Polynomial and rational solutions of linear differential/recurrence equations

Alin Bostan

Inria informatics mathematics

ENS Lyon

M2, CR11

November 18, 2019

The exercise from last lecture

Let $(a_n)_{n\geq 0}$ be a sequence with $a_0 = a_1 = 1$ satisfying the recurrence

$$(n+3)a_{n+1} = (2n+3)a_n + 3na_{n-1}, \quad \text{for all } \; n > 0.$$

Show that a_n is an integer for all n.

The exercise from last lecture

Let $(a_n)_{n\geq 0}$ be a sequence with $a_0 = a_1 = 1$ satisfying the recurrence

$$(n+3)a_{n+1} = (2n+3)a_n + 3na_{n-1}, \quad \text{for all } n > 0.$$

Show that a_n is an integer for all n.

Follow the next steps:

1. Compute the first 5 terms of the sequence, $a_0, \dots, a_4$;
2. Determine a Hermite-Padé approximant of type $(0,1,2)$ for $(1, f, f^2)$, where $f = \sum_n a_n x^n$;
3. Deduce that $P(x, f(x)) = 0 \bmod x^5$ for $P(x,y) := 1 + (x-1)y + x^2y^2$;
4. Show that the equation $P(x,y) = 0$ admits a root $y = g(x) \in \mathbb{Q}[[x]]$ whose coefficients satisfy the same linear recurrence as $(a_n)_{n\geq 0}$;
5. Deduce that $a_{n+2} = a_{n+1} + \sum_{k=0}^{n} a_k \cdot a_{n-k}$ for all n, and conclude.

Solution

▷ 1. Let's compute the first 5 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(4);
```

$$[1, 1, 2, 4, 9]$$

Solution

▷ 1. Let's compute the first 5 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(4);
```

$$[1, 1, 2, 4, 9]$$

▷ 2. Determine a Hermite-Padé approximant of type $(0, 1, 2)$ for $(1, f, f^2)$:

```
> f:=listtoseries(pro(4),x):
> numapprox[hermite_pade]([1, f, f^2], x, [0, 1, 2]);
```

$$[-1, -x+1, -x^2]$$

Solution

▷ 1. Let's compute the first 5 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(4);
```

$$[1, 1, 2, 4, 9]$$

▷ 2. Determine a Hermite-Padé approximant of type $(0, 1, 2)$ for $(1, f, f^2)$:

```
> f:=listtoseries(pro(4),x):
> numapprox[hermite_pade]([1, f, f^2], x, [0, 1, 2]);
```

$$[-1, -x+1, -x^2]$$

▷ 3. We guessed $P(x, f(x)) = 0 \bmod x^5$ for $P(x, y) = 1 + (x-1)y + x^2y^2$.

Solution

▷ 4. The equation $P(x,y) = 0$ admits a root $y = g(x) = \sum_{n\geq 0} g_n x^n$ in $\mathbb{Q}[[x]]$:

$$g(x) = \frac{1 - x - \sqrt{1 - 2\,x - 3\,x^2}}{2\,x^2} = 1 + x + 2\,x^2 + 4\,x^3 + 9\,x^4 + \cdots$$

Solution

▷ 4. The equation $P(x, y) = 0$ admits a root $y = g(x) = \sum_{n \geq 0} g_n x^n$ in $\mathbb{Q}[[x]]$:

$$g(x) = \frac{1 - x - \sqrt{1 - 2x - 3x^2}}{2x^2} = 1 + x + 2x^2 + 4x^3 + 9x^4 + \cdots$$

▷ $(g_n)_{n \geq 0}$ is an integer sequence, as (by coefficient extraction) it satisfies

$$g_{n+2} = g_{n+1} + \sum_{k=0}^{n} g_k \cdot g_{n-k}.$$

Solution

▷ 4. The equation $P(x,y)=0$ admits a root $y=g(x)=\sum_{n\geq 0} g_n x^n$ in $\mathbb{Q}[[x]]$:

$$g(x) = \frac{1-x-\sqrt{1-2\,x-3\,x^2}}{2\,x^2} = 1+x+2\,x^2+4\,x^3+9\,x^4+\cdots$$

▷ $(g_n)_{n\geq 0}$ is an integer sequence, as (by coefficient extraction) it satisfies

$$g_{n+2} = g_{n+1} + \sum_{k=0}^{n} g_k \cdot g_{n-k}.$$

▷ We show that $(g_n)_{n\geq 0}$ satisfies the same *linear* recurrence as $(a_n)_{n\geq 0}$. Let

$$h(x) := \sqrt{1-2\,x-3\,x^2} = 1-x-2\,x^2\,g(x).$$

Clearly, $h_0=1$, $h_1=-1$, $h_{n+2}=-2\,g_n$ for $n\geq 0$, and

$$\frac{h'(x)}{h(x)} = \frac{3\,x+1}{3\,x^2+2\,x-1}$$

Solution

▷ 4. The equation $P(x,y)=0$ admits a root $y=g(x)=\sum_{n\geq 0} g_n x^n$ in $\mathbb{Q}[[x]]$:

$$g(x)=\frac{1-x-\sqrt{1-2x-3x^2}}{2x^2}=1+x+2x^2+4x^3+9x^4+\cdots$$

▷ $(g_n)_{n\geq 0}$ is an integer sequence, as (by coefficient extraction) it satisfies

$$g_{n+2}=g_{n+1}+\sum_{k=0}^{n} g_k\cdot g_{n-k}.$$

▷ We show that $(g_n)_{n\geq 0}$ satisfies the same *linear* recurrence as $(a_n)_{n\geq 0}$. Let

$$h(x):=\sqrt{1-2x-3x^2}=1-x-2x^2\,g(x).$$

Clearly, $h_0=1$, $h_1=-1$, $h_{n+2}=-2\,g_n$ for $n\geq 0$, and

$$\frac{h'(x)}{h(x)}=\frac{3x+1}{3x^2+2x-1}$$

▷ Hence, $(h_n)_n$ and $(g_n)_n$ satisfy the recurrences

$$(3n-3)\,h_n+(2n+1)\,h_{n+1}-(n+2)\,h_{n+2}=0,$$
$$(3n-3)\,g_{n-2}+(2n+1)\,g_{n-1}-(n+2)\,g_n=0.$$

Solution

▷ 4. The equation $P(x,y)=0$ admits a root $y=g(x)=\sum_{n\geq 0} g_n x^n$ in $\mathbb{Q}[[x]]$:

$$g(x)=\frac{1-x-\sqrt{1-2\,x-3\,x^2}}{2\,x^2}=1+x+2\,x^2+4\,x^3+9\,x^4+\cdots$$

▷ $(g_n)_{n\geq 0}$ is an integer sequence, as (by coefficient extraction) it satisfies

$$g_{n+2}=g_{n+1}+\sum_{k=0}^{n} g_k\cdot g_{n-k}.$$

▷ We show that $(g_n)_{n\geq 0}$ satisfies the same *linear* recurrence as $(a_n)_{n\geq 0}$. Let

$$h(x):=\sqrt{1-2\,x-3\,x^2}=1-x-2\,x^2\,g(x).$$

Clearly, $h_0=1$, $h_1=-1$, $h_{n+2}=-2\,g_n$ for $n\geq 0$, and

$$\frac{h'(x)}{h(x)}=\frac{3\,x+1}{3\,x^2+2\,x-1}$$

▷ Hence, $(h_n)_n$ and $(g_n)_n$ satisfy the recurrences

$$(3\,n-3)\,h_n+(2\,n+1)\,h_{n+1}-(n+2)\,h_{n+2}=0,$$
$$(3\,n-3)\,g_{n-2}+(2\,n+1)\,g_{n-1}-(n+2)\,g_n=0.$$

▷ Conclusion: $a_n=g_n$ is an integer for all n. □

Solution

▷ 4. The equation $P(x, y) = 0$ admits a root $y = g(x) = \sum_{n\geq 0} g_n x^n$ in $\mathbb{Q}[[x]]$:

$$g(x) = \frac{1 - x - \sqrt{1 - 2x - 3x^2}}{2x^2} = 1 + x + 2x^2 + 4x^3 + 9x^4 + \cdots$$

▷ $(g_n)_{n\geq 0}$ is an integer sequence, as (by coefficient extraction) it satisfies

$$g_{n+2} = g_{n+1} + \sum_{k=0}^{n} g_k \cdot g_{n-k}.$$

Solution

▷ 4. The equation $P(x,y)=0$ admits a root $y=g(x)=\sum_{n\geq 0} g_n x^n$ in $\mathbb{Q}[[x]]$:

$$g(x) = \frac{1-x-\sqrt{1-2x-3x^2}}{2x^2} = 1+x+2x^2+4x^3+9x^4+\cdots$$

▷ $(g_n)_{n\geq 0}$ is an integer sequence, as (by coefficient extraction) it satisfies

$$g_{n+2} = g_{n+1} + \sum_{k=0}^{n} g_k \cdot g_{n-k}.$$

▷ We show that $(g_n)_{n\geq 0}$ satisfies the same *linear* recurrence as $(a_n)_{n\geq 0}$.

```
> pol:=x^2*y^2 + (x-1)*y + 1;
> deq:=gfun:-algeqtodiffeq(pol,y(x)):
> recg:=gfun:-diffeqtorec(deq,y(x),g(n));
```

$$\{(3n+3)\,g_n + (2n+5)\,g_{n+1} - (n+4)\,g_{n+2} = 0,\ g_0 = 1,\ g_1 = 1\}$$

Solution

▷ 4. The equation $P(x,y)=0$ admits a root $y=g(x)=\sum_{n\geq 0} g_n x^n$ in $\mathbb{Q}[[x]]$:

$$g(x) = \frac{1-x-\sqrt{1-2x-3x^2}}{2x^2} = 1+x+2x^2+4x^3+9x^4+\cdots$$

▷ $(g_n)_{n\geq 0}$ is an integer sequence, as (by coefficient extraction) it satisfies

$$g_{n+2} = g_{n+1} + \sum_{k=0}^{n} g_k \cdot g_{n-k}.$$

▷ We show that $(g_n)_{n\geq 0}$ satisfies the same *linear* recurrence as $(a_n)_{n\geq 0}$.

```
> pol:=x^2*y^2 + (x-1)*y + 1;
> deq:=gfun:-algeqtodiffeq(pol,y(x)):
> recg:=gfun:-diffeqtorec(deq,y(x),g(n));
```

$$\{(3n+3)\,g_n + (2n+5)\,g_{n+1} - (n+4)\,g_{n+2} = 0,\ g_0 = 1,\ g_1 = 1\}$$

▷ Conclusion: $a_n = g_n$ is an integer for all n. $\square$

Resolution of Linear Differential Equations (LDEs):

- homogeneous LDE

$$c_m(x)y^{(m)}(x) + \cdots + c_0(x)y(x) = 0, \qquad c_i \in \mathbb{K}[x]$$

- inhomogeneous LDE

$$c_m(x)y^{(m)}(x) + \cdots + c_0(x)y(x) = b(x), \qquad c_i, b \in \mathbb{K}[x]$$

- inhomogeneous parametrized LDE

$$c_m(x)y^{(m)}(x) + \cdots + c_0(x)y(x) = \sum_{j=0}^{S} \lambda_j b_j(x) \quad \lambda_j \in \mathbb{K},\ c_i,\ b_j \in \mathbb{K}[x]$$

▷ Input in blue, output in red

Resolution of Linear Recurrence Equations (LREs):

- homogeneous LRE

$$p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0, \qquad p_i \in \mathbb{K}[n]$$

- inhomogeneous LRE

$$p_r(n)u_{n+r} + \cdots + p_0(n)u_n = b(n), \qquad p_i, b \in \mathbb{K}[n]$$

- inhomogeneous parametrized LRE

$$p_r(n)u_{n+r} + \cdots + p_0(n)u_n = \sum_{j=0}^{S} \lambda_j b_j(n) \quad \lambda_j \in \mathbb{K},\ p_i,\ b_j \in \mathbb{K}[n]$$

▷ Input in blue, output in red

Context

- Tasks: solve all these equations for
  - power series solutions of LDEs, finite-support solutions of LREs
  - polynomial and rational solutions $\longrightarrow$ central tool in $\sum$ and $\int$ algos

- Sub-tasks:
  - structure of space of solutions
  - complexity issues
  - inhomogeneous parametrized: existence and values of parameters λ_i for which there exist polynomial / rational solutions

- Main focus: homogeneous case (the other cases reduce to it)

Context

▷ Basic, but important, observation: polynomial/rational solutions may have exponentially large degree with respect to the bit-size of the input equation

- E.g., $u_n = n(n+1)\cdots(n+10^{10}-1)$ is a degree-10^{10} solution of LRE

$$n u_{n+1} - (n+10^{10}) u_n = 0$$

- E.g., $y(x) = \sum_{k=0}^{10^{10}} \binom{10^{10}}{k} x^k$ is a degree-10^{10} solution of LDE

$$(x+1) y'(x) - 10^{10} y(x) = 0$$

▷ In both cases, when written in the monomial basis of $\mathbb{K}[n]$, resp. of $\mathbb{K}[x]$, outputs have degree $\tilde{O}(N)$ and bit-size $\tilde{O}(N^2)$, for inputs of bit-size $\log N$.

Theorem. The set of sequences $(u_n)_{n\geq 0}$ solutions of the LRE

$$\text{(LRE):} \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0$$

is a $\mathbb{K}$-vector space of finite dimension, lying between r and $r + |H|$, where

$$H := \{h \in \mathbb{N} \mid p_r(h) = 0\}.$$

Solution space of LREs

Theorem. The set of sequences $(u_n)_{n\geq 0}$ solutions of the LRE

$$\text{(LRE)}: \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0$$

is a $\mathbb{K}$-vector space of finite dimension, lying between r and $r + |H|$, where

$$H := \{h \in \mathbb{N} \mid p_r(h) = 0\}.$$

Remarks:

▷ When $p_r \in \mathbb{K} \setminus \{0\}$ (e.g., for r.l.s.c.c.), this dimension is exactly r.

▷ Same is true for all regular recurrences, that is when $H = \emptyset$.

▷ A singular example: $n(n-1)u_{n+3} - (n-1)u_{n+2} + (n+1)u_{n+1} + 2nu_n = 0$

- for $n = 0 \Rightarrow u_2 + u_1 = 0$ and u_3 is free
- for $n = 1 \Rightarrow 2u_2 + 2u_1 = 0$ and u_4 is free
- for $n \geq 2 \Rightarrow$ recurrence forces value of u_{n+3} in terms of previous ones

So $\dim = 4$: u_0, u_1, u_3, u_4 are free, all other are linear combinations of them.

Solution space of LREs

Theorem. The set of sequences $(u_n)_{n\geq 0}$ solutions of the LRE

$$\text{(LRE)}: \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0$$

is a $\mathbb{K}$-vector space of finite dimension, lying between r and $r + |H|$, where

$$H := \{h \in \mathbb{N} \mid p_r(h) = 0\}.$$

Remarks:

▷ When $p_r \in \mathbb{K} \setminus \{0\}$ (e.g., for r.l.s.c.c.), this dimension is exactly r.

▷ Same is true for all regular recurrences, that is when $H = \emptyset$.

▷ A singular example: $n(n-1)u_{n+3} - (n-1)u_{n+2} + (n+1)u_{n+1} + 3nu_n = 0$

- for $n = 0 \;\Rightarrow\; u_2 + u_1 = 0$ and u_3 is free
- for $n = 1 \;\Rightarrow\; 2u_2 + 3u_1 = 0$ and u_4 is free
- for $n \geq 2 \;\Rightarrow\;$ recurrence forces value of u_{n+3} in terms of previous ones

So $\dim = 3$: u_0, u_3, u_4 are free, all other are linear combinations of them.

Theorem. The set of sequences $(u_n)_{n\geq 0}$ solutions of the LRE

$$\text{(LRE):} \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0$$

is a $\mathbb{K}$-vector space of finite dimension, lying between r and $r + |H|$, where

$$H := \{h \in \mathbb{N} \mid p_r(h) = 0\}.$$

Proof:

- Let $J := \{0, \ldots, r-1\} \cup \{h + r \mid h \in H\}$. Note: $|J| = r + |H|$.
- For $n \in \mathbb{N} \setminus J$, value of u_{n+r} is uniquely determined from previous ones.
- $\dim \Lambda_\ell = \dim \Lambda_{\ell-1}$ for $\ell \notin J$, and $\dim \Lambda_j \leq 1 + \dim \Lambda_{j-1}$ for $j \in J$, where

$$\Lambda_\ell := \left\{ (u_0, \ldots, u_\ell) \in \mathbb{K}^{\ell+1} \;\middle|\; \text{(LRE) true for } n \in \{0, \ldots, \ell - r\} \right\}.$$

- $\dim \Lambda_0 = 1, \ldots, \dim \Lambda_{r-1} = r$ and $\dim \mathsf{Sols}(\mathsf{LRE}) = \dim \Lambda_{\max(J)}$ $\square$

▷ Linear algebra in dimension $\max(J) \longrightarrow$ basis of solution space $\mathsf{Sols}(\mathsf{LRE})$.

Theorem. If $y(x) = \sum_{n\geq 0} u_n x^n \in \mathbb{K}[[x]]$ is a solution of the LDE

$$\text{(LDE):} \qquad c_m(x) y^{(m)}(x) + \cdots + c_0(x) y(x) = 0,$$

with $c_i(x) = \sum_{j=0}^{d} c_{i,j} x^j$ in $\mathbb{K}[x]$, then the sequence $(u_n)_{n\geq 0}$ satisfies the LRE

$$\sum_{i=0}^{m} \sum_{j=0}^{d} c_{i,j} (n+i-j) \cdots (n+1-j) u_{n+i-j} = 0,$$

for all $n \in \mathbb{Z}$, with $u_\ell = 0$ for $\ell < 0$. This writes for some $0 \leq r \leq m+d$:

$$p_r(n) u_{n+r} + \cdots + p_0(n) u_n = 0,$$

together with the equations (translating the constraints $u_\ell = 0$ for $\ell < 0$):

$$p_r(-1) u_{r-1} + \cdots + p_1(-1) u_0 = 0, \quad p_r(-2) u_{r-2} + \cdots = 0, \ldots, \quad p_r(-r) u_0 = 0.$$

Proof: Extract coefficient of x^n in $\text{LDE}(y(x)) = 0$.

Indicial equations of LDEs

Let, as before, the linear differential equation

$$\text{(LDE):}\qquad c_m(x)y^{(m)}(x) + \cdots + c_0(x)y(x) = 0,$$

with associated linear recurrence equation

$$\text{(LRE):}\qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0.$$

Def. Polynomial $p_r(n-r)$ in $\mathbb{K}[x]$ is called indicial polynomial at 0 of (LDE)
Def. Polynomial $p_0(n)$ in $\mathbb{K}[x]$ is called indicial polynomial at infinity of (LDE)

Let (LDE_α): $c_m(x+\alpha)y^{(m)}(x) + \cdots + c_0(x+\alpha)y(x) = 0$ for any $\alpha \in \overline{\mathbb{K}}$.

Def. Indicial polynomial at $x = \alpha$ of (LDE) is indicial poly. at $x = 0$ of (LDE_α).

▷ Indicial polynomials at infinity of LDE and of (LDE_α) coincide.

(LDE): $c_m(x)y^{(m)}(x) + \cdots + c_0(x)y(x) = 0$,   (LRE): $p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0$.

Theorem.
(1) If $F \in \mathbb{K}[[x]]$ is a solution of (LDE) then its valuation $\mathrm{val}(F)$ is a root of the indicial polynomial at 0 of (LDE).
(2) (Cauchy) If $c_m(0) \neq 0$ then (LDE) admits a basis of m solutions in $\mathbb{K}[[x]]$, with valuations $0, 1, \ldots, m-1$.

(LDE): $c_m(x)y^{(m)}(x)+\cdots+c_0(x)y(x)=0, \quad$ (LRE): $p_r(n)u_{n+r}+\cdots+p_0(n)u_n=0.$

Theorem.
(1) If $F\in\mathbb{K}[[x]]$ is a solution of (LDE) then its valuation $\operatorname{val}(F)$ is a root of the indicial polynomial at 0 of (LDE).
(2) (Cauchy) If $c_m(0)\neq 0$ then (LDE) admits a basis of m solutions in $\mathbb{K}[[x]]$, with valuations $0,1,\ldots,m-1$.

Proof:
(1) Evaluate (LRE) at $n=\operatorname{val}(F)-r$.
(2) Assume $c_m(0)\neq 0$. Then (LRE) reads

$$0=c_m(0)\cdot(n+m)\cdots(n+1)u_{n+m}+\big(\text{terms in } u_{<n+m}\big)$$

▷ Thus, (LRE) has order at least m, and it is regular,
so there exist $y_i=x^i+O(x^m)$ solutions of (LDE) for $i=0,1,\ldots,m-1$.
▷ The indicial polynomial at 0 equals $p_r(n-r)=c_m(0)\cdot n\cdots(n-m+1)$,
so by (1) these y_i form a basis of solutions of (LDE).

Series solutions of LDEs

$$\text{(LDE)}: \ c_m(x)y^{(m)}(x)+\cdots+c_0(x)y(x)=0, \quad \text{(LRE)}: \ p_r(n)y_{n+r}+\cdots+p_0(n)y_n=0.$$

Theorem.
(1) If $F \in \mathbb{K}[[x]]$ is a solution of (LDE) then its valuation $\mathrm{val}(F)$ is a root of the indicial polynomial at 0 of (LDE).
(2) (Cauchy) If $c_m(0) \neq 0$ then (LDE) admits a basis of m solutions in $\mathbb{K}[[x]]$, with valuations $0, 1, \ldots, m-1$.

▷ Ex: The converse of (2) is also true: if (LDE) admits a basis of m solutions in $\mathbb{K}[[x]]$ with valuations $0, 1, \ldots, m-1$, then $c_m(0) \neq 0$.

▷ When $c_m(0) \neq 0$, one says that $x = 0$ is an ordinary point for (LDE).

Corollary: If $x = 0$ is an ordinary point for (LDE), then one can compute a full basis of power series solutions mod x^N in $O(N)$ operations in $\mathbb{K}$.

(LDE) of order $m = 3$

$$(x-1)(x+1)\,y'''(x) + y'(x) + \left(x^2-1\right) y(x) = 0$$

▷ Corresponding (LRE) of order $r = 5$

$$-(n+3)(n+2)(n+1)\,u_{n+3} + (n+1)\left(n^2 - n + 1\right) u_{n+1} - u_n + u_{n-2} = 0$$

▷ Indicial equation at 0 equals $-n(n-1)(n-2)$.

▷ Basis of solutions of (LDE):

$$1 + 0\cdot x + 0\cdot x^2 - \frac{1}{6}\cdot x^3 + 0\cdot x^4 - \frac{1}{120}\cdot x^5 + O\left(x^6\right),$$
$$0 + 1\cdot x + 0\cdot x^2 + \frac{1}{6}\cdot x^3 - \frac{1}{24}\cdot x^4 + \frac{1}{40}\cdot x^5 + O\left(x^6\right),$$
$$0 + 0\cdot x + 1\cdot x^2 + 0\cdot x^3 + \frac{1}{12}\cdot x^4 - \frac{1}{60}\cdot x^5 + O\left(x^6\right).$$

Solutions with finite support of LRE

Def: A sequence $(u_n)_{n\geq 0}$ has finite support if $\exists N \geq 0$ s.t. $u_n = 0$ for $n > N$. We call N the degree of $(u_n)_{n\geq 0}$ if $u_N \neq 0$.

Task: Find solutions with finite support of

$$\text{(LRE):} \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0.$$

- ▷ The degree of such a solution must be a root of $p_0(n)$.
- ▷ Solution space: vector space of dim $\leq$ number of roots in $\mathbb{N}$ of $p_0(n)$.
- ▷ Algorithm:
  - Compute $S := \{h \in \mathbb{N} \mid p_0(h) \cdot p_r(h) = 0\}$
  - If $S = \varnothing$, return no solution; if not, let $N := \max S$.
  - Solve a linear system:
    - equations: eval. (LRE) at $n = 0, 1, \ldots, N$; add $u_{N+i} = 0$ for $i = 1, \ldots, r$
    - unknowns: $u_0, u_1, \ldots, u_{N+r}$
- ▷ Complexity: $O(N^\theta)$
- ▷ One can do better: $O(N + |K|^\theta)$

Polynomial solutions of LDEs

Task: Given $c_0, \dots, c_m \in \mathbb{K}[x]$, compute a basis of solutions in $\mathbb{K}[x]$ of

$$\text{(LDE)}: \qquad c_m(x)y^{(m)}(x) + \cdots + c_0(x)y(x) = 0.$$

▷ If a bound N on the degree of a solution $y(x) \in \mathbb{K}[x]$ is known, then the coefficients of $y(x)$ can be computed by linear algebra

▷ Such a bound on the degree is the largest root N in $\mathbb{N}$ of the indicial polynomial of (LDE) at infinity

▷ One can compute a basis of polynomial solutions:

- in $O(N^\theta)$ by dense linear algebra
- in $O(N)$ by exploiting the structure (banded matrix)

▷ One can decide *existence* of nonzero polynomial solutions faster! $\tilde{O}(\sqrt{N})$

Existence of polynomial solutions of LDEs

Task: Given $c_0, \dots, c_m \in \mathbb{K}[x]$, decide if there exist solutions in $\mathbb{K}[x] \setminus \{0\}$ of

$$\text{(LDE):} \qquad c_m(x) y^{(m)}(x) + \cdots + c_0(x) y(x) = 0.$$

▷ Up to a shift, one may assume $c_m(0) \neq 0$, i.e. $x = 0$ is an ordinary point

▷ Let $\{y_1, \dots, y_m\} \subset \mathbb{K}[[x]]$ be a basis of power series solutions of (LDE) (and N the largest root in $\mathbb{N}$ of the indicial polynomial of (LDE) at infinity).

▷ Any solution in $\mathbb{K}[x]_{\leq N}$ of (LDE) is a $\mathbb{K}$-linear combination of the y_i's

▷ With $d = \max(\deg c_i)$, one can choose

$$y_i = x^i + u_{i,m} x^m + \cdots + u_{i,N} x^N + \cdots + u_{i,N+m+d} x^{N+m+d} + \cdots$$

▷ One can compute coefficients in blue in $\tilde{O}(\sqrt{N})$ by baby-steps/giant-steps

▷ $y = \sum_i \lambda_i y_i$ is in $\mathbb{K}[x]_{\leq N} \iff \sum_{i=1}^m \lambda_i u_{i,N+j} = 0$ for all $1 \leq j \leq m + d$

▷ Computing the kernel does not depend on N

Polynomial solutions of LREs

Task: Given $p_0, \ldots, p_r \in \mathbb{K}[n]$, compute a basis of solutions in $\mathbb{K}[n]$ of

$$\text{(LRE)}: \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0.$$

▷ Same principle as for LDEs: "degree bound + linear algebra"

Main sub-task: Degree bound

▷ With $(\Delta \cdot u)(n) = u(n+1) - u(n)$, rewrite recurrence equation (LRE) as

$$\text{(LRE)}: \qquad L \cdot u = \sum_{k=0}^{s} b_k(n)\Delta^k u = 0.$$

▷ Advantage: Δ decreases degrees by 1, thus $\deg(\Delta^k P) \leq \max(\deg P - k, 0)$.

▷ Corollary: $\deg(L \cdot P) \leq B + \deg P$, with $B := \max_k\{\deg(b_k) - k\}$

▷ If $P = n^D + \cdots \in \mathbb{K}[n]$ is a solution of (LRE), then

- either $D + B < 0$, thus D is upper bounded by $-(B+1)$;
- or $[n^{D+B}]\,(L \cdot P) = \sum_{\deg b_k - k = B} \operatorname{lc}(b_k) D(D-1)\cdots(D-k+1)$ is zero

Bound on Degree for Polynomial solutions of LREs

Task: Given $p_0, \ldots, p_r \in \mathbb{K}[n]$, bound the degree of polynomial solutions of

$$\text{(LRE):} \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0.$$

▷ With $(\Delta \cdot u)(n) = u(n+1) - u(n)$, rewrite recurrence equation (LRE) as

$$\text{(LRE):} \qquad L \cdot u = \sum_{k=0}^{s} b_k(n)\Delta^k u = 0.$$

▷ Theorem. A bound on the degree of polynomial solutions of (LRE) is

$$\max\left(-(B+1),\ \text{largest root } D \in \mathbb{N} \text{ of } \underbrace{\sum_{k\in E} \mathrm{lc}(b_k)D(D-1)\cdots(D-k+1)}_{=:\text{indicial polynomial of (LRE)}} \right)$$

where

- $B := \max_k\{\deg(b_k) - k\}$, weighted (n, Δ)-degree of L, for $\deg(\Delta) = -1$;
- $E := \{\, k \mid \deg(b_k) - k = B \,\}$, indices where weighted degree is reached.

Polynomial solutions of LREs: an example

Question: Find all polynomial solutions of

$$(n-3)u_{n+2} - (2n-3)u_{n+1} + nu_n = 0$$

▷ The recurrence can be rewritten:

$$(n-3)(\Delta^2 u_n + 2\Delta u_n + u_n) - (2n-3)(\Delta u_n + u_n) + nu_n = 0,$$

that is

$$L(u) \;=\; \Big((n-3)\Delta^2 - 3\Delta\Big)\,(u_n) = 0$$

▷ B is -1 and the set E is $\{1,2\}$.

▷ Indicial polynomial is $D(D-1) - 3D = D(D-4)$

▷ Degree bound is 4; solution $P(n) = n^4 + an^3 + bn^2 + cn + d$

▷ $L(P) = (-3\,a - 30)\,n^2 + (-21\,a - 70 - 4\,b)\,n - 21\,a - 45 - 9\,b - 3\,c = 0,$
with solution $a = -10,\ b = 35,\ c = -50$, and d is free.

▷ Basis of solutions given by

$$\Big\{(n-1)\,(n-2)\,(n-3)\,(n-4)\,, \qquad n\,(n-5)\,\Big(n^2 - 5\,n + 10\Big)\Big\}$$

Polynomial solutions of LREs: binomial basis

Remark: Degree bound can be exponentially large in the bit size of (LRE)!

▷ E.g., $nu_{n+1} - (n+100)u_n = 0$ has solution $u_n = n(n+1)\cdots(n+99)$.

▷ For LDEs, we exploited the fact that coefficients sequence of a series solution satisfies a LRE. This is false for LREs in the monomial basis. Still:

Theorem. If (u_n) is a polynomial solution of a LRE of order r with coefficients of degree at most d, then its coefficient sequence (c_k) in the binomial basis $\{\binom{n}{k}, k \in \mathbb{N}\}$ is a solution with finite support of another LRE, of order at most $d+r$, degree at most d, with no additional singularities.

Polynomial solutions of LREs: binomial basis

Remark: Degree bound can be exponentially large in the bit size of (LRE)!

▷ E.g., $nu_{n+1} - (n+100)u_n = 0$ has solution $u_n = n(n+1)\cdots(n+99)$.

▷ For LDEs, we exploited the fact that coefficients sequence of a series solution satisfies a LRE. This is false for LREs in the monomial basis. Still:

Theorem. If (u_n) is a polynomial solution of a LRE of order r with coefficients of degree at most d, then its coefficient sequence (c_k) in the binomial basis $\{\binom{n}{k}, k \in \mathbb{N}\}$ is a solution with finite support of another LRE, of order at most $d+r$, degree at most d, with no additional singularities.

Proof:

$$u_n = \sum_{k=0}^{d} c_k \binom{n}{k} \Longrightarrow nu_n = \sum_{k=0}^{d+1} k(c_k + c_{k-1}) \binom{n}{k}, \; u_{n+1} = \sum_{k=0}^{d} (c_k + c_{k+1}) \binom{n}{k}.$$

Remark: Degree bound can be exponentially large in the bit size of (LRE)!

▷ E.g., $nu_{n+1} - (n+100)u_n = 0$ has solution $u_n = n(n+1)\cdots(n+99)$.

▷ For LDEs, we exploited the fact that coefficients sequence of a series solution satisfies a LRE. This is false for LREs in the monomial basis. Still:

Theorem. If (u_n) is a polynomial solution of a LRE of order r with coefficients of degree at most d, then its coefficient sequence (c_k) in the binomial basis $\{\binom{n}{k}, k \in \mathbb{N}\}$ is a solution with finite support of another LRE, of order at most $d+r$, degree at most d, with no additional singularities.

Proof:

$$u_n = \sum_{k=0}^{d} c_k \binom{n}{k} \Longrightarrow nu_n = \sum_{k=0}^{d+1} k(c_k + c_{k-1})\binom{n}{k}, \; u_{n+1} = \sum_{k=0}^{d} (c_k + c_{k+1})\binom{n}{k}.$$

▷ Example: for $nu_{n+1} - (n+100)u_n = 0$, we have

$$k(c_k + c_{k+1} + c_{k-1} + c_k) - k(c_k + c_{k-1}) - 100c_k = kc_{k+1} + (k-100)c_k = 0.$$

A first exercise for next time (25/11/2019)

Find all polynomial solutions of the recurrence equation

$$3u_{n+2} - nu_{n+1} + (n-1)u_n = 0.$$

Task: Given $c_0, \ldots, c_m \in \mathbb{K}[x]$, compute a basis of solutions in $\mathbb{K}(x)$ of

$$\text{(LDE)}: \qquad c_m(x)y^{(m)}(x) + \cdots + c_0(x)y(x) = 0.$$

▷ Even assuming numerator/denominator bounds, a naive approach by undetermined coefficients would lead to a non-linear polynomial system.

▷ Better strategy [Liouville, 1833]:

1. find a multiple of denominators of all rational solutions $\longrightarrow$ singularity analysis
2. reduce to polynomial solutions for numerators $\longrightarrow$ change of unknowns

▷ Singularity analysis based on:

1. any solution $y(x) \in \mathbb{K}(x)$ of (LDE) has an expansion, around any of its poles $\alpha \in \overline{\mathbb{K}}$, as generalized series $(x-\alpha)^v \sum_i u_i (x-\alpha)^i$, with $v \in \mathbb{Z} \setminus \mathbb{N}$
2. order $-v$ of the pole at $x = \alpha$ is bounded by the opposite of the smallest root in $\mathbb{Z}_-$ of the indicial polynomial at α

Liouville(LDE)

In: A LDE $c_m(x)y^{(m)}(x) + \cdots + c_0(x)y(x) = 0$ with $c_i \in \mathbb{K}[x]$

Out: A basis of its rational solutions in $\mathbb{K}(x)$.

1. At each root α of c_m:
   - compute the indicial polynomial $p_\alpha(n)$;
   - compute the smallest root N_α in $\mathbb{Z}_-$ of p_α; if none, set $N_\alpha := 0$.
2. Form the polynomial $P = \prod_{c_m(\alpha)=0} (x-\alpha)^{-N_\alpha}$.
3. Make the change of unknowns $y = Y/P$ in (LDE)
4. Find a basis $\mathcal{B}$ of polynomial solutions $Y(x)$ of the new LDE.
5. Return $\{b/P \mid b \in \mathcal{B}\}$.

Question: Find (a bound on the degree of) all polynomial solutions of

$$(n-3)u_{n+2} - (2n-3)u_{n+1} + nu_n = 0$$

▷ If u_n polynomial solution of degree D, then $y(x) = \sum_n u_n x^n$ is a rational solution of the form $N(x)/(1-x)^{D+1}$ of the corresponding LDE:

$$\begin{aligned} x\,(x-1)^2\left((5\,u_0 - 4\,u_1)x - 5\,u_0\right) y''(x) \\ +2\,(x-1)\left((5\,u_0 - 4\,u_1)x^2 + (5\,u_0 - 10\,u_1)x - 10\,u_0\right) y'(x) \\ -20\,u_1 y(x) = 0 \end{aligned}$$

▷ Indicial equation at $x = 1$ is $(n+1)(n+5)$, so $D + 1 \leq 5$

Consider the differential equation

$$(x-1)(x^2-2)y''(x) + 2x(x^2-x-1)y'(x) + 4(x-2)y(x) = 0.$$

1. Prove that this equation has no nonzero polynomial solution.
2. Show that any rational solution $y(x) \in \mathbb{Q}(x)$ of this equation has at most a pole of order 1 at $x = 1$, and cannot have any other pole.
3. Find all rational solutions $y(x) \in \mathbb{Q}(x)$ of this equation.

Rational solutions of LREs

Task: Given $p_0, \dots, p_r \in \mathbb{K}[n]$, compute a basis of solutions in $\mathbb{K}(n)$ of

$$\text{(LRE):} \qquad p_r(n) u_{n+r} + \cdots + p_0(n) u_n = 0.$$

▷ Even assuming numerator/denominator bounds, a naive approach by undetermined coefficients would lead to a non-linear polynomial system.

▷ Better strategy [Abramov, 1995]:

1. find a multiple of denominators of all rational solutions $\longrightarrow$ singularity analysis
2. reduce to polynomial solutions for numerators $\longrightarrow$ change of unknowns

Task: Given $p_0, \ldots, p_r \in \mathbb{K}[n]$, compute a basis of solutions in $\mathbb{K}(n)$ of

$$\text{(LRE):} \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0.$$

Assume $u_n = P(n)/Q(n)$ solution of (LRE) with $\gcd(P, Q) = 1$. Multiplying

$$p_r(n)\frac{P(n+r)}{Q(n+r)} + \cdots + p_0(n)\frac{P(n)}{Q(n)} = 0$$

by

$$M(n) = \operatorname{lcm}(Q(n+1), \ldots, Q(n+r))$$

yields

$$Q(n) \mid p_0(n)M(n).$$

▷ Idea in simplest case: Assume Q has no two roots with integer difference.
Then $\gcd(Q, M) = 1$. Thus Q divides $p_0(n)$. Similarly, Q divides $p_r(n-r)$.

Rational solutions of LREs: singularity analysis –general case

Task: Given $p_0, \ldots, p_r \in \mathbb{K}[n]$, compute a basis of solutions in $\mathbb{K}(n)$ of

$$\text{(LRE):} \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0.$$

Theorem. Assume $u_n = P(n)/Q(n)$ solution of (LRE) with $\gcd(P, Q) = 1$.
Let α, β be roots in $\overline{\mathbb{K}}$ of Q s.t. $\alpha - \beta = H \in \mathbb{N}$ maximal (H = *dispersion* of Q).
Then $p_0(\alpha) = 0$ and $p_r(\beta - r) = 0$.

Proof: $\alpha + 1, \alpha + 2, \ldots,$ are not roots of Q, i.e., α not pole of $u_{n+1}, \ldots, u_{n+r}$.
So α is not a pole of $p_0(n)u_n$. Since α is a pole of u_n, necessarily $p_0(\alpha) = 0$.

$\beta - 1, \beta - 2, \ldots,$ are not roots of Q, i.e., β not pole of $u_{n-1}, \ldots, u_{n-r}$. So β is not a pole of $p_r(n-r)u_n$. Since β is a pole of u_n, necessarily $p_r(\beta - r) = 0$. □

Corollary. The dispersion H is a root of $\mathrm{Res}_n(p_0(n+h), p_r(n-r)) \in \mathbb{K}[h]$.

Proof: $(n, h) = (\beta, H)$ is solution of system $p_0(n+h) = 0, p_r(n-r) = 0$. □

Task: Given $p_0, \dots, p_r \in \mathbb{K}[n]$, compute a basis of solutions in $\mathbb{K}(n)$ of

$$\text{(LRE):} \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0.$$

Theorem. Assume $u_n = P(n)/Q(n)$ solution of (LRE) with $\gcd(P, Q) = 1$. Let H be the dispersion of Q. Then

$$Q(n) \mid \gcd\left(p_0(n) \cdots p_0(n+H),\ p_r(n-r) \cdots p_r(n-r-H)\right)$$

Proof: We've already proved that $Q(n) \mid p_0(n)\,\mathrm{lcm}(Q(n+1), \dots, Q(n+r))$. Substituting $n \leftarrow n+1$ and repeating yields:

$$\begin{aligned} Q(n) &\mid p_0(n)\,\mathrm{lcm}(p_0(n+1)\,\mathrm{lcm}(Q(n+2), \dots, Q(n+r+1)), Q(n+2), \dots, Q(n+r)) \\ &\mid p_0(n)p_0(n+1)\,\mathrm{lcm}(Q(n+2), \dots, Q(n+r+1)) \\ \cdots &\mid p_0(n) \cdots p_0(n+j)\,\mathrm{lcm}(Q(n+j+1), \dots, Q(n+j+r)). \end{aligned}$$

As $\gcd(Q(n), Q(n+j)) = 1$ for $j > H$, we get $Q(n) \mid p_0(n) \cdots p_0(n+H)$. $\square$

Rational solutions of LREs: singularity analysis –general case

Task: Given $p_0, \dots, p_r \in \mathbb{K}[n]$, compute a basis of solutions in $\mathbb{K}(n)$ of

$$\text{(LRE):} \qquad p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0.$$

Theorem. Assume $u_n = P(n)/Q(n)$ solution of (LRE) with $\gcd(P, Q) = 1$. Let H be the dispersion of Q. Then

$$Q(n) \mid \gcd\big(p_0(n)\cdots p_0(n+H),\ p_r(n-r)\cdots p_r(n-r-H)\big)$$

▷ A refinement: Q divides the (generally smaller) polynomial

$$\prod_{i=1}^{m}\prod_{j=0}^{h_i} \gcd(p_0(n-j+h_i), p_r(n-j-r)),$$

where $h_1 > h_2 > \cdots > h_m \geq 0$ are the roots in $\mathbb{N}$ of

$$R(h) = \operatorname{Res}_n\big(p_0(n+h), p_r(n-r)\big).$$

Rational solutions of LREs: Abramov's algorithm

Abramov(LRE)

In: A LRE $p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0$ with $p_i \in \mathbb{K}[n]$

Out: A multiple of the denominator of all its rational solutions.

1. Compute the polynomial
$$R(h) = \mathrm{Res}_n\big(p_0(n+h), p_r(n-r)\big).$$
2. If R has no roots in $\mathbb{N}$, then return 1; else, let $h_1 > h_2 > \cdots > h_m \geq 0$ be its roots in $\mathbb{N}$. Initialize Q to 1, A to $p_0(n)$, B to $p_r(n-r)$.
3. For $i = 1, \ldots, m$ do
   $g(n) := \gcd\big(A(n+h_i), B(n)\big);$
   $Q(n) := g(n)g(n-1)\cdots g(n-h_i)Q(n);$
   $A(n) := A(n)/g(n-h_i);$
   $B(n) := B(n)/g(n).$
4. Return Q. $\qquad$ // $\prod_{i=1}^{m}\prod_{j=0}^{h_i}\gcd(p_0(n-j+h_i), p_r(n-j-r))$

A third, and last, exercise for next time (25/11/2019)

The aim of this exercise is to show that the sum

$$S_n := \sum_{k=1}^{n} \frac{1}{k!}$$

cannot be simplified under the form

$$S_n = r(n)/n!$$

where $r(n)$ is a rational function in n.

1. Give a linear recurrence with polynomial coefficients satisfied by $r(n)$;
2. Find all rational solutions of the recurrence equation:

$$u_{n+1} - (n+1)u_n = 1.$$

3. Conclude.