Fast skew arithmetic

Alin Bostan

ENS Lyon

M2, CR06

September 21, 2020

The exercise from last week

Prove the identity

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

by performing the following steps:

1. Show that $y = \arcsin(x)$ can be represented by the differential equation $(1-x^2)y'' - xy' = 0$ and the initial conditions $y(0) = 0$, $y'(0) = 1$.
2. Compute a linear differential equation satisfied by $z(x) = y(x)^2$.
3. Deduce a linear recurrence relation satisfied by the coefficients of $z(x)$.
4. Conclude.

Solution, Part 1

The starting point is the identity

$$(\arcsin(x))' = \frac{1}{\sqrt{1-x^2}},$$

which allows to represent $\arcsin(x)$ by the differential equation

$$(1-x^2)y'' - xy' = 0$$

together with the initial conditions

$$y(0) = \arcsin(0) = 0, \quad y'(0) = \frac{1}{\sqrt{1-0^2}} = 1.$$

Solution, Part 2

Let $z = y^2$, with $y'' = \frac{x}{1-x^2} y'$.

Solution, Part 2

Let $z = y^2$, with $y'' = \frac{x}{1-x^2} y'$. By successive differentiations, we get

Solution, Part 2

Let $z = y^2$, with $y'' = \frac{x}{1-x^2} y'$. By successive differentiations, we get

$$\begin{aligned}
z' &= 2yy', \\
z'' &= 2y'^2 + 2yy'' = 2y'^2 + \frac{2x}{1-x^2} yy', \\
z''' &= 4y'y'' + \frac{2x}{1-x^2}(y'^2 + yy'') + \left(\frac{2}{1-x^2} + \frac{4x^2}{(1-x^2)^2} \right) yy' \\
&= \left(\frac{2}{1-x^2} + \frac{6x^2}{(1-x^2)^2} \right) yy' + \frac{6x}{1-x^2} y'^2.
\end{aligned}$$

Solution, Part 2

Let $z = y^2$, with $y'' = \frac{x}{1-x^2} y'$. By successive differentiations, we get

$$
\begin{aligned}
z' &= 2yy', \\
z'' &= 2y'^2 + 2yy'' = 2y'^2 + \frac{2x}{1-x^2} yy', \\
z''' &= 4y'y'' + \frac{2x}{1-x^2}(y'^2 + yy'') + \left(\frac{2}{1-x^2} + \frac{4x^2}{(1-x^2)^2} \right) yy' \\
&= \left(\frac{2}{1-x^2} + \frac{6x^2}{(1-x^2)^2} \right) yy' + \frac{6x}{1-x^2} y'^2.
\end{aligned}
$$

▷ z, z', z'', z''' are $\mathbb{Q}(x)$-linear comb. of y^2, yy', y'^2, thus $\mathbb{Q}(x)$-dependent

Solution, Part 2

Let $z = y^2$, with $y'' = \frac{x}{1-x^2} y'$. By successive differentiations, we get

$$\begin{aligned}
z' &= 2yy', \\
z'' &= 2y'^2 + 2yy'' = 2y'^2 + \frac{2x}{1-x^2} yy', \\
z''' &= 4y'y'' + \frac{2x}{1-x^2}(y'^2 + yy'') + \left(\frac{2}{1-x^2} + \frac{4x^2}{(1-x^2)^2} \right) yy' \\
&= \left(\frac{2}{1-x^2} + \frac{6x^2}{(1-x^2)^2} \right) yy' + \frac{6x}{1-x^2} y'^2.
\end{aligned}$$

▷ z, z', z'', z''' are $\mathbb{Q}(x)$-linear comb. of y^2, yy', y'^2, thus $\mathbb{Q}(x)$-dependent

▷ A dependence relation is determined by computing the kernel of

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & \frac{2x}{1-x^2} & \frac{2}{1-x^2} + \frac{6x^2}{(1-x^2)^2} \\ 0 & 0 & 2 & \frac{6x}{1-x^2} \end{bmatrix}$$

Solution, Part 2

Let $z = y^2$, with $y'' = \frac{x}{1-x^2} y'$. By successive differentiations, we get

$$\begin{aligned} z' &= 2yy', \\ z'' &= 2y'^2 + 2yy'' = 2y'^2 + \frac{2x}{1-x^2} yy', \\ z''' &= 4y'y'' + \frac{2x}{1-x^2}(y'^2 + yy'') + \left(\frac{2}{1-x^2} + \frac{4x^2}{(1-x^2)^2} \right) yy' \\ &= \left(\frac{2}{1-x^2} + \frac{6x^2}{(1-x^2)^2} \right) yy' + \frac{6x}{1-x^2} y'^2. \end{aligned}$$

▷ z, z', z'', z''' are $\mathbb{Q}(x)$-linear comb. of y^2, yy', y'^2, thus $\mathbb{Q}(x)$-dependent
▷ A dependence relation is determined by computing the kernel of

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & \frac{2x}{1-x^2} & \frac{2}{1-x^2} + \frac{6x^2}{(1-x^2)^2} \\ 0 & 0 & 2 & \frac{6x}{1-x^2} \end{bmatrix}$$

▷ The kernel of M is generated by $[0,\ 1,\ 3x,\ x^2 - 1]^T$
▷ The corresponding differential equation is

$$(x^2 - 1) z''' + 3x z'' + z' = 0.$$

Solution, Part 2, a variant

Let $z = y^2$, with $y'' = \frac{x}{1-x^2} y'$.

Solution, Part 2, a variant

Let $z = y^2$, with $y'' = \frac{x}{1-x^2} y'$. By successive differentiations, we get

Solution, Part 2, a variant

Let $z = y^2$, with $y'' = \frac{x}{1-x^2} y'$. By successive differentiations, we get

$$\begin{aligned}
z' &= 2yy', \\
z'' &= 2y'^2 + 2yy'' = 2y'^2 + \frac{2x}{1-x^2} yy' = 2y'^2 + \frac{x}{1-x^2} z', \\
z''' &= 4y'y'' + \frac{x}{1-x^2} z'' + \left(\frac{1}{1-x^2} + \frac{2\,x^2}{(1-x^2)^2} \right) z' \\
&= \frac{4x}{1-x^2} y'^2 + \frac{x}{1-x^2} z'' + \frac{x^2+1}{(x^2-1)^2} z' \\
&= \frac{2x}{1-x^2} \left(z'' - \frac{x}{1-x^2} z' \right) + \frac{x}{1-x^2} z'' + \frac{x^2+1}{(x^2-1)^2} z'.
\end{aligned}$$

▷ The corresponding differential equation is

$$(x^2-1)z''' + 3xz'' + z' = 0.$$

Solution, Part 3

▷ Write $z(x) = \sum_n a_n x^n$. Then:

Solution, Part 3

▷ Write $z(x) = \sum_n a_n x^n$. Then:

$$z' = \sum_n (n+1) a_{n+1} x^n,$$

Solution, Part 3

▷ Write $z(x) = \sum_n a_n x^n$. Then:

$$z' = \sum_n (n+1) a_{n+1} x^n,$$

$$z'' = \sum_n (n+1)(n+2) a_{n+2} x^n,$$

Solution, Part 3

▷ Write $z(x) = \sum_n a_n x^n$. Then:

$$z' = \sum_n (n+1) a_{n+1} x^n,$$

$$z'' = \sum_n (n+1)(n+2) a_{n+2} x^n,$$

$$z''' = \sum_n (n+1)(n+2)(n+3) a_{n+3} x^n.$$

Solution, Part 3

▷ Write $z(x) = \sum_n a_n x^n$. Then:

$$z' = \sum_n (n+1) a_{n+1} x^n,$$

$$z'' = \sum_n (n+1)(n+2) a_{n+2} x^n,$$

$$z''' = \sum_n (n+1)(n+2)(n+3) a_{n+3} x^n.$$

▷ The coefficient of x^n in $(x^2-1)z''' + 3xz'' + z'$ is

$$(n-1)n(n+1)a_{n+1} - (n+1)(n+2)(n+3)a_{n+3} + 3n(n+1)a_{n+1} + (n+1)a_{n+1}$$

Solution, Part 3

▷ Write $z(x) = \sum_n a_n x^n$. Then:

$$z' = \sum_n (n+1) a_{n+1} x^n,$$

$$z'' = \sum_n (n+1)(n+2) a_{n+2} x^n,$$

$$z''' = \sum_n (n+1)(n+2)(n+3) a_{n+3} x^n.$$

▷ The coefficient of x^n in $(x^2-1)z''' + 3xz'' + z'$ is

$$(n-1)n(n+1)a_{n+1} - (n+1)(n+2)(n+3)a_{n+3} + 3n(n+1)a_{n+1} + (n+1)a_{n+1}$$

▷ Thus, the recurrence corresponding to $(x^2-1)z''' + 3xz'' + z' = 0$ is

$$(n+1)(n+2)(n+3)a_{n+3} = (n+1)^3 a_{n+1}.$$

Solution, Part 3

- Write $z(x) = \sum_n a_n x^n$. Then:

$$z' = \sum_n (n+1) a_{n+1} x^n,$$

$$z'' = \sum_n (n+1)(n+2) a_{n+2} x^n,$$

$$z''' = \sum_n (n+1)(n+2)(n+3) a_{n+3} x^n.$$

- The coefficient of x^n in $(x^2-1)z''' + 3xz'' + z'$ is

$$(n-1)n(n+1)a_{n+1} - (n+1)(n+2)(n+3)a_{n+3} + 3n(n+1)a_{n+1} + (n+1)a_{n+1}$$

- Thus, the recurrence corresponding to $(x^2-1)z''' + 3xz'' + z' = 0$ is

$$(n+1)(n+2)(n+3)a_{n+3} = (n+1)^3 a_{n+1}.$$

- Since $(n+1)$ has no roots in $\mathbb{N}$, it further simplifies to

$$(n+2)(n+3)a_{n+3} - (n+1)^2 a_{n+1} = 0.$$

▷ $z = \sum_n a_n x^n$ satisfies

$$(n+2)(n+3)a_{n+3} - (n+1)^2 a_{n+1} = 0.$$

▷ Initial conditions:

$$a_0 = z(0) = y(0)^2 = 0,\ a_1 = z'(0) = 2y(0)y'(0) = 0,\ a_2 = \frac{1}{2}z''(0) = y'(0)^2 = 1.$$

▷ Recurrence and $a_1 = 0$ imply $a_{2k+1} = 0$, so the series is even.

▷ Let $b_k = a_{2k+2}$. Then $z(x) = \sum_k b_k x^{2k+2}$ and

$$(2k+1)(2k+2)b_k = 4k^2 b_{k-1}, \quad b_0 = 1$$

▷ Thus, the sequence $(b_k)_k$ is hypergeometric and

$$b_k = 2\frac{k^2}{(k+1)(2k+1)}b_{k-1} = \cdots = 2^k \frac{k!^2}{(k+1)!(2k+1)(2k-1)\cdots 3}$$

Solution, Part 4

▷ $z = \sum_n a_n x^n$ satisfies

$$(n+2)(n+3)a_{n+3} - (n+1)^2 a_{n+1} = 0.$$

▷ Initial conditions:

$$a_0 = z(0) = y(0)^2 = 0,\ a_1 = z'(0) = 2y(0)y'(0) = 0,\ a_2 = \frac{1}{2}z''(0) = y'(0)^2 = 1.$$

▷ Recurrence and $a_1 = 0$ imply $a_{2k+1} = 0$, so the series is even.

▷ Let $b_k = a_{2k+2}$. Then $z(x) = \sum_k b_k x^{2k+2}$ and

$$(2k+1)(2k+2)b_k = 4k^2 b_{k-1}, \quad b_0 = 1$$

▷ Thus, the sequence $(b_k)_k$ is hypergeometric and

$$b_k = \frac{k!}{(k+1)\cdot(k+\frac{1}{2})(k-\frac{1}{2})\cdots\frac{3}{2}} = \frac{k!}{(k+\frac{1}{2})(k-\frac{1}{2})\cdots\frac{1}{2}}\frac{1}{2k+2} \qquad \square$$

Solution in Maple

1. Compute D-finite representation for $y(x) = \arcsin(x)$:

```
> gfun:-holexprtodiffeq(arcsin(x),y(x));
```

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

Solution in Maple

1. Compute D-finite representation for $y(x) = \arcsin(x)$:

```
> gfun:-holexprtodiffeq(arcsin(x),y(x));
```

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

2. Compute D-finite representation for $z(x) = \arcsin(x)^2$:

```
> deqz:=gfun:-`diffeq*diffeq`(deq1,deq1, y(x));
```

$$\left\{ \frac{d}{dx} y(x) + 3x \frac{d^2}{dx^2} y(x) + \left(x^2-1\right) \frac{d^3}{dx^3} y(x), y(0) = 0, D(y)(0) = 0, \left(D^{(2)}\right)(y)(0) = 2 \right\}$$

Solution in Maple

3. Compute linear recurrence satisfied by the coefficients a_n of $z(x)$:

```
> recz:=gfun:-diffeqtorec(deqz,y(x),a(n));
```

$$\left\{\left(n^2+2\,n+1\right)a\left(n+1\right)+\left(-n^2-5\,n-6\right)a\left(n+3\right),a\left(0\right)=0,a\left(1\right)=0,a\left(2\right)=1\right\}$$

Solution in Maple

3. Compute linear recurrence satisfied by the coefficients a_n of $z(x)$:

```
> recz:=gfun:-diffeqtorec(deqz,y(x),a(n));
```

$$\left\{\left(n^2+2n+1\right)a(n+1)+\left(-n^2-5n-6\right)a(n+3), a(0)=0, a(1)=0, a(2)=1\right\}$$

4. Compute a closed form for a_n and conclude:

```
> rsolve({recz[1], a(1) = 0, a(2) = 1}, a(n)):
> a2k:=simplify(subs(n=2*k,%)) assuming k::posint;
> subs(GAMMA(k+1/2)=GAMMA(2*k)*sqrt(Pi)/2^(2*k-1)/GAMMA(k),a2k);
```

$$\frac{\sqrt{\pi}\,\Gamma(k)}{2k}\left(\Gamma\left(k+\frac{1}{2}\right)\right)^{-1}, \quad \frac{2^{2k-1}\left((k-1)!\right)^2}{2\,(2k-1)!\,k}$$

Solution in Maple

3. Compute linear recurrence satisfied by the coefficients a_n of $z(x)$:

```
> recz:=gfun:-diffeqtorec(deqz,y(x),a(n));
```

$$\left\{\left(n^2+2\,n+1\right)a\left(n+1\right)+\left(-n^2-5\,n-6\right)a\left(n+3\right),a\left(0\right)=0,a\left(1\right)=0,a\left(2\right)=1\right\}$$

4. Compute a closed form for a_n and conclude:

```
> rsolve({recz[1], a(1) = 0, a(2) = 1}, a(n)):
> a2k:=simplify(subs(n=2*k,%)) assuming k::posint;
> subs(GAMMA(k+1/2)=GAMMA(2*k)*sqrt(Pi)/2^(2*k-1)/GAMMA(k),a2k);
```

$$\frac{\sqrt{\pi}\Gamma\left(k\right)}{2\,k}\left(\Gamma\left(k+\frac{1}{2}\right)\right)^{-1},\quad \frac{2^{2\,k-1}\left(\left(k-1\right)!\right)^2}{2\,\left(2\,k-1\right)!\,k}$$

5. Check

```
> sum(a2k*x^(2*k), k=1..infinity) assuming x>0 and x<1;
```

$$\left(\arcsin\left(x\right)\right)^2$$

LINEAR DIFFERENTIAL OPERATORS

Context and Aim

- $\mathbb{K}$ = an effective field (e.g., $\mathbb{K} = \mathbb{Q}$, or $\mathbb{K} = \mathbb{F}_p$)

Context and Aim

• $\mathbb{K}$ = an effective field (e.g., $\mathbb{K} = \mathbb{Q}$, or $\mathbb{K} = \mathbb{F}_p$)
• $\mathbb{K}[x]\langle\partial\rangle$ = the Weyl algebra of linear differential operators with polynomial coefficients in $\mathbb{K}[x]$; commutation rule $\partial x = x\partial + 1$

Context and Aim

• $\mathbb{K}$ = an effective field (e.g., $\mathbb{K} = \mathbb{Q}$, or $\mathbb{K} = \mathbb{F}_p$)
• $\mathbb{K}[x]\langle\partial\rangle$ = the Weyl algebra of linear differential operators with polynomial coefficients in $\mathbb{K}[x]$; commutation rule $\partial x = x\partial + 1$

Algebraic formalization of the notion of linear differential equation

Context and Aim

- $\mathbb{K}$ = an effective field (e.g., $\mathbb{K} = \mathbb{Q}$, or $\mathbb{K} = \mathbb{F}_p$)
- $\mathbb{K}[x]\langle\partial\rangle$ = the Weyl algebra of linear differential operators with polynomial coefficients in $\mathbb{K}[x]$; commutation rule $\partial x = x\partial + 1$

Algebraic formalization of the notion of linear differential equation

$$a_r(x)y^{(r)}(x) + \cdots + a_1(x)y'(x) + a_0(x)y(x) = 0$$

$$\iff$$

$$L(y) = 0, \quad \text{where} \quad L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

Context and Aim

• $\mathbb{K}$ = an effective field (e.g., $\mathbb{K} = \mathbb{Q}$, or $\mathbb{K} = \mathbb{F}_p$)
• $\mathbb{K}[x]\langle\partial\rangle$ = the Weyl algebra of linear differential operators with polynomial coefficients in $\mathbb{K}[x]$; commutation rule $\partial x = x\partial + 1$

Algebraic formalization of the notion of linear differential equation

$$a_r(x)y^{(r)}(x) + \cdots + a_1(x)y'(x) + a_0(x)y(x) = 0$$
$$\Longleftrightarrow$$
$$L(y) = 0, \quad \text{where} \quad L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

Commutation rule formalizes Leibniz's rule $(fg)' = f'g + fg'$

Context and Aim

• $\mathbb{K}$ = an effective field (e.g., $\mathbb{K} = \mathbb{Q}$, or $\mathbb{K} = \mathbb{F}_p$)
• $\mathbb{K}[x]\langle\partial\rangle$ = the Weyl algebra of linear differential operators with polynomial coefficients in $\mathbb{K}[x]$; commutation rule $\partial x = x\partial + 1$

Algebraic formalization of the notion of linear differential equation

$$a_r(x)y^{(r)}(x) + \cdots + a_1(x)y'(x) + a_0(x)y(x) = 0$$
$$\Longleftrightarrow$$
$$L(y) = 0, \quad \text{where} \quad L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

Commutation rule formalizes Leibniz's rule $(fg)' = f'g + fg'$

▷ General aim: understand **complexity** of operations in $\mathbb{K}[x]\langle\partial\rangle$
▷ Specific aims: **degree bounds** / **fast algorithms** for $\star$, GCRD, LCLM, $\otimes$

Context and Aim

• $\mathbb{K}$ = an effective field (e.g., $\mathbb{K} = \mathbb{Q}$, or $\mathbb{K} = \mathbb{F}_p$)
• $\mathbb{K}[x]\langle\partial\rangle$ = the Weyl algebra of linear differential operators with polynomial coefficients in $\mathbb{K}[x]$; commutation rule $\partial x = x\partial + 1$

Algebraic formalization of the notion of linear differential equation

$$a_r(x)y^{(r)}(x) + \cdots + a_1(x)y'(x) + a_0(x)y(x) = 0$$
$$\Longleftrightarrow$$
$$L(y) = 0, \quad \text{where} \quad L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

Commutation rule formalizes Leibniz's rule $(fg)' = f'g + fg'$

▷ General aim: understand **complexity** of operations in $\mathbb{K}[x]\langle\partial\rangle$
▷ Specific aims: **degree bounds** / **fast algorithms** for $\star$, GCRD, LCLM, $\otimes$

▷ General message: complexity analysis = tool for algorithmic design
▷ Today: polynomial linear algebra = non-comm. **complexity yardstick**

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\operatorname{ord}(L)$

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\mathrm{ord}(L)$

▷ Degree $\deg_x(L) := \max(\deg_x(a_i(x))$ is the **degree** of L, denoted $\deg(L)$

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\operatorname{ord}(L)$

▷ Degree $\deg_x(L) := \max(\deg_x(a_i(x))$ is the **degree** of L, denoted $\deg(L)$

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star P(x) = P(x) \star \partial + P'(x)$

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators
  - ▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$
  - ▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\mathrm{ord}(L)$
  - ▷ Degree $\deg_x(L) := \max(\deg_x(a_i(x)))$ is the **degree** of L, denoted $\deg(L)$
  - ▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star P(x) = P(x) \star \partial + P'(x)$

- $\mathbb{K}(x)\langle\partial\rangle$ = the rational Weyl algebra of linear differential operators

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\operatorname{ord}(L)$

▷ Degree $\deg_x(L) := \max(\deg_x(a_i(x))$ is the **degree** of L, denoted $\deg(L)$

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star P(x) = P(x) \star \partial + P'(x)$

- $\mathbb{K}(x)\langle\partial\rangle$ = the rational Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}(x)$

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\mathrm{ord}(L)$

▷ Degree $\deg_x(L) := \max(\deg_x(a_i(x))$ is the **degree** of L, denoted $\deg(L)$

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star P(x) = P(x) \star \partial + P'(x)$

- $\mathbb{K}(x)\langle\partial\rangle$ = the rational Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}(x)$

▷ $r = \deg_\partial(L)$ is called the **order** of L, denoted $\mathrm{ord}(L)$

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\operatorname{ord}(L)$

▷ Degree $\deg_x(L) := \max(\deg_x(a_i(x))$ is the **degree** of L, denoted $\deg(L)$

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star P(x) = P(x) \star \partial + P'(x)$

- $\mathbb{K}(x)\langle\partial\rangle$ = the rational Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}(x)$

▷ $r = \deg_\partial(L)$ is called the **order** of L, denoted $\operatorname{ord}(L)$

▷ $\deg(L) := \max(\deg(c), \deg(b_i))$, where $a_i = b_i/c$ with c of minimal degree

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\operatorname{ord}(L)$

▷ Degree $\deg_x(L) := \max(\deg_x(a_i(x))$ is the **degree** of L, denoted $\deg(L)$

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star P(x) = P(x) \star \partial + P'(x)$

- $\mathbb{K}(x)\langle\partial\rangle$ = the rational Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}(x)$

▷ $r = \deg_\partial(L)$ is called the **order** of L, denoted $\operatorname{ord}(L)$

▷ $\deg(L) := \max(\deg(c), \deg(b_i))$, where $a_i = b_i/c$ with c of minimal degree

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star R(x) = R(x) \star \partial + R'(x)$

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\operatorname{ord}(L)$

▷ Degree $\deg_x(L) := \max(\deg_x(a_i(x))$ is the **degree** of L, denoted $\deg(L)$

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star P(x) = P(x) \star \partial + P'(x)$

- $\mathbb{K}(x)\langle\partial\rangle$ = the rational Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}(x)$

▷ $r = \deg_\partial(L)$ is called the **order** of L, denoted $\operatorname{ord}(L)$

▷ $\deg(L) := \max(\deg(c), \deg(b_i))$, where $a_i = b_i/c$ with c of minimal degree

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star R(x) = R(x) \star \partial + R'(x)$

▷ Mathematically, the rational Weyl algebra $\mathbb{K}(x)\langle\partial\rangle$ is nicer

Skew (differential) polynomials

- $\mathbb{K}[x]\langle\partial\rangle$ = the polynomial Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}[x]$

▷ Degree $r = \deg_\partial(L)$ is called the **order** of L, denoted $\mathrm{ord}(L)$

▷ Degree $\deg_x(L) := \max(\deg_x(a_i(x))$ is the **degree** of L, denoted $\deg(L)$

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star P(x) = P(x) \star \partial + P'(x)$

- $\mathbb{K}(x)\langle\partial\rangle$ = the rational Weyl algebra of linear differential operators

▷ Elements: $L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$ with $a_i(x) \in \mathbb{K}(x)$

▷ $r = \deg_\partial(L)$ is called the **order** of L, denoted $\mathrm{ord}(L)$

▷ $\deg(L) := \max(\deg(c), \deg(b_i))$, where $a_i = b_i/c$ with c of minimal degree

▷ Usual $+$; *skew* multiplication $\star$ defined by $\partial \star R(x) = R(x) \star \partial + R'(x)$

▷ Mathematically, the rational Weyl algebra $\mathbb{K}(x)\langle\partial\rangle$ is nicer

▷ Algorithmically, the polynomial Weyl algebra $\mathbb{K}[x]\langle\partial\rangle$ is nicer

Rational Weyl algebra is Euclidean

Theorem [Libri 1833, Brassinne 1864, Wedderburn 1932, Ore 1932]
$\mathbb{K}(x)\langle\partial\rangle$ is a non-commutative (left and right) Euclidean domain: for $A, B \in \mathbb{K}(x)\langle\partial\rangle$, there exist unique $Q, R \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$A = QB + R, \qquad \text{and} \quad \operatorname{ord}(R) < \operatorname{ord}(B).$$

Rational Weyl algebra is Euclidean

Theorem [Libri 1833, Brassinne 1864, Wedderburn 1932, Ore 1932]
$\mathbb{K}(x)\langle\partial\rangle$ is a non-commutative (left and right) Euclidean domain: for $A, B \in \mathbb{K}(x)\langle\partial\rangle$, there exist unique $Q, R \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$A = QB + R, \qquad \text{and} \quad \operatorname{ord}(R) < \operatorname{ord}(B).$$

(This is called the Euclidean right division of A by B.)

Rational Weyl algebra is Euclidean

Theorem [Libri 1833, Brassinne 1864, Wedderburn 1932, Ore 1932]
$\mathbb{K}(x)\langle\partial\rangle$ is a non-commutative (left and right) Euclidean domain: for $A, B \in \mathbb{K}(x)\langle\partial\rangle$, there exist unique $Q, R \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$A = QB + R, \qquad \text{and} \quad \operatorname{ord}(R) < \operatorname{ord}(B).$$

(This is called the Euclidean right division of A by B.)

▷ As a consequence, any $A, B \in \mathbb{K}(x)\langle\partial\rangle$ admit a greatest common right divisor (GCRD) and a least common left multiple (LCLM).

Rational Weyl algebra is Euclidean

Theorem [Libri 1833, Brassinne 1864, Wedderburn 1932, Ore 1932]
$\mathbb{K}(x)\langle\partial\rangle$ is a non-commutative (left and right) Euclidean domain: for $A, B \in \mathbb{K}(x)\langle\partial\rangle$, there exist unique $Q, R \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$A = QB + R, \qquad \text{and} \qquad \operatorname{ord}(R) < \operatorname{ord}(B).$$

(This is called the Euclidean right division of A by B.)

▷ As a consequence, any $A, B \in \mathbb{K}(x)\langle\partial\rangle$ admit a greatest common right divisor (GCRD) and a least common left multiple (LCLM).

▷ Moreover, $\operatorname{GCRD}(A, B)$ and $\operatorname{LCLM}(A, B)$ can be computed by a non-commutative version of the extended Euclidean algorithm.

Implementation in `Maple`'s `DEtools` package

▷ `diffop2de`, `de2diffop`, `mult`

```
> with(DEtools):
> mult(Dx,x,[Dx,x]);
```

$$x\partial + 1$$

implements the basic skew multiplication rule.

Implementation in Maple's DEtools package

▷ diffop2de, de2diffop, mult

```
> with(DEtools):
> mult(Dx,x,[Dx,x]);
```

$$x\partial + 1$$

implements the basic skew multiplication rule.

▷ rightdivision, GCRD, LCLM

```
> rightdivision(Dx^10,Dx^2-x,[Dx,x])[2];
```

$$\left(20\,x^3 + 80\right)\,\partial + x^5 + 100\,x^2$$

proves that $\mathrm{Ai}^{(10)}(x) = (20x^3+80)\mathrm{Ai}'(x) + (x^5+100x^2)\mathrm{Ai}(x)$.

Solution spaces

Any element of $\mathbb{K}(x)\langle\partial\rangle$

$$L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

admits a *full solution space* $V(L)$ in some ring R (*Picard-Vessiot extension*)

$$V(L) = \{y \in R \mid L(y) = 0\}$$

which contains "all" solutions of L, in the sense that $\dim_C V(L) = r$, where

$$C = \{y \in R \mid \partial(y) = 0\}$$

Solution spaces

Any element of $\mathbb{K}(x)\langle\partial\rangle$

$$L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

admits a *full solution space* $V(L)$ in some ring R (*Picard-Vessiot extension*)

$$V(L) = \{y \in R \mid L(y) = 0\}$$

which contains "all" solutions of L, in the sense that $\dim_C V(L) = r$, where

$$C = \{y \in R \mid \partial(y) = 0\}$$

▷ Such an R is an analogue of the notion of "splitting field" for polynomials

Solution spaces

Any element of $\mathbb{K}(x)\langle\partial\rangle$

$$L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

admits a *full solution space* $V(L)$ in some ring R (*Picard-Vessiot extension*)

$$V(L) = \{y \in R \mid L(y) = 0\}$$

which contains "all" solutions of L, in the sense that $\dim_C V(L) = r$, where

$$C = \{y \in R \mid \partial(y) = 0\}$$

▷ Such an R is an analogue of the notion of "splitting field" for polynomials

▷ $V(L)$: algebraic counterpart of the notion of "fundamental set of solutions"

Solution spaces

Any element of $\mathbb{K}(x)\langle\partial\rangle$

$$L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

admits a *full solution space* $V(L)$ in some ring R (*Picard-Vessiot extension*)

$$V(L) = \{y \in R \mid L(y) = 0\}$$

which contains "all" solutions of L, in the sense that $\dim_C V(L) = r$, where

$$C = \{y \in R \mid \partial(y) = 0\}$$

▷ Such an R is an analogue of the notion of "splitting field" for polynomials

▷ $V(L)$: algebraic counterpart of the notion of "fundamental set of solutions"

▷ If $\mathrm{char}(\mathbb{K}) = 0$ and if $x = \alpha$ is an *ordinary point* (not pole of any a_j/a_r), then one may choose $R = \mathbb{K}[[x-\alpha]]$ (by the Cauchy-Lipschitz theorem)

Solution spaces

Any element of $\mathbb{K}(x)\langle\partial\rangle$

$$L = a_r(x)\partial^r + \cdots + a_1(x)\partial + a_0(x)$$

admits a *full solution space* $V(L)$ in some ring R (*Picard-Vessiot extension*)

$$V(L) = \{y \in R \mid L(y) = 0\}$$

which contains "all" solutions of L, in the sense that $\dim_C V(L) = r$, where

$$C = \{y \in R \mid \partial(y) = 0\}$$

▷ Such an R is an analogue of the notion of "splitting field" for polynomials

▷ $V(L)$: algebraic counterpart of the notion of "fundamental set of solutions"

▷ If $\operatorname{char}(\mathbb{K}) = 0$ and if $x = \alpha$ is an *ordinary point* (not pole of any a_j/a_r), then one may choose $R = \mathbb{K}[[x-\alpha]]$ (by the Cauchy-Lipschitz theorem)

Exercise 1: Prove that L admits at most $r = \operatorname{ord}(L)$ linearly independent solutions (over C). Hint: use Wronskians.

Definition of LCLM and GCRD

The *least common left multiple* (*LCLM*) of $A, B \in \mathbb{K}(x)\langle\partial\rangle$ is the least order monic operator $L \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$L = Q_1 \star A = Q_2 \star B \quad \text{for some cofactors } Q_1, Q_2 \in \mathbb{K}(x)\langle\partial\rangle$$

Definition of LCLM and GCRD

The *least common left multiple* (*LCLM*) of $A, B \in \mathbb{K}(x)\langle\partial\rangle$ is the least order monic operator $L \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$L = Q_1 \star A = Q_2 \star B \quad \text{for some cofactors } Q_1, Q_2 \in \mathbb{K}(x)\langle\partial\rangle$$

▷ In terms of solution spaces: $V(\mathrm{LCLM}(A, B)) = V(A) + V(B)$

Definition of LCLM and GCRD

The *least common left multiple* (*LCLM*) of $A, B \in \mathbb{K}(x)\langle\partial\rangle$ is the least order monic operator $L \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$L = Q_1 \star A = Q_2 \star B \quad \text{for some cofactors } Q_1, Q_2 \in \mathbb{K}(x)\langle\partial\rangle$$

▷ In terms of solution spaces: $V(\mathrm{LCLM}(A, B)) = V(A) + V(B)$

The *greatest common right divisor* (*GCRD*) of $A, B \in \mathbb{K}(x)\langle\partial\rangle$ is the highest order monic operator $G \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$A = U_1 \star G \quad \text{and} \quad B = U_2 \star G \quad \text{for some cofactors } U_1, U_2 \in \mathbb{K}(x)\langle\partial\rangle$$

Definition of LCLM and GCRD

The *least common left multiple* (*LCLM*) of $A, B \in \mathbb{K}(x)\langle\partial\rangle$ is the least order monic operator $L \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$L = Q_1 \star A = Q_2 \star B \quad \text{for some cofactors } Q_1, Q_2 \in \mathbb{K}(x)\langle\partial\rangle$$

▷ In terms of solution spaces: $V(\mathrm{LCLM}(A,B)) = V(A) + V(B)$

The *greatest common right divisor* (*GCRD*) of $A, B \in \mathbb{K}(x)\langle\partial\rangle$ is the highest order monic operator $G \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$A = U_1 \star G \quad \text{and} \quad B = U_2 \star G \quad \text{for some cofactors } U_1, U_2 \in \mathbb{K}(x)\langle\partial\rangle$$

▷ In terms of solution spaces: $V(GCRD(A,B)) = V(A) \cap V(B)$

Definition of LCLM and GCRD

The *least common left multiple* (*LCLM*) of $A, B \in \mathbb{K}(x)\langle\partial\rangle$ is the least order monic operator $L \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$L = Q_1 \star A = Q_2 \star B \quad \text{for some cofactors } Q_1, Q_2 \in \mathbb{K}(x)\langle\partial\rangle$$

▷ In terms of solution spaces: $V(\mathrm{LCLM}(A,B)) = V(A) + V(B)$

The *greatest common right divisor* (*GCRD*) of $A, B \in \mathbb{K}(x)\langle\partial\rangle$ is the highest order monic operator $G \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$A = U_1 \star G \quad \text{and} \quad B = U_2 \star G \quad \text{for some cofactors } U_1, U_2 \in \mathbb{K}(x)\langle\partial\rangle$$

▷ In terms of solution spaces: $V(GCRD(A,B)) = V(A) \cap V(B)$

▷ Contrary to the commutative case: $A \star B \neq \mathrm{LCLM}(A,B) \star \mathrm{GCRD}(A,B)$
but $\mathrm{ord}(A \star B) = \mathrm{ord}(A) + \mathrm{ord}(B) = \mathrm{ord}(\mathrm{LCLM}(A,B)) + \mathrm{ord}(\mathrm{GCRD}(A,B))$

Example

```
> A:=(x-1)*Dx^3+(x-x^2)*Dx^2+(3-2*x)*Dx-x:
> B:=3*Dx^2+(x^3-3*x)*Dx-x^4-3:
> G:=rightdivision(A,B,[Dx,x]);
```

$$\left[\left(\frac{x}{3}-\frac{1}{3}\right)\partial-\frac{x^4}{9}+\frac{x^3}{9},\left(1-x^3+x^2+\frac{x^7}{9}-\frac{x^6}{9}\right)\partial-x+x^4-x^3-\frac{x^8}{9}+\frac{x^7}{9}\right]$$

Example

```
> A:=(x-1)*Dx^3+(x-x^2)*Dx^2+(3-2*x)*Dx-x:
> B:=3*Dx^2+(x^3-3*x)*Dx-x^4-3:
> G:=rightdivision(A,B,[Dx,x]);
```

$$\left[\left(\frac{x}{3}-\frac{1}{3}\right)\partial-\frac{x^4}{9}+\frac{x^3}{9},\left(1-x^3+x^2+\frac{x^7}{9}-\frac{x^6}{9}\right)\partial-x+x^4-x^3-\frac{x^8}{9}+\frac{x^7}{9}\right]$$

```
> rightdivision(B,G,[Dx,x]);
```

$$\left[\frac{27}{x^7-x^6-9\,x^3+9\,x^2+9}\,\partial+9\,\frac{x\left(x^9-x^8-30\,x^5+27\,x^4+9\,x^2+81\,x-54\right)}{\left(x^7-x^6-9\,x^3+9\,x^2+9\right)^2},0\right]$$

Example

```
> A:=(x-1)*Dx^3+(x-x^2)*Dx^2+(3-2*x)*Dx-x:
> B:=3*Dx^2+(x^3-3*x)*Dx-x^4-3:
> G:=rightdivision(A,B,[Dx,x]);
```

$$\left[\left(\frac{x}{3}-\frac{1}{3}\right)\partial-\frac{x^4}{9}+\frac{x^3}{9},\left(1-x^3+x^2+\frac{x^7}{9}-\frac{x^6}{9}\right)\partial-x+x^4-x^3-\frac{x^8}{9}+\frac{x^7}{9}\right]$$

```
> rightdivision(B,G,[Dx,x]);
```

$$\left[\frac{27}{x^7-x^6-9\,x^3+9\,x^2+9}\,\partial+9\,\frac{x\left(x^9-x^8-30\,x^5+27\,x^4+9\,x^2+81\,x-54\right)}{\left(x^7-x^6-9\,x^3+9\,x^2+9\right)^2},0\right]$$

```
> GCRD(A,B,[Dx,x]);
```

$$\partial-x$$

Euclidean algorithm in $\mathbb{K}[x]$

Euclid(A, B)

In: A and B in $\mathbb{K}[x]$.
Out: A gcd G of A and B.

1. $R_0 := A$; $R_1 := B$; $i := 1$.
2. While R_i is non-zero, do:
   $R_{i+1} := R_{i-1} \bmod R_i$
   $i := i + 1$.
3. Return R_{i-1}.

▷ Termination: $\deg(B) > \deg(R_2) > \deg(R_1) > \cdots$
▷ Correctness: $\gcd(A, B) = \gcd(B, A \bmod B)$
▷ Quadratic complexity: $O\big(\deg(A)\deg(B)\big)$ operations in $\mathbb{K}$

Skew Euclidean algorithm in $\mathbb{K}(x)\langle\partial\rangle$

$\mathsf{SkewEuclid}(A, B)$

In: A and B in $\mathbb{K}(x)\langle\partial\rangle$.
Out: A GCRD G of A and B.

1. $R_0 := A$; $R_1 := B$; $i := 1$.
2. While R_i is non-zero, do:
   $R_{i+1} := R_{i-1} \text{ rmod } R_i$
   $i := i + 1$.
3. Return R_{i-1}.

▷ Termination: $\mathrm{ord}(B) > \mathrm{ord}(R_2) > \mathrm{ord}(R_1) > \cdots$
▷ Correctness: $\mathrm{GCRD}(A, B) = \mathrm{GCRD}(B, A \text{ rmod } B)$
▷ "Complexity": $O\big(\mathrm{ord}(A)\,\mathrm{ord}(B)\big)$ operations in $\mathbb{K}(x)$

Extended Euclidean algorithm in $\mathbb{K}[x]$

ExtendedEuclid(A, B)

In: A and B in $\mathbb{K}[x]$.

Out: A gcd G of A and B, and cofactors U and V.

1. $R_0 := A$; $U_0 := 1$; $V_0 := 0$; $R_1 := B$; $U_1 := 0$; $V_1 := 1$; $i := 1$.
2. While R_i is non-zero, do:
   1. $(Q_i, R_{i+1}) := \text{QuotRem}(R_{i-1}, R_i)$ $\quad\quad$ $\#R_{i-1} = Q_i R_i + R_{i+1}$
   2. $U_{i+1} := U_{i-1} - Q_i U_i$; $V_{i+1} := V_{i-1} - Q_i V_i$.
   3. $i := i + 1$.
3. Return $\big(R_{i-1}, U_{i-1}, V_{i-1}\big)$.

▷ Termination: $\deg(B) > \deg(R_2) > \deg(R_1) > \cdots$

▷ Correctness: $R_i = U_i A + V_i B$ (by induction):

$$R_{i+1} = R_{i-1} - Q_i R_i = U_{i-1}A + V_{i-1}B - Q_i(U_i A + V_i B) = U_{i+1}A + V_{i+1}B$$

▷ Quadratic complexity: $O\big(\deg(A)\deg(B)\big)$ operations in $\mathbb{K}$

Skew Extended Euclidean algorithm in $\mathbb{K}(x)\langle\partial\rangle$

SkewExtendedEuclid(A, B)

In: A and B in $\mathbb{K}(x)\langle\partial\rangle$.

Out: A GCRD G of A and B, and cofactors U and V.

1. $R_0 := A$; $U_0 := 1$; $V_0 := 0$; $R_1 := B$; $U_1 := 0$; $V_1 := 1$; $i := 1$.
2. While R_i is non-zero, do:
   1. $(Q_i, R_{i+1}) := \text{RightDivision}(R_{i-1}, R_i)$ $\quad$ $\#R_{i-1} = Q_i R_i + R_{i+1}$
   2. $U_{i+1} := U_{i-1} - Q_i U_i$; $V_{i+1} := V_{i-1} - Q_i V_i$.
   3. $i := i + 1$.
3. Return $\left(R_{i-1}, U_{i-1}, V_{i-1}\right)$.

▷ Termination: $\text{ord}(B) > \text{ord}(R_2) > \text{ord}(R_1) > \cdots$

▷ Correctness: $R_i = U_i A + V_i B$ (by induction):

$$R_{i+1} = R_{i-1} - Q_i R_i = U_{i-1}A + V_{i-1}B - Q_i(U_i A + V_i B) = U_{i+1}A + V_{i+1}B$$

▷ "Complexity": $O\big(\text{ord}(A)\,\text{ord}(B)\big)$ operations in $\mathbb{K}(x)$

Half-Extended Euclidean algorithm in $\mathbb{K}[x]$

HalfExtendedEuclid(A, B)

In: A and B in $\mathbb{K}[x]$.

Out: A gcd G and an lcm L of A and B.

1. $R_0 := A$; $U_0 := 1$; $R_1 := B$; $U_1 := 0$; $i := 1$.
2. While R_i is non-zero, do:
   1. $(Q_i, R_{i+1}) := \mathrm{QuotRem}(R_{i-1}, R_i)$ #$R_{i-1} = Q_i R_i + R_{i+1}$
   2. $U_{i+1} := U_{i-1} - Q_i U_i$.
   3. $i := i + 1$.
3. Return $(R_{i-1}, U_i A)$.

▷ Quadratic complexity: $O\big(\deg(A)\deg(B)\big)$ operations in $\mathbb{K}$

Skew Half-Extended Euclidean algorithm in $\mathbb{K}(x)\langle\partial\rangle$

SkewHalfExtendedEuclid(A, B)

In: A and B in $\mathbb{K}(x)\langle\partial\rangle$.

Out: A GCRD G and an LCLM L of A and B.

1. $R_0 := A$; $U_0 := 1$; $R_1 := B$; $U_1 := 0$; $i := 1$.
2. While R_i is non-zero, do:
   1. $(Q_i, R_{i+1}) :=$ RightDivision(R_{i-1}, R_i) $\quad \# R_{i-1} = Q_i R_i + R_{i+1}$
   2. $U_{i+1} := U_{i-1} - Q_i U_i$.
   3. $i := i + 1$.
3. Return $\left(R_{i-1}, U_i A\right)$.

▷ "Complexity": $O\big(\mathrm{ord}(A)\,\mathrm{ord}(B)\big)$ operations in $\mathbb{K}(x)$

Definition of SYM

Def. The *symmetric product* (*SYM*) of $L_1, L_2 \in \mathbb{K}(x)\langle\partial\rangle$, denoted $\mathrm{Sym}(L_1, L_2)$, or $L_1 \otimes L_2$, is the least order monic operator $S \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$S(y_1 y_2) = 0 \quad \text{for all } y_1 \in V(L_1), y_2 \in V(L_2)$$

Definition of SYM

Def. The *symmetric product* (*SYM*) of $L_1, L_2 \in \mathbb{K}(x)\langle\partial\rangle$, denoted $\mathrm{Sym}(L_1, L_2)$, or $L_1 \otimes L_2$, is the least order monic operator $S \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$S(y_1 y_2) = 0 \quad \text{for all } y_1 \in V(L_1), y_2 \in V(L_2)$$

▷ In terms of solution spaces: $V(A \otimes B) = V(A) \otimes V(B)$

Def. The *symmetric product* (*SYM*) of $L_1, L_2 \in \mathbb{K}(x)\langle\partial\rangle$, denoted $\mathrm{Sym}(L_1, L_2)$, or $L_1 \otimes L_2$, is the least order monic operator $S \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$S(y_1 y_2) = 0 \quad \text{for all } y_1 \in V(L_1), y_2 \in V(L_2)$$

▷ In terms of solution spaces: $V(A \otimes B) = V(A) \otimes V(B)$

```
> symmetric_product(Dx^3, Dx^2, [Dx,x]);
```

$$\partial^4$$

Definition of SYM

Def. The *symmetric product* (*SYM*) of $L_1, L_2 \in \mathbb{K}(x)\langle\partial\rangle$, denoted $\mathrm{Sym}(L_1, L_2)$, or $L_1 \otimes L_2$, is the least order monic operator $S \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$S(y_1 y_2) = 0 \quad \text{for all } y_1 \in V(L_1), y_2 \in V(L_2)$$

▷ In terms of solution spaces: $V(A \otimes B) = V(A) \otimes V(B)$

```
> symmetric_product(Dx^3, Dx^2, [Dx,x]);
```

$$\partial^4$$

Def. The *m-th symmetric power* (*SYMP*) of $L \in \mathbb{K}(x)\langle\partial\rangle$, denoted $\mathrm{Sym}^m(L)$, is the least order monic operator $S \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$S(y^m) = 0 \quad \text{for all } y \in V(L).$$

Definition of SYM

Def. The *symmetric product* (*SYM*) of $L_1, L_2 \in \mathbb{K}(x)\langle\partial\rangle$, denoted $\mathrm{Sym}(L_1, L_2)$, or $L_1 \otimes L_2$, is the least order monic operator $S \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$S(y_1 y_2) = 0 \quad \text{for all } y_1 \in V(L_1), y_2 \in V(L_2)$$

▷ In terms of solution spaces: $V(A \otimes B) = V(A) \otimes V(B)$

```
> symmetric_product(Dx^3, Dx^2, [Dx,x]);
```

$$\partial^4$$

Def. The *m-th symmetric power* (*SYMP*) of $L \in \mathbb{K}(x)\langle\partial\rangle$, denoted $\mathrm{Sym}^m(L)$, is the least order monic operator $S \in \mathbb{K}(x)\langle\partial\rangle$ such that

$$S(y^m) = 0 \quad \text{for all } y \in V(L).$$

```
> symmetric_power(Dx^3, 2, [Dx,x]);
```

$$\partial^5$$

Example – back to the exercise

```
> deqin:=(1-x^2)*diff(diff(y(x),x),x)-x*diff(y(x),x):
> de:={deqin, y(0)=rand(100)(), D(y)(0)=rand(100)()};
```

$$\left\{-x\frac{\mathrm{d}}{\mathrm{d}x}y\left(x\right)+\left(1-x^{2}\right)\frac{\mathrm{d}^{2}}{\mathrm{d}x^{2}}y\left(x\right),y\left(0\right)=82,\mathrm{D}\left(y\right)\left(0\right)=31\right\}$$

Example – back to the exercise

```
> deqin:=(1-x^2)*diff(diff(y(x),x),x)-x*diff(y(x),x):
> de:={deqin, y(0)=rand(100)(), D(y)(0)=rand(100)()};
```

$$\left\{-x\frac{d}{dx}y(x)+\left(1-x^2\right)\frac{d^2}{dx^2}y(x), y(0)=82, D(y)(0)=31\right\}$$

```
> with(numapprox): Order:=30; p:=%: r:=3:
> Z:=series(op(2, dsolve(de, y(x), series))^2,x,p):
> hermite_pade([Z,seq(series(diff(Z,x$k),x,p),k=1..r)],x,p):
> deqout:=add(HP[k+1]*diff(z(x),x$k), k=1..r);
```

$$\frac{d}{dx}z(x)+3x\frac{d^2}{dx^2}z(x)+\left(x^2-1\right)\frac{d^3}{dx^3}z(x)$$

The case of constant coefficients

▷ Linear differential operators $L = p_r\partial^r + \cdots + p_0$ with coefficients $p_i \in \mathbb{K}$

The case of constant coefficients

▷ Linear differential operators $L = p_r\partial^r + \cdots + p_0$ with coefficients $p_i \in \mathbb{K}$

▷ Characteristic polynomial: $P(x) = p_r x^r + \cdots + p_0$ splits over $\overline{\mathbb{K}}$

$$P(x) = p_r(x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k}, \quad \alpha_i \in \overline{\mathbb{K}}, m_i \in \mathbb{N}^\star,$$

The case of constant coefficients

▷ Linear differential operators $L = p_r \partial^r + \cdots + p_0$ with coefficients $p_i \in \mathbb{K}$

▷ Characteristic polynomial: $P(x) = p_r x^r + \cdots + p_0$ splits over $\overline{\mathbb{K}}$

$$P(x) = p_r (x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k}, \quad \alpha_i \in \overline{\mathbb{K}}, m_i \in \mathbb{N}^\star,$$

▷ $V(L)$ is generated (over $\overline{\mathbb{K}}$) by

$$\left\{ e^{\alpha_1 x}, x e^{\alpha_1 x}, \ldots, x^{m_1 - 1} e^{\alpha_1 x}, \ldots, e^{\alpha_k x}, x e^{\alpha_k x}, \ldots, x^{m_k - 1} e^{\alpha_k x} \right\},$$

where for $\alpha \in \overline{\mathbb{K}}$, we denote by $e^{\alpha x}$ the power series $\sum_{n \geq 0} \alpha^n x^n / n!$ of $\overline{\mathbb{K}}[[x]]$.

The case of constant coefficients

▷ Linear differential operators $L = p_r \partial^r + \cdots + p_0$ with coefficients $p_i \in \mathbb{K}$

▷ Characteristic polynomial: $P(x) = p_r x^r + \cdots + p_0$ splits over $\overline{\mathbb{K}}$

$$P(x) = p_r (x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k}, \quad \alpha_i \in \overline{\mathbb{K}}, m_i \in \mathbb{N}^\star,$$

▷ $V(L)$ is generated (over $\overline{\mathbb{K}}$) by

$$\left\{ e^{\alpha_1 x}, x e^{\alpha_1 x}, \ldots, x^{m_1 - 1} e^{\alpha_1 x}, \ldots, e^{\alpha_k x}, x e^{\alpha_k x}, \ldots, x^{m_k - 1} e^{\alpha_k x} \right\},$$

where for $\alpha \in \overline{\mathbb{K}}$, we denote by $e^{\alpha x}$ the power series $\sum_{n \geq 0} \alpha^n x^n / n!$ of $\overline{\mathbb{K}}[[x]]$.

▷ GCRD and LCLM can be computed by the usual Euclidean algorithm

The case of constant coefficients

▷ Linear differential operators $L = p_r \partial^r + \cdots + p_0$ with coefficients $p_i \in \mathbb{K}$

▷ Characteristic polynomial: $P(x) = p_r x^r + \cdots + p_0$ splits over $\overline{\mathbb{K}}$

$$P(x) = p_r (x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k}, \quad \alpha_i \in \overline{\mathbb{K}}, m_i \in \mathbb{N}^\star,$$

▷ $V(L)$ is generated (over $\overline{\mathbb{K}}$) by

$$\left\{ e^{\alpha_1 x}, x e^{\alpha_1 x}, \ldots, x^{m_1 - 1} e^{\alpha_1 x}, \ldots, \; e^{\alpha_k x}, x e^{\alpha_k x}, \ldots, x^{m_k - 1} e^{\alpha_k x} \right\},$$

where for $\alpha \in \overline{\mathbb{K}}$, we denote by $e^{\alpha x}$ the power series $\sum_{n \geq 0} \alpha^n x^n / n!$ of $\overline{\mathbb{K}}[[x]]$.

▷ GCRD and LCLM can be computed by the usual Euclidean algorithm

▷ SYM can be computed by resultants: SYM(L_1, L_2)$= P_1 \oplus P_2$ if all $m_i = 1$

Exercise 2: Estimate the cost of SYM in the case of constant coefficients.

Example

```
> L1:=225*Dx^3-1375*Dx^2-2054*Dx+2088: L2:=245*Dx^2-1759*Dx-36:
> GCRD(L1,L2,[Dx,x]), LCLM(L1,L2,[Dx,x]);
```

$$\partial - \frac{36}{5}, \quad \partial^4 - \frac{2686\,\partial^3}{441} - \frac{34007\,\partial^2}{3675} + \frac{100258\,\partial}{11025} + \frac{232}{1225}$$

Example

```
> L1:=225*Dx^3-1375*Dx^2-2054*Dx+2088: L2:=245*Dx^2-1759*Dx-36:
> GCRD(L1,L2,[Dx,x]), LCLM(L1,L2,[Dx,x]);
```

$$\partial - \frac{36}{5}, \quad \partial^4 - \frac{2686\,\partial^3}{441} - \frac{34007\,\partial^2}{3675} + \frac{100258\,\partial}{11025} + \frac{232}{1225}$$

```
> gcd(L1,L2): expand(%/lcoeff(%,Dx));
> lcm(L1,L2): expand(%/lcoeff(%,Dx));
```

$$\partial - \frac{36}{5}, \quad \partial^4 - \frac{2686\,\partial^3}{441} - \frac{34007\,\partial^2}{3675} + \frac{100258\,\partial}{11025} + \frac{232}{1225}$$

Example

```
> L1:=225*Dx^3-1375*Dx^2-2054*Dx+2088: L2:=245*Dx^2-1759*Dx-36:
> GCRD(L1,L2,[Dx,x]), LCLM(L1,L2,[Dx,x]);
```

$$\partial - \frac{36}{5}, \quad \partial^4 - \frac{2686\,\partial^3}{441} - \frac{34007\,\partial^2}{3675} + \frac{100258\,\partial}{11025} + \frac{232}{1225}$$

```
> gcd(L1,L2): expand(%/lcoeff(%,Dx));
> lcm(L1,L2): expand(%/lcoeff(%,Dx));
```

$$\partial - \frac{36}{5}, \quad \partial^4 - \frac{2686\,\partial^3}{441} - \frac{34007\,\partial^2}{3675} + \frac{100258\,\partial}{11025} + \frac{232}{1225}$$

```
> symmetric_product(L1,L2,[Dx,x]);
> subs(t=Dx, resultant(subs(Dx=x,L1), subs(Dx=t-x,L2),x)):
> expand(%/lcoeff(%,Dx));
```

$$\partial^6 - \frac{74443\,\partial^5}{2205} + \frac{1909137901\,\partial^4}{4862025} - \frac{700478668231\,\partial^3}{397065375} + \frac{7570609408322\,\partial^2}{5955980625} + \frac{2240061794008\,\partial}{283618125} - \frac{1233423295936}{220591875}$$

Rational Weyl algebra is a factorization domain

Theorem [Schlesinger 1887, Beke 1894, Landau 1902, Loewy 1903]
Elements of $\mathbb{K}(x)\langle\partial\rangle$ can be expressed as products of irreducible factors.

Rational Weyl algebra is a factorization domain

Theorem [Schlesinger 1887, Beke 1894, Landau 1902, Loewy 1903]
Elements of $\mathbb{K}(x)\langle\partial\rangle$ can be expressed as products of irreducible factors.

More precisely, any $L \in \mathbb{K}(x)\langle\partial\rangle$ can be written $L = r(x) \star L_1 \star \cdots \star L_m$, where $r \in \mathbb{K}(x)$ and the L_i's are monic and irreducible in $\mathbb{K}(x)\langle\partial\rangle$.

Rational Weyl algebra is a factorization domain

Theorem [Schlesinger 1887, Beke 1894, Landau 1902, Loewy 1903]
Elements of $\mathbb{K}(x)\langle\partial\rangle$ can be expressed as products of irreducible factors.

More precisely, any $L \in \mathbb{K}(x)\langle\partial\rangle$ can be written $L = r(x) \star L_1 \star \cdots \star L_m$, where $r \in \mathbb{K}(x)$ and the L_i's are monic and irreducible in $\mathbb{K}(x)\langle\partial\rangle$.

Moreover, if $\tilde{L} = \tilde{r}(x) \star \tilde{L}_1 \star \cdots \star \tilde{L}_s$ for monic irreducible $\tilde{L}_j$ and $\tilde{r} \in \mathbb{K}(x)$, then $r = \tilde{r}$, $m = s$ and there exists $\sigma \in \mathcal{S}_m$ such that $\mathrm{ord}(\tilde{L}_j) = \mathrm{ord}(\tilde{L}_{\sigma(j)})$.

Rational Weyl algebra is a factorization domain

Theorem [Schlesinger 1887, Beke 1894, Landau 1902, Loewy 1903]
Elements of $\mathbb{K}(x)\langle\partial\rangle$ can be expressed as products of irreducible factors.

More precisely, any $L \in \mathbb{K}(x)\langle\partial\rangle$ can be written $L = r(x) \star L_1 \star \cdots \star L_m$, where $r \in \mathbb{K}(x)$ and the L_i's are monic and irreducible in $\mathbb{K}(x)\langle\partial\rangle$.

Moreover, if $\tilde{L} = \tilde{r}(x) \star \tilde{L}_1 \star \cdots \star \tilde{L}_s$ for monic irreducible $\tilde{L}_j$ and $\tilde{r} \in \mathbb{K}(x)$, then $r = \tilde{r}$, $m = s$ and there exists $\sigma \in \mathcal{S}_m$ such that $\mathrm{ord}(\tilde{L}_j) = \mathrm{ord}(\tilde{L}_{\sigma(j)})$.

▷ Right-factors of order 1 of L correspond to hyperexponential solutions of $L(y) = 0$, that is $y'(x)/y(x) \in \mathbb{K}(x)$, or $y(x) = \exp(\int r(x))$ for $r \in \mathbb{K}(x)$

Rational Weyl algebra is a factorization domain

Theorem [Schlesinger 1887, Beke 1894, Landau 1902, Loewy 1903]
Elements of $\mathbb{K}(x)\langle\partial\rangle$ can be expressed as products of irreducible factors.

More precisely, any $L \in \mathbb{K}(x)\langle\partial\rangle$ can be written $L = r(x) \star L_1 \star \cdots \star L_m$, where $r \in \mathbb{K}(x)$ and the L_i's are monic and irreducible in $\mathbb{K}(x)\langle\partial\rangle$.

Moreover, if $\tilde{L} = \tilde{r}(x) \star \tilde{L}_1 \star \cdots \star \tilde{L}_s$ for monic irreducible $\tilde{L}_j$ and $\tilde{r} \in \mathbb{K}(x)$, then $r = \tilde{r}$, $m = s$ and there exists $\sigma \in \mathcal{S}_m$ such that $\operatorname{ord}(\tilde{L}_j) = \operatorname{ord}(\tilde{L}_{\sigma(j)})$.

▷ Right-factors of order 1 of L correspond to hyperexponential solutions of $L(y) = 0$, that is $y'(x)/y(x) \in \mathbb{K}(x)$, or $y(x) = \exp(\int r(x))$ for $r \in \mathbb{K}(x)$

▷ Caution: infinitely many factorizations may exist. E.g., for any $c \in \mathbb{K}$,
$\partial \star \partial = \left(\partial + \frac{1}{x+c}\right) \star \left(\partial - \frac{1}{x+c}\right) \neq \left(\partial - \frac{1}{x+c}\right) \star \left(\partial + \frac{1}{x+c}\right) = \partial^2 - \frac{2}{(x+c)^2}$.

Example

```
> with(DEtools):
> A:=(x-1)*Dx^3+(x-x^2)*Dx^2+(3-2*x)*Dx-x:
> B:=3*Dx^2+(x^3-3*x)*Dx-x^4-3:
> DFactor(A,[Dx,x]);
```

$$\left[(x-1)\left(\partial^2+(x-1)^{-1}\right),\partial-x\right]$$

Example

```
> with(DEtools):
> A:=(x-1)*Dx^3+(x-x^2)*Dx^2+(3-2*x)*Dx-x:
> B:=3*Dx^2+(x^3-3*x)*Dx-x^4-3:
> DFactor(A,[Dx,x]);
```

$$\left[(x-1)\left(\partial^2+(x-1)^{-1}\right), \partial - x\right]$$

```
> DFactor(B,[Dx,x]);
```

$$\left[3\,\partial + x^3, \partial - x\right]$$

Example

```
> with(DEtools):
> A:=(x-1)*Dx^3+(x-x^2)*Dx^2+(3-2*x)*Dx-x:
> B:=3*Dx^2+(x^3-3*x)*Dx-x^4-3:
> DFactor(A,[Dx,x]);
```

$$\left[(x-1)\left(\partial^2+(x-1)^{-1}\right),\partial-x\right]$$

```
> DFactor(B,[Dx,x]);
```

$$\left[3\,\partial+x^3,\partial-x\right]$$

```
> GCRD(A,B,[Dx,x]);
```

$$\partial-x$$

Bounds on right factors

Theorem [B., Rivoal, Salvy, 2020]
Let L have order m, degree q, height H. Let M be a monic right factor of L. Then:

$$\deg_x(M) \leq r^2(\mathcal{S}+1)\mathcal{E} + r(\mathcal{N}+1)\mathcal{S} + r\mathcal{N} + \frac{1}{2}r^2(r-1)\big((\mathcal{S}+1)(\mathcal{N}+1)-2\big),$$

where

- $r =$ the order of M;
- $\mathcal{E} =$ the largest modulus of the local generalized exponents of L at ∞ and at its finite non-apparent singularities;
- $\mathcal{N} =$ the largest slope of L at its finite singularities and at ∞;
- $\mathcal{S} =$ the number of finite non-apparent singularities of L.

▷ Previous bound [Grigoriev, 1990] was asymptotic $e^{2^{m \cdot o(2^m)}}$ as $m \to +\infty$

Theorem [B., Rivoal, Salvy, 2020]
Let L have order m, degree q, height H. Let M be a monic right factor of L. Then:

$$\deg_x(M) \leq r^2(\mathcal{S}+1)\mathcal{E} + r(\mathcal{N}+1)\mathcal{S} + r\mathcal{N} + \frac{1}{2}r^2(r-1)\big((\mathcal{S}+1)(\mathcal{N}+1)-2\big),$$

where

- $r \leq m$;
- $\mathcal{N} \leq m+q$;
- $\mathcal{S} \leq q$;
- $\mathcal{E} \leq 2^{(36(q+1)m)^{9(q+1)^2 m^{3m}}} H^{(5(q+1)m)^{9(q+1)^2 m^{3m}}}$.

▷ Previous bound [Grigoriev, 1990] was asymptotic $e^{2^{m \cdot o(2^m)}}$ as $m \to +\infty$

Not just bounds: Factors can really be big

The second-order operator

$$L := x\partial^2 + (2-x)\partial + N$$

admits the right factor of order 1 and degree N

$$M = \partial - \frac{H'(x)}{H(x)}, \quad \text{where } H(x) = {}_1F_1(-N;2;x) = \sum_{\ell=0}^{N} \binom{N}{\ell} \frac{(-x)^\ell}{(\ell+1)!}.$$

Not just bounds: Factors can really be big

The second-order operator

$$L := x\partial^2 + (2 - x)\partial + N$$

admits the right factor of order 1 and degree N

$$M = \partial - \frac{H'(x)}{H(x)}, \quad \text{where } H(x) = {}_1F_1(-N; 2; x) = \sum_{\ell=0}^{N} \binom{N}{\ell} \frac{(-x)^\ell}{(\ell+1)!}.$$

▷ Here, $m = 2$, $q = 1$, $r = 1$ and $\mathcal{E} = N$, $\mathcal{N} = 1$ and $\mathcal{S} = 0$.

Not just bounds: Factors can really be big

The second-order operator

$$L := x\partial^2 + (2-x)\partial + N$$

admits the right factor of order 1 and degree N

$$M = \partial - \frac{H'(x)}{H(x)}, \quad \text{where } H(x) = {}_1F_1(-N; 2; x) = \sum_{\ell=0}^{N} \binom{N}{\ell} \frac{(-x)^\ell}{(\ell+1)!}.$$

▷ Here, $m = 2$, $q = 1$, $r = 1$ and $\mathcal{E} = N$, $\mathcal{N} = 1$ and $\mathcal{S} = 0$.

▷ The bound of [B., Rivoal, Salvy, 2020] writes $\deg_x(M) \leq N$ (optimal).

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

- Differences

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

- Differences
  - $\mathbb{K}(x)\langle\partial\rangle$ is (slightly) non-commutative

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

- Differences
  - $\mathbb{K}(x)\langle\partial\rangle$ is (slightly) non-commutative
  - Only right-factors in $\mathbb{K}(x)\langle\partial\rangle$ correspond to "solutions"

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

- Differences
  - $\mathbb{K}(x)\langle\partial\rangle$ is (slightly) non-commutative
  - Only right-factors in $\mathbb{K}(x)\langle\partial\rangle$ correspond to "solutions"
  - Minimal-order annihilating skew polynomials for a D-finite function need not be irreducible

$$L^{\min}_{\ln(1-x)} = \left(\partial + \frac{1}{x-1}\right)\partial$$

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

- Differences
  - $\mathbb{K}(x)\langle\partial\rangle$ is (slightly) non-commutative
  - Only right-factors in $\mathbb{K}(x)\langle\partial\rangle$ correspond to "solutions"
  - Minimal-order annihilating skew polynomials for a D-finite function need not be irreducible $\qquad L^{\min}_{\ln(1-x)} = \left(\partial + \frac{1}{x-1}\right)\partial$
  - GCRDs and LCLMs in $\mathbb{K}(x)\langle\partial\rangle$ not always visible on factorizations

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

- Differences
  - $\mathbb{K}(x)\langle\partial\rangle$ is (slightly) non-commutative
  - Only right-factors in $\mathbb{K}(x)\langle\partial\rangle$ correspond to "solutions"
  - Minimal-order annihilating skew polynomials for a D-finite function need not be irreducible $\quad L^{\min}_{\ln(1-x)} = \left(\partial + \frac{1}{x-1}\right)\partial$
  - GCRDs and LCLMs in $\mathbb{K}(x)\langle\partial\rangle$ not always visible on factorizations
  - Factorization in $\mathbb{K}(x)\langle\partial\rangle$ is not unique

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

- Differences
  - $\mathbb{K}(x)\langle\partial\rangle$ is (slightly) non-commutative
  - Only right-factors in $\mathbb{K}(x)\langle\partial\rangle$ correspond to "solutions"
  - Minimal-order annihilating skew polynomials for a D-finite function need not be irreducible $\quad L^{\min}_{\ln(1-x)} = \left(\partial + \frac{1}{x-1}\right)\partial$
  - GCRDs and LCLMs in $\mathbb{K}(x)\langle\partial\rangle$ not always visible on factorizations
  - Factorization in $\mathbb{K}(x)\langle\partial\rangle$ is not unique
  - Worse, degrees on factors of $L \in \mathbb{K}(x)\langle\partial\rangle$ depend on the bit-size of L, not only on its order/degree

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

- Differences
  - $\mathbb{K}(x)\langle\partial\rangle$ is (slightly) non-commutative
  - Only right-factors in $\mathbb{K}(x)\langle\partial\rangle$ correspond to "solutions"
  - Minimal-order annihilating skew polynomials for a D-finite function need not be irreducible $\qquad L^{\min}_{\ln(1-x)} = \left(\partial + \frac{1}{x-1}\right)\partial$
  - GCRDs and LCLMs in $\mathbb{K}(x)\langle\partial\rangle$ not always visible on factorizations
  - Factorization in $\mathbb{K}(x)\langle\partial\rangle$ is not unique
  - Worse, degrees on factors of $L \in \mathbb{K}(x)\langle\partial\rangle$ depend on the bit-size of L, not only on its order/degree
  - Worse, degrees on factors are not polynomially bounded (!)

Polynomials and skew polynomials: analogies and differences

$$\mathbb{K}(x)[y] \quad \text{versus} \quad \mathbb{K}(x)\langle\partial\rangle$$

- Analogies
  - Both are (effective) algebras: addition, multiplication
  - Both are Euclidean: (effective) division with quotient and remainder
  - In both cases, there are polynomial time algorithms for algebra and Euclidean operations
  - Both are (effective) factorization domains, e.g. when $\mathbb{K} = \mathbb{Q}$
  - In both cases, irreducibility and factoring are decidable

- Differences
  - $\mathbb{K}(x)\langle\partial\rangle$ is (slightly) non-commutative
  - Only right-factors in $\mathbb{K}(x)\langle\partial\rangle$ correspond to "solutions"
  - Minimal-order annihilating skew polynomials for a D-finite function need not be irreducible $\qquad L^{\min}_{\ln(1-x)} = \left(\partial + \frac{1}{x-1}\right)\partial$
  - GCRDs and LCLMs in $\mathbb{K}(x)\langle\partial\rangle$ not always visible on factorizations
  - Factorization in $\mathbb{K}(x)\langle\partial\rangle$ is not unique
  - Worse, degrees on factors of $L \in \mathbb{K}(x)\langle\partial\rangle$ depend on the bit-size of L, not only on its order/degree
  - Worse, degrees on factors are not polynomially bounded (!)
  - Factoring in $\mathbb{K}(x)\langle\partial\rangle$ is much more difficult than in $\mathbb{K}(x)[y]$.

Main results (balanced case)

$$W_{n,n} = \text{ set of operators in } \mathbb{K}[x]\langle\partial\rangle \text{ with } \operatorname{ord} < n, \deg < n$$

Theorem [Hoeven'02; B.'03; B.-Chyzak-Li-Salvy'12; Hoeven'16]
One can compute — output (ord, deg)

- MUL in $W_{n,n}$ in $O(n^\omega)$ ops. in $\mathbb{K}$ — $(O(n), O(n))$
- GCRD in $W_{n,n}$ in $\tilde{O}(n^{\omega+1})$ ops. in $\mathbb{K}$ — $(O(n), O(n^2))$
- LCLM in $W_{n,n}$ in $\tilde{O}(n^{\omega+1})$ ops. in $\mathbb{K}$ — $(O(n), O(n^2))$
- REM in $W_{n,n}$ in $\tilde{O}(n^{\omega+1})$ ops. in $\mathbb{K}$ — $(O(n), O(n^2))$
- SYM in $W_{n,n}$ in $\tilde{O}(n^{2\omega+3})$ ops. in $\mathbb{K}$ — $(O(n^2), O(n^4))$

▷ Algorithms + Bounds + Complexity follow 2 distinct lines of thoughts:

- reduction to (polynomial) linear algebra
- reduction to fast skew multiplication

▷ FACTOR: $(N\mathcal{L})^{O(n^4)}$, with $\mathcal{L} = \text{bitsize}(L)$ and $N \leq e^{(\mathcal{L}\cdot 2^n)^{2^n}}$ [Grigoriev'90]

Degree bounds are (generically) reached

```
> for n from 1 to 8 do
>  A1:=add(randpoly(x,degree=n,dense)*Dx^i, i=0..n);
>  A2:=add(randpoly(x,degree=n,dense)*Dx^i, i=0..n);
>  L:=LCLM(A1,A2,[Dx,x]);
>  LL:=mult(denom(L), L, [Dx,x]):
>  print(n, [degree(LL,Dx),degree(LL,x)]);
> od:
```

$$
\begin{array}{ll}
1, & [2,4] \\
2, & [4,12] \\
3, & [6,24] \\
4, & [8,40] \\
5, & [10,60] \\
6, & [12,84] \\
7, & [14,112] \\
8, & [16,144]
\end{array}
$$

Degree bounds are (generically) reached

```
> for n from 1 to 8 do
>  A1:=add(randpoly(x,degree=n,dense)*Dx^i, i=0..n);
>  A2:=add(randpoly(x,degree=n,dense)*Dx^i, i=0..n);
>  L:=LCLM(A1,A2,[Dx,x]);
>  LL:=mult(denom(L), L, [Dx,x]):
>  print(n, [degree(LL,Dx),degree(LL,x)]);
> od:
```

$$
\begin{array}{ll}
1, & [2,4] \\
2, & [4,12] \\
3, & [6,24] \\
4, & [8,40] \\
5, & [10,60] \\
6, & [12,84] \\
7, & [14,112] \\
8, & [16,144]
\end{array}
$$

▷ Bounds for LCLM in $W_{n,n}$ can be read off: $(2n, 2n(n+1))$

Main results (unbalanced case)

$$W_{r,d} = \text{ set of operators in } \mathbb{K}[x]\langle\partial\rangle \text{ with } \text{ord} < r, \deg < d,$$

Theorem [B.'03; B.-Chyzak-Li-Salvy'12; Benoit-B.-Hoeven'12; Hoeven'16]

One can compute — output (ord, deg)

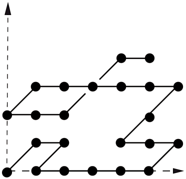
- MUL in $W_{r,d}$ in $O(dr \cdot \min(r,d)^{\omega-2})$ ops. in $\mathbb{K}$ — $(O(r), O(d))$
- GCRD in $W_{r,d}$ in $\tilde{O}(r^\omega d)$ ops. in $\mathbb{K}$ — $(O(r), O(rd))$
- LCLM in $W_{r,d}$ in $\tilde{O}(r^\omega d)$ ops. in $\mathbb{K}$ — $(O(r), O(rd))$
- REM in $W_{r,d}$ in $\tilde{O}(r^\omega d)$ ops. in $\mathbb{K}$ — $(O(r), O(rd))$
- SYM in $W_{r,d}$ in $\tilde{O}(r^{\omega+3} d^\omega)$ ops. in $\mathbb{K}$ — $(O(rd), O(r^3 d))$

▷ Algorithms + Bounds + Complexity follow 2 distinct lines of thoughts:

- reduction to (polynomial) linear algebra
- reduction to fast skew multiplication

▷ FACTOR: $(N\mathcal{L})^{O(r^4)}$, with $\mathcal{L} = \text{bitsize}(L)$ and $N \le e^{(\mathcal{L}\cdot 2^r)^{2^r}}$ [Grigoriev'90]

- $g(n)$ = number of n-steps $\{\nearrow, \swarrow, \leftarrow, \rightarrow\}$-walks in $\mathbb{N}^2$
  $1, 2, 7, 21, 78, 260, 988, 3458, 13300, 47880, \ldots$



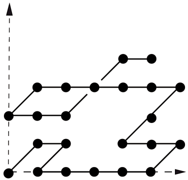
Question: What is the nature of the generating function

$$G(t) = \sum_{n=0}^{\infty} g(n)\, t^n \ ?$$

- $g(i,j;n)$ = number of n-steps $\{\nearrow, \swarrow, \leftarrow, \rightarrow\}$-walks in $\mathbb{N}^2$ from $(0,0)$ to (i,j)

Question: What is the nature of the generating function

$$G(x,y;t) = \sum_{i,j,n=0}^{\infty} g(i,j;n)\, x^i y^j t^n \ ?$$

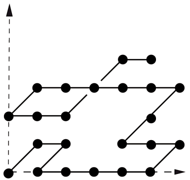


Combinatorial application: Gessel's conjecture

- $g(i,j;n)$ = number of n-steps $\{\nearrow, \swarrow, \leftarrow, \rightarrow\}$-walks in $\mathbb{N}^2$ from $(0,0)$ to (i,j)

Question: What is the nature of the generating function

$$G(x,y;t) = \sum_{i,j,n=0}^{\infty} g(i,j;n)\, x^i y^j t^n \ ?$$



Theorem [B., Kauers, 2010]

$G(x,y;t)$ is an algebraic function†.

▷ computer-driven discovery/proof via *algorithmic Guess-and-Prove*
▷ involves a LCLM computation of two 11th order (guessed) differential operators for $G(x,0;t)$, and $G(0,y;t)$.
▷ LCLM has order 20, tridegree (359,717,279) in (t,x,y), 1.5 billion coeffs

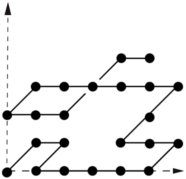
† Minimal polynomial $P(G(x,y;t);x,y,t) = 0$ has $> 10^{11}$ terms; $\approx 30\,\text{Gb}$ (6 DVDs!)

Combinatorial application: Gessel's conjecture

- $g(n)$ = number of n-steps $\{\nearrow, \swarrow, \leftarrow, \rightarrow\}$-walks in $\mathbb{N}^2$

Question: What is the nature of the generating function

$$G(t) = \sum_{n=0}^{\infty} g(n)\, t^n \;?$$

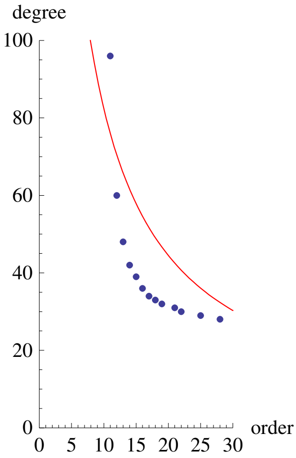


Corollary [B., Kauers, 2010] (former conjecture of Gessel's)

$(3n+1)\, g(2n) = (12n+2)\, g(2n-1)$ and $(n+1)\, g(2n+1) = (4n+2)\, g(2n)$

▷ involves a LCLM computation of two 11th order (guessed) differential operators for $G(x,0;t)$, and $G(0,y;t)$.
▷ LCLM has order 20, tridegree (359,717,279) in (t,x,y), 1.5 billion coeffs

Application to differential guessing



1000 terms of $G(x, 0; t)$ are enough to guess candidates differential equations below the red curve. GCRD of candidates could jump above the red curve.

Application to number theory

Def: p-curvature $\mathbf{A}_p(L)$ = the matrix in $\mathscr{M}_r(\mathbb{K}(x))$ whose (i,j) entry is the coefficient of ∂^i in ∂^{p+j} rmod L for $0 \leq i, j < r$

Application to number theory

Def: p-curvature $\mathbf{A}_p(L)$ = matrix of ∂^p modulo L (*"diff. Frobenius map"*)

Grothendieck's conjecture ('70s) $\Gamma \in \mathbb{Q}[x]\langle\partial\rangle$ has a basis of algebraic solutions over $\mathbb{Q}(x)$ if and only if $\mathbf{A}_p(\Gamma \bmod p)$ is zero for almost all primes p.

▷ Proved by [Katz 1982] for *Picard-Fuchs operators*; widely open in general.

Application to number theory

Def: p-curvature $\mathbf{A}_p(L)$ = matrix of ∂^p modulo L (*"diff. Frobenius map"*)

Grothendieck's conjecture ('70s) $\Gamma \in \mathbb{Q}[x]\langle\partial\rangle$ has a basis of algebraic solutions over $\mathbb{Q}(x)$ if and only if $\mathbf{A}_p(\Gamma \bmod p)$ is zero for almost all primes p.

▷ Proved by [Katz 1982] for *Picard-Fuchs operators*; widely open in general.

```
> holexprtodiffeq(hypergeom([1/9,4/9,7/9], [1/3, 2/3], x), y(x))[1]:
> L:=de2diffop(%, y(x), [Dx,x]);
```

$$\left(729\,x^3 - 729\,x^2\right)\partial^3 + \left(3159\,x^2 - 1458\,x\right)\partial^2 + (2052\,x - 162)\,\partial + 28$$

Application to number theory

Def: p-curvature $\mathbf{A}_p(L)$ = matrix of ∂^p modulo L (*"diff. Frobenius map"*)

Grothendieck's conjecture ('70s) $\Gamma \in \mathbb{Q}[x]\langle\partial\rangle$ has a basis of algebraic solutions over $\mathbb{Q}(x)$ if and only if $\mathbf{A}_p(\Gamma \bmod p)$ is zero for almost all primes p.

▷ Proved by [Katz 1982] for *Picard-Fuchs operators*; widely open in general.

```
> holexprtodiffeq(hypergeom([1/9,4/9,7/9], [1/3, 2/3], x), y(x))[1]:
> L:=de2diffop(%, y(x), [Dx,x]);
```

$$\left(729\,x^3 - 729\,x^2\right)\,\partial^3 + \left(3159\,x^2 - 1458\,x\right)\,\partial^2 + (2052\,x - 162)\,\partial + 28$$

```
> p:=7; for j to 3 do N:=rightdivision(Dx^p,L,[Dx,x])[2] mod p;
> p:=nextprime(p); print(p, N); od:
```

$$11, 0$$
$$13, 0$$
$$17, 0$$
$$19, 0$$
$$23, 0$$

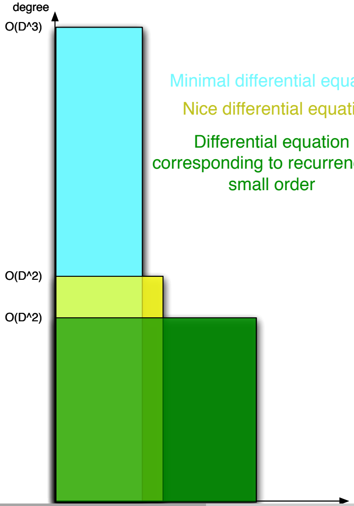
Bonus: sizes of differential equations for algebraic series

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

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

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

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

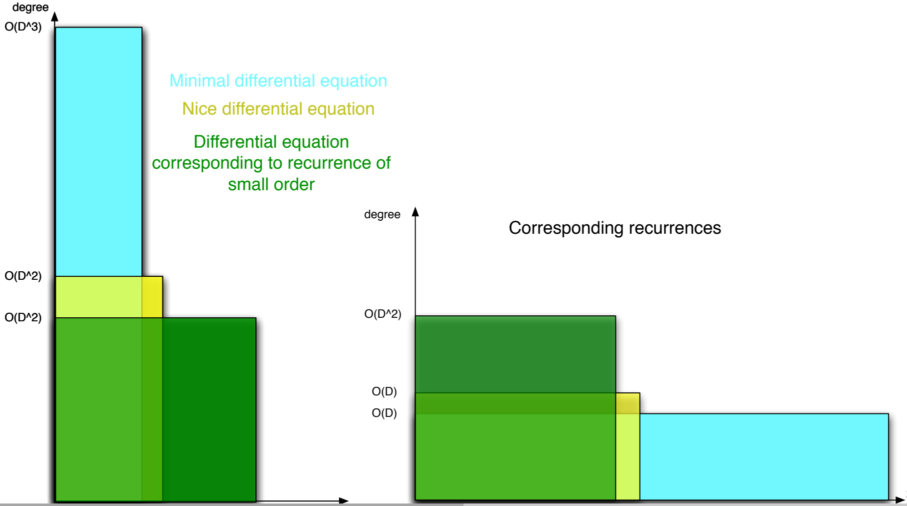


Theorem [Abel 1827, Cockle 1860, Harley 1862] Algebraic series are D-finite

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

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

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



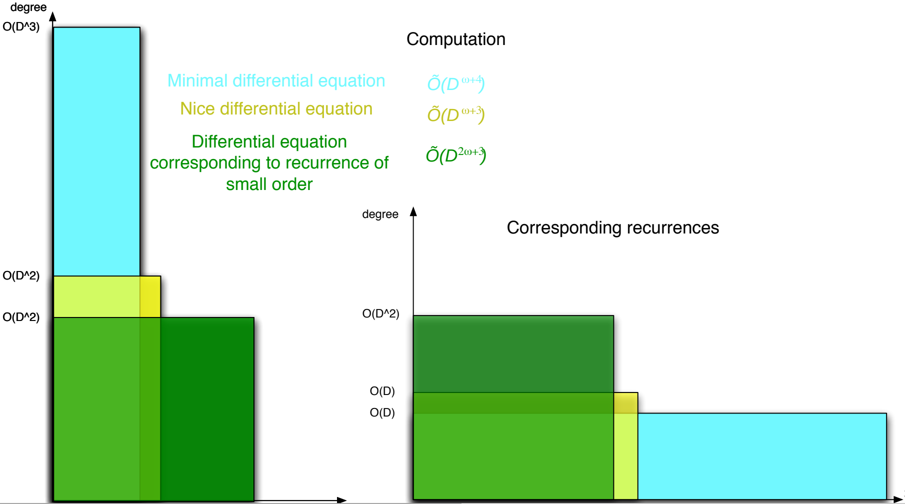
Bonus: sizes of differential equations for algebraic series

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

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

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

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



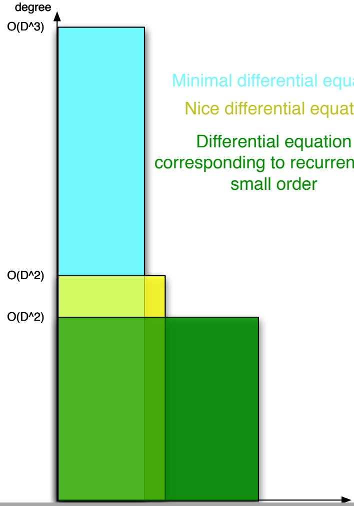
Theorem [Abel 1827, Cockle 1860, Harley 1862] Algebraic series are D-finite

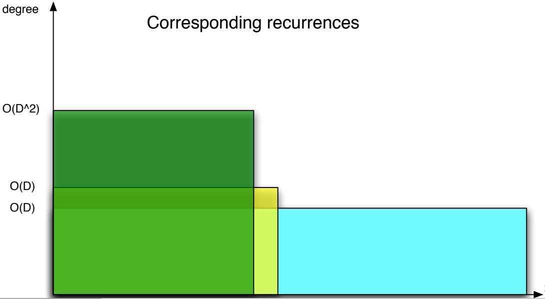
$$f \in \mathbb{Q}[[t]], \quad P(t, f(t)) = 0 \text{ with } \deg P = D$$

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	$\tilde{O}(D^{2\omega+3})$	$\tilde{O}(M(D^2) N)$





Exercises for next week

Exercise 1: Prove that L admits at most $r = \operatorname{ord}(L)$ linearly independent solutions (over C). Hint: use Wronskians.

Exercise 2: Estimate the cost of SYM in the case of constant coefficients.

Exercise 3: Assume that the LCLM of A, B in $W_{n,n}$ is computed using the algorithm from last time (closure of D-finite functions with respect to $+$).

- Estimate the size and the degree of the polynomial matrix;
- Deduce a bound on the degrees of LCLM(A, B);
- Estimate the complexity of computing LCLM(A, B) by this method.