1}=(4n+2)\,C_n$

$F_n=\frac{1}{\sqrt{5}}(\varphi^n-\tilde{\varphi}^n), \quad \varphi,\tilde{\varphi}=\frac{1\pm\sqrt{5}}{2}$ $\qquad\qquad F_{n+2}=F_n+F_{n+1}$

Differential equations and recurrences

Theorem. A power series is D-finite if and only if its coefficient sequence is P-finite.

($\Rightarrow$). Suppose $\sum_{i=0}^{r} a_i(x)\, f^{(i)}(x) = 0$. Substitute $a_i(x) = \sum_{i=0}^{d} a_{i,j}\, x^j$ and $f(x) = \sum_{n=0}^{\infty} f_n\, x^n$:

$$\sum_{i=0}^{r} \left(\sum_{j=0}^{d} a_{i,j}\, x^j \right) \left(\sum_{n=0}^{\infty} f_n\, n\,(n-1)\cdots(n-i)\, x^{n-i} \right) = 0,$$

$$\sum_{n=0}^{\infty} \sum_{i=0}^{r} \sum_{j=0}^{d} n\,(n-1)\cdots(n-i)\, a_{i,j}\, f_n\, x^{n-i+j} = 0,$$

$$\sum_{i=0}^{r} \sum_{j=0}^{d} \sum_{n'=-i+j}^{\infty} (n'+i-j)\,(n'+i-j-1)\cdots(n'-j)\, a_{i,j}\, f_{n'+i-j}\, x^{n'} = 0,$$

$$\sum_{n'=0}^{\infty} \left(\sum_{i=0}^{r} \sum_{j=0}^{d} (n'+i-j)\,(n'+i-j-1)\cdots(n'-j)\, a_{i,j}\, f_{n'+i-j} \right) x^{n'} = 0. \qquad \square$$

$(\Leftarrow)$. Suppose $\sum_{i=0}^{s} b_i(n)\, u_{n+i} = 0$ for all $n \in \mathbb{N}$. Extend (u_n) by setting $u_{n=0}$ for $n < 0$.

- By multiplying the relation with $n\,(n+1)\cdots(n+s-1)$, we can assume wlog

$$\forall n \in \mathbb{Z}, \quad \sum_{i=0}^{s} b_i(n)\, u_{n+i} = 0 \tag{RecZ}$$

- For any double-sided formal series $f(x) = \sum_{n\in\mathbb{Z}}^{\infty} f_n\, x^n$, one has

$$x^{-1} f(x) = \sum_{n\in\mathbb{Z}} f_{n+1}\, x^n, \qquad\qquad x\, f'(x) = \sum_{n\in\mathbb{Z}} n\, f_n\, x^n.$$

- Letting $\begin{cases} [X(f)](x) = x\, f(x), \\ [D(f)](x) = f'(x), \end{cases}$ we get from (RecZ) that

$$\sum_{i=0}^{s} b_i(X \circ D) \circ X^{-i}(f) = 0 \quad \text{where} \quad f(x) = \sum_{n\in\mathbb{Z}} u_n\, x^n.$$

□

Differential equations and recurrences: remarks

Theorem. A power series is D-finite if and only if its coefficient sequence is P-finite.

- The proof gives a conversion algorithm.
- Differential equation of $\left| \begin{array}{l} \text{order } \leqslant r \\ \text{degree } \leqslant d \end{array} \right.$ $\mapsto$ recurrence of $\left| \begin{array}{l} \text{order } \leqslant d + r \\ \text{degree } \leqslant r. \end{array} \right.$
- Also holds for $\begin{cases} \text{double-sided series } \sum_{n \in \mathbb{Z}} u_n z^n \\ \text{sequences } (u_n)_{n \in \mathbb{Z}}. \end{cases}$

Corollary. One can compute the first N terms of a D-finite series in $O(N)$ ops.

Lecture 14: nth term – but not in $O(\log n)$!

Equality tests

Proposition. Assume that $(u_n) \in \mathbb{K}^{\mathbb{N}}$ and $(v_n) \in \mathbb{K}^n$ both satisfy

$$b_s(n)\, y_{n+s} + \cdots + b_1(n)\, y_{n+1} + b_0(n)\, y_n = 0 \qquad (b_s \neq 0)$$

and $u_n = v_n$ for $n \leqslant \ell + s$ where $\ell = \max(0,$ largest integer root of $b_s)$. Then $u = v$.

Corollary. If $f, g \in \mathbb{K}[[x]]$ satisfy the same differential equation

$$a_r(x)\, y^{(r)}(x) + \cdots + a_1(x)\, y'(x) + a_0(x)\, y(x) = 0 \qquad (a_i \in \mathbb{K}[x])$$

one can test if $f = g$.

$\{(\mathrm{Rec}), u_0, \ldots, u_{\ell+s}\}$ = finite data structure for representing (u_n)

$\{(\mathrm{DiffEq}), f(0), f'(0), \ldots, f^{(\ell+s)}(0)\}$ = finite data structure for representing f

Inequalities

POSITIVITY CERTIFICATES FOR LINEAR RECURRENCES

ALAA IBRAHIM AND BRUNO SALVY

Abstract. We show that for solutions of linear recurrences with polynomial coefficients of Poincaré type and with a unique simple dominant eigenvalue, positivity reduces to deciding the genericity of initial conditions in a precisely defined way. We give an algorithm that produces a certificate of positivity that is a data-structure for a proof by induction. This induction works by showing that an explicitly computed cone is contracted by the iteration of the recurrence.

1. Introduction

A sequence $(u_n)_{n\in\mathbb{N}}$ of real numbers is called *P-finite* if it satisfies a linear recurrence

$$p_d(n)u_{n+d} = p_{d-1}(n)u_{n+d-1} + \cdots + p_0(n)u_n, \qquad n \in \mathbb{N}, \tag{1}$$

with coefficients $p_i \in \mathbb{R}[n]$ ([1]). When the coefficients p_i are constants in $\mathbb{R}$, the

2 D-finite closure properties

Common equations, closure by sum

Proposition. If $f, g \in \mathbb{K}[[x]]$ are D-finite, one can find a differential equation

$$a_r(x)\, y^{(r)}(x) + \cdots + a_1(x)\, y'(x) + a_0(x)\, y(x) = 0 \qquad (a_i \in \mathbb{K}[x])$$

satisfied by both f and g.

Corollary 1. One can test the equality of D-finite sequences.

Corollary 2. If $f, g \in \mathbb{K}[[x]]$ are D-finite, then $f + g$ is D-finite.

Similarly,

- One can find a common recurrence satisfied by two given P-finite sequences,
- The sum of two P-finite sequences is P-finite.

Closure by sum: direct proof

Corollary. If $f, g \in \mathbb{K}[[x]]$ are D-finite, then $f + g$ is D-finite.

Proof. Write $V_\varphi = \mathrm{span}_{\mathbb{K}(x)}(\varphi^{(i)})_{i \in \mathbb{N}}$.

Since $(f+g)' = f' + g'$, one has

$$V_{f+g} \subseteq V_f + V_g,$$

hence

$$\dim(V_{f+g}) \leqslant \dim(V_f) + \dim(V_g) < \infty. \qquad \square$$

Showing that something is D-finite / P-finite / (other analogous properties…)

$\Leftrightarrow$ Imprisoning its derivatives / shifts / (…) in finite dimension

Closure by sum: algorithm

Suppose $\begin{cases} a_r(x)\, f^{(r)}(x) + \cdots + a_1(x)\, f'(x) + a_0(x)\, f(x) = 0, \\ b_s(x)\, g^{(s)}(x) + \cdots + b_1(x)\, g'(x) + b_0(x)\, g(x) = 0. \end{cases}$

We are looking for an equation $c_t(x)\, y^{(t)}(x) + \cdots + c_0(x)\, y(x) = 0$ satisfied by both f and g.

Using the equations, we can rewrite any pair $(f^{(i)}, g^{(i)})$ on a finite basis $(f, 0), (f', 0), \dots,$ $(0, g), (0, g'), \dots$. Doing so, we set up a linear system:

$$\begin{array}{r} \\ (f, 0) \\ \vdots \\ (f^{(r-1)}, 0) \\ (0, g) \\ (0, g^{(s-1)}) \end{array} \begin{array}{c} (f, g) \qquad \dots \qquad (f^{(t)}, g^{(t)}) \\ \begin{pmatrix} 1 & & & \square & \square & \square \\ & 1 & & \square & \square & \square \\ & & 1 & \square & \square & \square \\ 1 & & \square & \square & \square & \square \\ & 1 & \square & \square & \square & \square \end{pmatrix} \end{array} \begin{pmatrix} c_0 \\ \\ \vdots \\ \\ c_t \end{pmatrix} = 0$$

As soon as $t + 1 > r + s$, this system has a nonzero solution $(c_0, \dots, c_t) \in \mathbb{K}(x)^{t+1}$.

Remark. $f + g$ satisfies a differential equation of order $\leqslant r + s$

Closure by product

Proposition.

- If $f, g \in \mathbb{K}[[x]]$ are D-finite, then $f\,g$ is D-finite.
- If $u, v \in \mathbb{K}^{\mathbb{N}}$ are P-recursive, then $u\,v$ is P-finite.

Corollary: If $f, g \in \mathbb{K}[[x]]$ are D-finite, their **Hadamard product** $f \odot g = \sum_{n=0}^{\infty} f_n\, g_n\, x^n$ too.

Proof. Again by linear algebra: if $\begin{cases} V_f \text{ is generated by } f, \dots, f^{(r-1)}, \\ V_g \text{ is generated by } g, \dots, g^{(s-1)}, \end{cases}$

then
$$\forall k \in \mathbb{N}, \quad (f\,g)^{(k)} \in \operatorname{span}_{\mathbb{K}(x)}\left(f^{(i)}\, g^{(j)}\right)_{\substack{0 \leqslant i \leqslant r-1 \\ 0 \leqslant j \leqslant s-1}}.$$
□

Remark. $f\,g$ satisfies a differential equation of order $\leqslant r\,s$.

Exercise. Give a better order bound in the case of f^2. (Answer: $r\,(r+1)/2$.)

Algebraic series

Definition. A series $f \in \mathbb{K}[[x]]$ is called **algebraic** if there exists $P \in \mathbb{K}[x,y] \setminus \{0\}$ such that

$$P(x, f(x)) = 0.$$

Examples.

- rational series, $\sqrt[3]{1+x}$
- generating series of non-ambiguous context-free languages are algebraic

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

More generally:
If $f \in \mathbb{K}[[x]]$ is D-finite and $g \in x\,\mathbb{K}[x]$ is algebraic, then $f \circ g$ is D-finite. (similar proof)

Algebraic series are D-finite: proof

Wlog, suppose $P(x, f(x)) = 0$ with $P \in \mathbb{K}(x)[y]$ irreducible of degree d.

$$\text{We have} \qquad \underbrace{\frac{\partial}{\partial x}\Big(P(x, f(x))\Big)}_{=0} = P_x\big(x, f(x)\big) + \underbrace{P_y\big(x, f(x)\big)}_{\neq 0} f'(x).$$

$$\begin{aligned}
\text{Hence} \qquad f'(x) &= -\frac{P_x\big(x, f(x)\big)}{P_y\big(x, f(x)\big)} \\
&= -Q\big(x, f(x)\big)\, P_x\big(x, f(x)\big) && \text{where} \quad Q = \frac{1}{P_y} \bmod P \\
&= R\big(x, f(x)\big) && R \in \mathbb{K}(x)[y].
\end{aligned}$$

$$\begin{aligned}
\text{Then} \qquad f''(x) &= R_x\big(x, f(x)\big) + R_y\big(x, f(x)\big)\, f'(x) \\
&= \mathrm{poly}\big(x, f(x)\big), && \text{and so on by induction.}
\end{aligned}$$

Since $P\big(x, y(x)\big) = 0$ any $\mathrm{poly}\big(x, f(x)\big)$ belongs to $\mathrm{span}_{\mathbb{K}(x)}\{1, f, f^2, \ldots, f^{d-1}\}$.

So $\dim_{\mathbb{K}(x)}(f, f', f'', \ldots) \leqslant d$.

Hypergeometric sequences and series

Definition.

- A sequence $(u_n)_{n\in\mathbb{N}}$ is **hypergeometric** if it satisfies a first-order recurrence relation with polynomial coefficients.

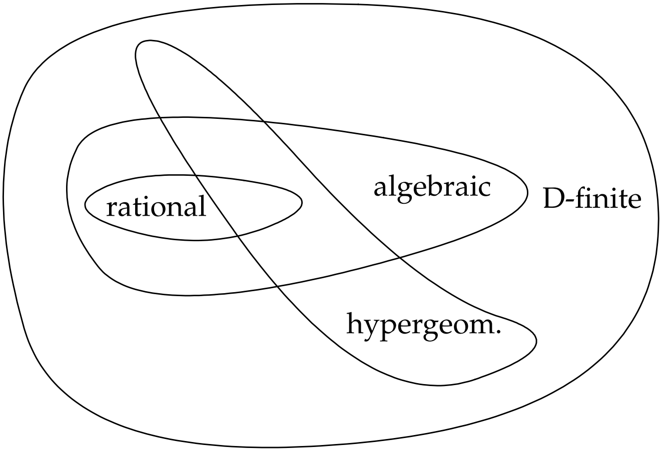
  In other words: if $\frac{u_{n+1}}{u_n} \in \mathbb{K}(n)$ [coincides with a rat. function for large enough n].

- A **generalized hypergeometric series** is a power series whose coefficient sequence is hypergeometric. Notation:

$$ {}_pF_q\left(\begin{matrix} a_1, \ldots, a_p \\ b_1, \ldots, b_q \end{matrix} \,\middle|\, x \right) = \sum_{n=0}^{\infty} u_n x^n \quad \text{where} \quad u_{n+1} = \frac{\prod_i (n+a_i)}{(n+1)\prod_j (n+b_j)} u_n, \quad u_0 = 1. $$

- $(1-x)^a = {}_1F_0(-a;;x)$, $\ln(1+x) = x\,{}_2F_1(1,1;2;-x)$, $\mathrm{Li}_2(x) = x\,{}_3F_2(1,1,1;2,2;x)$, etc.
- Many identities, e.g., ${}_2F_1(2\,a, 2\,b; a+b+\frac{1}{2}; x) = {}_2F_1(a, b; a+b+\frac{1}{2}; 4\,x\,(1-x))$ (Kummer)

Classes of power series



Summary

Theorem.

- D-finite series form an effective subring of $(\mathbb{K}[[x]], +, \times)$.
- P-finite sequences form an effective subring of $(\mathbb{K}^{\mathbb{N}}, +, \times)$.

This means that we can prove identities involving

- series like $\exp(x)$, $\ln(1+x)$, $\sqrt{1+x}$, ${}_pF_q\left(\begin{matrix} a_1, \dots, a_p \\ b_1, \dots, b_q \end{matrix} \middle| x\right)$ (and many more),
- sequences like Fibonacci's, Catalan's (and many more)

by computing in these rings.

3 Proof of identities

Automatic proof of identities

Problem. Prove that $\sin(x)^2+\cos(x)^2=1$.

Solution 1. Write $s(x)=\sin(x)$. We have $s''+s=0$.

$$\begin{aligned} z &= s^2 & \\ z' &= 2\,s\,s' & ✗ \\ z'' &= [2\,s\,s']' = 2\,(s')^2 + 2\,s\,s'' = 2\,(s')^2 - 2\,s^2 & ✗ \\ z''' &= [2\,(s')^2 - 2\,s^2]' = 4\,s'\,s'' - 4\,s\,s' = -8\,s\,s' & z''' + 4\,z' = 0 \end{aligned}$$

Same for $s(x)=\cos(x)$. Hence $y(x)=\sin(x)^2+\cos(x)^2$ satisfies $y'''+4\,y'=0$.

Now $f(x)=1$ satisfies the same equation.

The initial conditions $y(0)=1, \quad y'(0)=0, \quad y''(0)=0$ agree.

Since the leading coefficient does not vanish, this implies $y=f$.

Lazy proof of identities

Solution 2. Without even computing the equations, we know that

- any $(s^2)^{(k)}$ belongs to $\mathrm{span}_{\mathbb{Q}}\{s^2, s\,s', (s')^2\}$,

  so $\sin(x)^2$ must satisfy an ODE of order $\leqslant 3$, with constant coefficients,
- $\cos(x)^2$ must satisfy the same equation,
- $\sin(x)^2 + \cos(x)^2 - 1$ must satisfy an ODE of order $\leqslant 4$.

Since this equation has constant coefficients, in particular, it is nonsingular.

So it is enough to check that $\sin(x)^2 + \cos(x)^2 - 1 = O(x^4)$.

Remark: Minimal annihilators

We found an equation of non-minimal order!

Definition. The **minimal annihilator** of a D-finite function f is the equation

$$f^{(r)}(x) + \cdots + a_1(x)\, f'(x) + a_0(x)\, f(x) = 0, \qquad a_i \in \mathbb{K}(x)$$

of minimal order with leading coefficient $= 1$.

MATHEMATICS OF COMPUTATION
Volume 93, Number 347, May 2024, Pages 1427–1472
https://doi.org/10.1090/mcom/3912
Article electronically published on October 23, 2023

MINIMIZATION OF DIFFERENTIAL EQUATIONS AND ALGEBRAIC VALUES OF E-FUNCTIONS

ALIN BOSTAN, TANGUY RIVOAL, AND BRUNO SALVY

Abstract. A power series being given as the solution of a linear differential equation with appropriate initial conditions, minimization consists in finding a non-trivial linear differential equation of minimal order having this power series as a solution. This problem exists in both homogeneous and inhomogeneous variants; it is distinct from, but related to, the classical problem of factorization of differential operators. Recently, minimization has found ap-

Proof of identities: another example

$$F_{n+2} = F_n + F_{n+1}, \quad F_0 = 0, \quad F_1 = 1, \qquad u_n = F_{n+2}F_n - F_{n+1}^2$$

Any homog. poly. of degree 2 in $F_n, F_{n+1}, \ldots$ belongs to $\mathrm{span}_{\mathbb{Q}}(F_n^2, F_n F_{n+1}, F_{n+1}^2)$.

We know that the sequences $(u_n), \ldots, (u_{n+3})$ must satisfy a linear relation over $\mathbb{Q}$.

$$\begin{aligned}
u_n &= F_{n+2}F_n - F_{n+1}^2 \\
&= F_n^2 + F_n F_{n+1} - F_{n+1}^2 \\
u_{n+1} &= F_{n+1}^2 + F_{n+1}F_{n+2} - F_{n+2}^2 \\
&= F_{n+1}^2 + F_{n+1}(F_n + F_{n+1}) - (F_n + F_{n+1})^2 \\
&= -F_n^2 - F_n F_{n+1} + F_{n+1}^2
\end{aligned}$$

It turns out that $u_{n+1} = -u_n$.

Since $u_0 = F_0^2 + F_0 F_1 - F_1^2 = -1$, we conclude that $u_n = (-1)^{n+1}$ for all n.

An exercise for next week

Prove the following identity of formal power series:

$$\arcsin(x)^2 = \sum_{k=0}^{\infty} \frac{k!}{\frac{1}{2}\frac{3}{2}\cdots\left(k+\frac{1}{2}\right)} \frac{x^{2k+2}}{2k+2}.$$

For this:

1. Check that $y(x) = \arcsin(x)$ is solution to $(1 - x^2)\, y''(x) = x\, y'(x)$.
2. Deduce a linear differential equation satified by $z(x) = y(x)^2$.
3. Deduce a linear recurrence relation satisfied by the coefficients of the series.
4. Conclude.

4 Guessing

A riddle

What is the next term in this sequence?

$$1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511, 41835, 113634, 310572, 853467, \ldots$$

Is it generated by a "small" differential equation / recurrence?

```
sage: from ore_algebra import OreAlgebra, guess
sage: guess([1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798,
....:        15511, 41835, 113634, 310572, 853467],
....:       OreAlgebra(PolynomialRing(ZZ, 'n'), 'Sn'))
(-n - 4)*Sn^2 + (2*n + 5)*Sn + 3*n + 3
```

$$\ldots, 2356779, 6536382, 18199284, 50852019, 142547559, 400763223, 1129760415, \ldots$$

(Motzkin numbers)

Guessing linear equations: principle

$$1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511, 41835, 113634, 310572, 853467, \ldots$$

Ansatz:

$$(\mathbf{b}_{2,1}\, n + \mathbf{b}_{2,0})\, u_{n+2} + (\mathbf{b}_{1,1}\, n + \mathbf{b}_{1,0})\, u_{n+1} + (\mathbf{b}_{0,1}\, n + \mathbf{b}_{0,0})\, u_n = 0$$

Solution by linear algebra:

$$\begin{matrix} n=0 \\ n=1 \\ n=2 \\ n=3 \\ n=4 \\ n=5 \end{matrix} \quad \begin{pmatrix} 1 & 0 & 1 & 0 & 2 & 0 \\ 1 & 1 & 2 & 2 & 4 & 4 \\ 2 & 4 & 4 & 8 & 9 & 18 \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{pmatrix} \begin{pmatrix} \mathbf{b}_{0,0} \\ \mathbf{b}_{0,1} \\ \mathbf{b}_{1,0} \\ \mathbf{b}_{1,1} \\ \mathbf{b}_{2,0} \\ \mathbf{b}_{2,1} \end{pmatrix} = 0$$

- #equations $\geqslant$ #variables $\Rightarrow$ generically no solution
- Repeat for various (order, degree) compatible with available #terms
- Naïve complexity: $(\#\text{terms})^\theta$

Hermite-Padé approximation

Hermite-Padé approximation problem.

Given k power series $f_1, \dots, f_k \in \mathbb{K}[[x]]$,
k degree bounds $d_1, \dots, d_k$,
an approximation order σ,

find polynomials $p_1, \dots, p_k \in \mathbb{K}[x]$ such that $\deg p_i < d_i$ and

$$p_1(x)\, f_1(x) + \cdots + p_k(x)\, f_k(x) = O(x^\sigma).$$

When σ is chosen “just right” ($\sigma = d_1 + \cdots + d_k - 1$), the tuple $(p_1, \dots, p_k)$ is called a **Hermite-Padé approximant** of type $(d_1 - 1, \dots, d_k - 1)$ of f.

Naïve algorithm: $O(\sigma^\theta)$ ops

Fast algorithm: $O(k^\theta\, M(\sigma) \log \sigma)$, lecture 9
[Beckermann-Labahn 1994]

Guessing using Hermite-Padé approximation

- To guess a differential equation for the generating series $\sum_i f_i x^i$, compute Hermite-Padé approximants $(a_0, \ldots, a_r)$ of $(f, f', \ldots, f^{(r)})$ for various (r, d)
- To guess an algebraic equation for $\sum_i f_i x^i$, compute Hermite-Padé approximants of $(1, f, f^2, \ldots, f^k)$
- To guess a recurrence for $(f_i)_i$, proceed as above and convert
- Extensively used in enumerative combinatorics (Lecture 16)

Remark. Order and degree **bounds** make guessing into a rigorous algorithm.

For instance, **given a bound on its degree**, one can compute the minimal annihilator of a D-finite series using Hermite-Padé approximation.

5 Bonus

Differential operators as skew polynomials

Algebraic framework for working with differential operators $f \mapsto (x \mapsto \sum_i a_i(x)\, f^{(i)}(x))$

Definition.

$$\mathbb{K}(x)\langle D\rangle = \left\{ \sum_{i=0}^{r} a_i(x)\, D^i \;\middle|\; \begin{array}{l} r \in \mathbb{N}, \\ a_i \in \mathbb{K}(x) \end{array} \right\}$$

with the usual addition of polynomials,
multiplication defined by $D \cdot x = x \cdot D + 1$ and linearity.

Alt.: $A/(A\,\langle D\,x - 1\rangle\, A)$ where $A =$ ring of noncommutative polynomials in D over $\mathbb{K}(x)$.

Exercise.

- Compute $D\,(x\,D - 1)$
- Interpret in terms of the solutions of $y' = 0$ and $x\,y' = y$

Skew Euclidean structure

- Euclidean right division:

$$L = Q\,P + R \qquad \text{with } \operatorname{order}(R) < \operatorname{order}(P)$$

- Greatest common right divisor:

$$\begin{cases} L_1 = Q_1\,G \\ L_2 = Q_2\,G \end{cases} \qquad \text{with } G \text{ of max order}$$

- Least common left multiple: (↔ closure by sum!)

$$U_1\,L_1 = U_2\,L_2 = M \quad \text{of min order}$$

- Non-commutative Euclidean algorithm
- Annihilating (left) ideal:

$$\begin{aligned} \operatorname{Ann}(f) &= \{L \mid L(f) = 0\} \\ &= G\,\mathbb{K}(x)\langle D\rangle \quad \text{where } G = \text{minimal annihilator of } f \end{aligned}$$

Recurrence operators as skew polynomials

Definition.

$$\mathbb{K}(n)\langle S\rangle = \left\{ \sum_{i=0}^{s} b_i(n)\, S^i \;\middle|\; \begin{array}{l} s \in \mathbb{N}, \\ b_i \in \mathbb{K}(n) \end{array} \right\}$$

with the usual addition of polynomials,
multiplication defined by $S \cdot n = (n+1) \cdot S$ and linearity.

- Also a skew Euclidean ring
- Diff. eq. $\leftrightarrow$ rec. correspondance:

$$\mathbb{K}[x, x^{-1}]\langle D\rangle \quad \cong \quad \mathbb{K}[n]\langle S, S^{-1}\rangle \qquad \text{by} \begin{cases} x \mapsto S^{-1} \\ D \mapsto (n+1)\, S. \end{cases}$$

Several variables

- The idea of D-/P-finiteness generalizes to functions of several variables:

$$\binom{n}{k}^2 \binom{n+k}{k}^2, \quad e^{-x^2} \sin(\alpha x), \quad \ldots$$

- Diff. equations / recurrences are replaced by suitable systems (finitely many ini. cond.):

$$u_{n,k} = \binom{n}{k} \qquad \longleftrightarrow \qquad \begin{cases} (n+1-k)\, u_{n+1,k} = (n+1)\, u_{n,k} \\ (k+1)\, u_{n,k+1} = (n-k)\, u_{n,k} \end{cases}$$

- Equations can mix derivatives and shifts (and other kinds of operator):

$$\begin{cases} x\, J_n'(x) + x\, J_{n+1}(x) - n\, J_n(x) = 0 \\ x\, J_{n+2}(x) - 2\,(n+1)\, J_{n+1}(x) + x\, J_n(x) = 0 \end{cases} \qquad \text{(Bessel functions)}$$

- The closure properties extend ($\Rightarrow$ proofs of identities)

  (algorithms based on noncommutative Gröbner bases)

Creative telescoping

New closure property: by definite summation / integration (under assumptions)

$$u_{n,k} = \binom{n}{k} \qquad \longleftrightarrow \qquad \begin{cases} (n+1-k)\,u_{n+1,k} - (n+1)\,u_{n,k} = 0 \\ (k+1)\,u_{n,k+1} - (n-k)\,u_{n,k} = 0 \end{cases}$$

$$\Big\downarrow \Sigma_k$$

$$v_n = \sum_k u_{n,k} \qquad \longleftrightarrow \qquad v_{n+1} - 2\,v_n = 0$$

Leads to automatic proofs of many more identities:

$$\sum_{k=0}^{n} \left(\sum_{j=0}^{k} \binom{n}{k} \right) = \left(\frac{n}{2} + 1 \right) 2^{3n} - 3\,n\,2^{n-2} \binom{2\,n}{n}$$

$$\int_0^{+\infty} x\,e^{-px^2}\,J_n(b\,x)\,I_n(c\,x)\,dx = \frac{1}{2\,p} \exp\left(\frac{c^2 - b^2}{4\,p} \right) J_n\left(\frac{b\,c}{p} \right)$$

$$\ldots$$

[Zeilberger 1990, Chyzak 2000, …]