A taste of bivariate resultant

September 28th, 2020

Overview

Bivariate resultant

See also September 14th lesson

$p, q \in \mathsf{K}[x]$, of degree n and m

$$\begin{aligned} \phi : \quad & \mathsf{K}[x] \times \mathsf{K}[x] \to \mathsf{K}[x] \\ & (u, v) \mapsto up + vq \end{aligned}$$

$\mathsf{K}_n[x]$ the polynomials of degree less than n

$$\begin{aligned} \varphi : \quad & \mathsf{K}_m[x] \times \mathsf{K}_n[x] \to \mathsf{K}_{n+m}[x] \\ & (u, v) \mapsto up + vq \end{aligned}$$

$p, q \in \mathsf{K}[x]$, of degree n and m

$$\begin{aligned} \phi : \quad & \mathsf{K}[x] \times \mathsf{K}[x] \to \mathsf{K}[x] \\ & (u, v) \mapsto up + vq \end{aligned}$$

$\mathsf{K}_n[x]$ the polynomials of degree less than n

$$\begin{aligned} \varphi : \quad & \mathsf{K}_m[x] \times \mathsf{K}_n[x] \to \mathsf{K}_{n+m}[x] \\ & (u, v) \mapsto up + vq \end{aligned}$$

Theorem: φ si an isomorphism if and only if $\gcd(p, q) = 1$

$p, q \in \mathsf{K}[x]$, of degree n and m

$$\varphi : \quad \mathsf{K}_m[x] \times \mathsf{K}_n[x] \to \mathsf{K}_{n+m}[x]$$
$$(u, v) \mapsto up + vq$$

Basis for $\mathsf{K}_m[x] \times \mathsf{K}_n[x]$: $(x^i, 0)$ for $0 \leq i < m$ and $(0, x^j)$ for $0 \leq j < n$ and

Basis for $\mathsf{K}_{n+m}[x]$: x^l for $0 \leq l < n + m$

Entries in K

$p, q \in \mathsf{K}[x]$

$\deg p, q = n$

Sylvester matrix

$$S = \begin{bmatrix} p_n & & & & q_n & & & \\ p_{n-1} & p_n & & & q_{n-1} & q_n & & \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\ \vdots & \vdots & & p_n & \vdots & \vdots & & q_n \\ p_0 & \vdots & & p_{n-1} & q_0 & \vdots & & q_{n-1} \\ & p_0 & & \vdots & & q_0 & & \vdots \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & p_0 & & & & q_0 \end{bmatrix} \in \mathsf{K}^{2n \times 2n}$$

$\longrightarrow$ $\mathrm{Res}(p, q) = \det S \in \mathsf{K}$?

```
> p1:=randpoly(x,degree=n) mod q;
```

$$p1 := 70\,x^4 + 28\,x^3 + 52\,x^2 + 69\,x + 47$$

```
>
> p2:=randpoly(x,degree=n) mod q;
```

$$p2 := 70\,x^4 + 27\,x^3 + 59\,x^2 + 51\,x + 3$$

```
>
>
> S:=Transpose(SylvesterMatrix(p1,p2,x));
```

$$S := \begin{bmatrix} 70 & 0 & 0 & 0 & 70 & 0 & 0 & 0 \\ 28 & 70 & 0 & 0 & 27 & 70 & 0 & 0 \\ 52 & 28 & 70 & 0 & 59 & 27 & 70 & 0 \\ 69 & 52 & 28 & 70 & 51 & 59 & 27 & 70 \\ 47 & 69 & 52 & 28 & 3 & 51 & 59 & 27 \\ 0 & 47 & 69 & 52 & 0 & 3 & 51 & 59 \\ 0 & 0 & 47 & 69 & 0 & 0 & 3 & 51 \\ 0 & 0 & 0 & 47 & 0 & 0 & 0 & 3 \end{bmatrix}$$

```
>
```

```
> p1:=randpoly(x,degree=n) mod q;
```

$$p1 := 70\,x^4 + 28\,x^3 + 52\,x^2 + 69\,x + 47$$

```
>
> p2:=randpoly(x,degree=n) mod q;
```

$$p2 := 70\,x^4 + 27\,x^3 + 59\,x^2 + 51\,x + 3$$

```
>
>
> S:=Transpose(SylvesterMatrix(p1,p2,x));
```

$$S := \begin{bmatrix} 70 & 0 & 0 & 0 & 70 & 0 & 0 & 0 \\ 28 & 70 & 0 & 0 & 27 & 70 & 0 & 0 \\ 52 & 28 & 70 & 0 & 59 & 27 & 70 & 0 \\ 69 & 52 & 28 & 70 & 51 & 59 & 27 & 70 \\ 47 & 69 & 52 & 28 & 3 & 51 & 59 & 27 \\ 0 & 47 & 69 & 52 & 0 & 3 & 51 & 59 \\ 0 & 0 & 47 & 69 & 0 & 0 & 3 & 51 \\ 0 & 0 & 0 & 47 & 0 & 0 & 0 & 3 \end{bmatrix}$$

```
>
```

```
>
> alpha:=-S[1,1]/S[1,n+1];
```

$$\alpha := -1$$

```
> for j from 1 to n do S:=map(t->t mod q, ColumnOperation(S,[j,j+n],alpha)): od: S;
>
```

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 70 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 27 & 70 & 0 & 0 \\ 64 & 1 & 0 & 0 & 59 & 27 & 70 & 0 \\ 18 & 64 & 1 & 0 & 51 & 59 & 27 & 70 \\ 44 & 18 & 64 & 1 & 3 & 51 & 59 & 27 \\ 0 & 44 & 18 & 64 & 0 & 3 & 51 & 59 \\ 0 & 0 & 44 & 18 & 0 & 0 & 3 & 51 \\ 0 & 0 & 0 & 44 & 0 & 0 & 0 & 3 \end{bmatrix}$$

```
>
> p3:=Rem(p1,p2,x) mod q;
```

$$p3 := x^3 + 64\,x^2 + 18\,x + 44$$

```
>
>
```

```
>
> alpha:=-S[1,1]/S[1,n+1];
```

$$\alpha := -1$$

```
> for j from 1 to n do S:=map(t->t mod q, ColumnOperation(S,[j,j+n],alpha)): od: S;
>
```

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 70 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 27 & 70 & 0 & 0 \\ 64 & 1 & 0 & 0 & 59 & 27 & 70 & 0 \\ 18 & 64 & 1 & 0 & 51 & 59 & 27 & 70 \\ 44 & 18 & 64 & 1 & 3 & 51 & 59 & 27 \\ 0 & 44 & 18 & 64 & 0 & 3 & 51 & 59 \\ 0 & 0 & 44 & 18 & 0 & 0 & 3 & 51 \\ 0 & 0 & 0 & 44 & 0 & 0 & 0 & 3 \end{bmatrix}$$

```
>
> p3:=Rem(p1,p2,x) mod q;
```

$$p3 := x^3 + 64\,x^2 + 18\,x + 44$$

```
>
>
```

```
>
> alpha:=-S[2,n+2]/S[2,1];
```

$$\alpha := -70$$

```
> for j from 1 to n-1 do S:=map(t->t mod q, ColumnOperation(S,[j+n+1,j],alpha)): od: S;
```

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 70 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 27 & 0 & 0 & 0 \\ 64 & 1 & 0 & 0 & 59 & 20 & 0 & 0 \\ 18 & 64 & 1 & 0 & 51 & 6 & 20 & 0 \\ 44 & 18 & 64 & 1 & 3 & 24 & 6 & 20 \\ 0 & 44 & 18 & 64 & 0 & 3 & 24 & 6 \\ 0 & 0 & 44 & 18 & 0 & 0 & 3 & 24 \\ 0 & 0 & 0 & 44 & 0 & 0 & 0 & 3 \end{bmatrix}$$

```
> alpha:=-S[3,n+2]/S[3,2];
```

$$\alpha := -20$$

```
> for j from 2 to n do S:=map(t->t mod q, ColumnOperation(S,[j+n,j],alpha)): od: S;
```

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 70 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 27 & 0 & 0 & 0 \\ 64 & 1 & 0 & 0 & 59 & 0 & 0 & 0 \\ 18 & 64 & 1 & 0 & 51 & \boxed{4} & 0 & 0 \\ 44 & 18 & 64 & 1 & 3 & 19 & 4 & 0 \\ 0 & 44 & 18 & 64 & 0 & 46 & 19 & 4 \\ 0 & 0 & 44 & 18 & 0 & 0 & 46 & 19 \\ 0 & 0 & 0 & 44 & 0 & 0 & 0 & 46 \end{bmatrix}$$

```
>
>
>
> Rem(p2,p3,x) mod q;
```

$$\boxed{4x^2 + 19x + 46}$$

Resultant algorithm à la Euclid

$p(x)$ and $q(x)$ of degree m and n

Euclidean division: $p(x) = u(x)q(x) + r(x)$, with $\deg r = d$

$$\text{Res}(p, q) = (-1)^{mn} q_n^{m-d} \,\text{Res}(q, r)$$

Entries in K

$p, q \in \mathsf{K}[x]$

$\deg p, q = n$

Sylvester matrix

$$S = \begin{bmatrix} p_n & & & & q_n & & & \\ p_{n-1} & p_n & & & q_{n-1} & q_n & & \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\ \vdots & \vdots & & p_n & \vdots & \vdots & & q_n \\ p_0 & \vdots & & p_{n-1} & q_0 & \vdots & & q_{n-1} \\ & p_0 & & \vdots & & q_0 & & \vdots \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & p_0 & & & & q_0 \end{bmatrix} \in \mathsf{K}^{2n \times 2n}$$

$\longrightarrow$ $\mathrm{Res}(p, q) = \det S \in \mathsf{K}$?

Knuth-Schönhage-Moenck recursive polynomial gcd: $\tilde{O}(n)$ operations

Elimination property

R an integral domain, $p, q \in \mathrm{R}[x]$ non zero

Theorem: There exist non zero u an v in $\mathrm{R}[x]$ such that

$$u(x)p(x) + v(x)q(x) = \mathrm{Res}(p, q), \ \ \deg u < \deg q, \ \ \deg v < \deg p$$

Elimination property

$p(x, y), q(x, y)$ seen as polynomial in $(\mathsf{K}(x))[y]$

$r(x) = \mathrm{Res}_y(p(x, y), q(x, y))$

There exist non zero u and v in $\mathsf{K}[x, y]$ such that

$$u(x, y)p(x, y) + v(x, y)q(x, y) = r(x)$$

Hint: see the relation over $\mathsf{K}(x)$ and multiply by a common denominator

$= 0$ or linear system with the Sylvester matrix and Cramers' rule

Entries in K[x]

$p, q \in \mathsf{K}[x, y] \qquad \deg_x = 1,\ \deg_y = n$

$$S(x) = \begin{bmatrix} p_n(x) & & & & q_n(x) & & & \\ p_{n-1}(x) & p_n(x) & & & q_{n-1}(x) & q_n(x) & & \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\ \vdots & \vdots & & p_n(x) & \vdots & \vdots & & q_n(x) \\ p_0(x) & \vdots & & p_{n-1}(x) & q_0(x) & \vdots & & q_{n-1}(x) \\ & p_0(x) & & \vdots & & q_0(x) & & \vdots \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & p_0(x) & & & & q_0(x) \end{bmatrix} \in \mathsf{K}[x]^{2n \times 2n}$$

$\det S(x)$?

Output degree: $2n$

$2n$ *points* $\Longrightarrow$ $\tilde{O}(n \times n)$

Rule of thumb:

$$\text{Cost over } \mathsf{K}[x] \preceq \text{Cost over } \mathsf{K} \times \text{Output degree}$$

(Evaluation-interpolation scheme)

?

Rule of thumb:

Cost over $\mathsf{K}[x]$ $\preceq$ Cost over K $\times$ Output degree

(Evaluation-interpolation scheme)

The difficulty

Tool 1: **Structure that is kept recursively**

Tool 2: **Minimal bases for mastering the degrees, recursively**

Tool 1: **Structure that is kept recursively**

Tool 2: **Minimal bases for mastering the degrees, recursively**

$\rightsquigarrow$ **It is unknown how to combine those tools “optimally”**

However, one may split the difference ...

Another determinant approach?

Simplified problem

Bivariate resultant $\equiv$ determinant of a polynomial quasi-Toeplitz (Sylvester) matrix

$$\downarrow$$

Determinant of $(A - x)$ for A Toeplitz

Why?

$$(A - x)^{-1} = \sum_{k \geq 0} (A^{-1})^k x^k = \sum_{i \geq 0} \frac{1}{x^{i+1}} A^i$$

$\rightsquigarrow$ **One can compute a truncated expansion fast**

then recover the determinant

Why?

$$(A - x)^{-1} = \sum_{k \geq 0} (A^{-1})^k x^k = \sum_{i \geq 0} \frac{1}{x^{i+1}} A^i$$

$\rightsquigarrow$ **One can compute a truncated expansion fast**

then recover the determinant

- Lifting approach
- Krylov subspace approach

Expansion at zero: lifting

$$(A - x)^{-1} = \sum_{k \geq 0} (A^{-1})^k$$

Newton-iterative system solution

[Lipson 1969] [Moenck, Carter 1979] [Dixon 1982]

$$A \in \mathsf{K}[x]^{n\times n}$$

1. First terms of the solution $A^{-1}(x)b(x) = s_0(x) \mod x^d$

2. Residue $b(x) - A(x)s_0(x) = x^d r_1(x)$

3. Next terms of the solution $A^{-1}b = s_0 + (A^{-1}r_1)x^d + \dots$

....

Newton-iterative system solution

[Lipson 1969] [Moenck, Carter 1979] [Dixon 1982]

$$A \in \mathsf{K}[x]^{n \times n}$$

1. First terms of the solution $A^{-1}(x)b(x) = s_0(x) \mod x^d$

2. Residue $b(x) - A(x)s_0(x) = x^d r_1(x)$

3. Next terms of the solution $A^{-1}b = s_0 + (A^{-1}r_1)x^d + \dots$

....

Newton-iterative system solution

[Lipson 1969] [Moenck, Carter 1979] [Dixon 1982]

$$A \in \mathsf{K}[x]^{n \times n}$$

1. First terms of the solution $\quad A^{-1}(x)b(x) = s_0(x) \mod x^d$

2. Residue $\quad b(x) - A(x)s_0(x) = x^d r_1(x)$

3. Next terms of the solution $\quad A^{-1}b = s_0 + (A^{-1}r_1)x^d + \dots$

....

[Storjohann 2003]

Lifting approach (Krylov after linearization)

Linear system $A(x)u(x) = b(x)$, $n \times n$ of degree d:

$$A(x)^{-1}b(x) = C(x)\sum_{i\geq 0}\varphi^i(b)X^{i+1}$$

for a well chosen operator φ (linear in K^{nd})

Expansion at infinity: Krylov

$$(A - x)^{-1} = \sum_{i \geq 0} \frac{1}{x^{i+1}} A^i$$

Krylov-Wiedemann subspace method

Ex: **Characteristic polynomial** (Cayley-Hamilton theorem)
(Generic case)

$$I, A, \ldots, A^{n-1}, A^n$$

The relation gives

$$p_A(x) = p_0 + p_1 x + \ldots + p_{n-1} x^{n-1} + x^n$$

$$\downarrow$$

$$\det A$$

Krylov-Wiedemann subspace method

Ex: **Characteristic polynomial** (Cayley-Hamilton theorem)
(Generic case)

$$I, A, \ldots, A^{n-1}, A^n$$

$$b, Ab, \ldots, A^{n-1}b, A^n b$$

The relation gives

$$p_A(x) = p_0 + p_1 x + \ldots + p_{n-1}x^{n-1} + x^n$$

$$\downarrow$$

$$\det A$$

Krylov-Wiedemann subspace method

Ex: **Characteristic polynomial** (Cayley-Hamilton theorem)
(Generic case)

$$I, A, \ldots, A^{n-1}, A^n$$

The relation gives

$$p_A(x) = p_0 + p_1 x + \ldots + p_{n-1}x^{n-1} + x^n$$

$$\downarrow$$

$$\det A$$

$$b, Ab, \ldots, A^{n-1}b, A^n b$$

$$c^t b, c^t Ab, \ldots, c^t A^{n-1} b, c^t A^n b$$

Scalar sequence

Let’s split the difference: only one level (non recursive)

- Use of the **structure** for computing a truncated expansion
- **Minimal approximants**
- (+ Baby steps giant steps paradigm)

$$A = \begin{bmatrix} 2 & -5 & -10 & 10 & -10 & 10 & 0 & 0 & -10 & 11 \\ 2 & 11 & -5 & -12 & 6 & 4 & -11 & 2 & -11 & 8 \\ -9 & 0 & 11 & -3 & -2 & -3 & 4 & 5 & -2 & -10 \\ -1 & 8 & -4 & 5 & 1 & 3 & 11 & 10 & -6 & 11 \\ 8 & 10 & -12 & 12 & 2 & -2 & 8 & 2 & 8 & 1 \\ 7 & -7 & 4 & 5 & 7 & -10 & -5 & -2 & -5 & -11 \\ 3 & 12 & -5 & 5 & -2 & 8 & -6 & -5 & 4 & -10 \\ 12 & -3 & -2 & 8 & 1 & 0 & -6 & 6 & -2 & -9 \\ 10 & -6 & 2 & -1 & 12 & 10 & -12 & -5 & -11 & 4 \\ 10 & 2 & 3 & -5 & 6 & 1 & 0 & -7 & -12 & -12 \end{bmatrix}$$

$$A^{-1}b = \begin{bmatrix} \frac{69591193773}{203713103035} \\ \frac{97579672962}{203713103035} \\ \frac{284823690824}{203713103035} \\ \frac{29281306465}{40742620607} \\ -\frac{187605083672}{203713103035} \\ -\frac{7390918941}{203713103035} \\ -\frac{39531524706}{203713103035} \\ -\frac{28866179508}{40742620607} \\ -\frac{19372027446}{40742620607} \\ \frac{35285114899}{203713103035} \end{bmatrix}$$

Determinant ?

Cramer's rule: $\det A = -\,20371310335$

$$A = \begin{bmatrix} 2 & -5 & -10 & 10 & -10 & 10 & 0 & 0 & -10 & 11 \\ 2 & 11 & -5 & -12 & 6 & 4 & -11 & 2 & -11 & 8 \\ -9 & 0 & 11 & -3 & -2 & -3 & 4 & 5 & -2 & -10 \\ -1 & 8 & -4 & 5 & 1 & 3 & 11 & 10 & -6 & 11 \\ 8 & 10 & -12 & 12 & 2 & -2 & 8 & 2 & 8 & 1 \\ 7 & -7 & 4 & 5 & 7 & -10 & -5 & -2 & -5 & -11 \\ 3 & 12 & -5 & 5 & -2 & 8 & -6 & -5 & 4 & -10 \\ 12 & -3 & -2 & 8 & 1 & 0 & -6 & 6 & -2 & -9 \\ 10 & -6 & 2 & -1 & 12 & 10 & -12 & -5 & -11 & 4 \\ 10 & 2 & 3 & -5 & 6 & 1 & 0 & -7 & -12 & -12 \end{bmatrix}$$

$$A^{-1}b = \begin{bmatrix} \frac{69591193773}{203713103035} \\ \frac{97579672962}{203713103035} \\ \frac{284823690824}{203713103035} \\ \frac{29281306465}{40742620607} \\ -\frac{187605083672}{203713103035} \\ -\frac{7390918941}{203713103035} \\ -\frac{39531524706}{203713103035} \\ -\frac{28866179508}{40742620607} \\ -\frac{19372027446}{40742620607} \\ \frac{35285114899}{203713103035} \end{bmatrix}$$

Determinant ?

Cramer's rule: $\det A = -20371310335$

What if solving a linear system has prohibitive quadratic cost ?

A few entries of a few solutions

$$A^{-1} = \begin{bmatrix}
-\frac{378816900}{3134047739} & -\frac{20495829114}{203713103035} & -\frac{67053094413}{203713103035} & \frac{9396074080}{40742620607} & -\frac{58841813322}{203713103035} & \frac{8641632698}{203713103035} & \frac{1176300782}{10721742265} & \frac{17807806326}{203713103035} & -\frac{23405165014}{203713103035} & \frac{10100538629}{203713103035} \\
-\frac{305542579}{3134047739} & -\frac{11872538116}{203713103035} & -\frac{49238615442}{203713103035} & \frac{8998738354}{40742620607} & -\frac{48926872543}{203713103035} & \frac{17364341402}{203713103035} & \frac{1603975448}{10721742265} & \frac{2562596724}{203713103035} & -\frac{20657616816}{203713103035} & \frac{1957476176}{203713103035} \\
-\frac{595667827}{3134047739} & -\frac{34850589482}{203713103035} & -\frac{93065264584}{203713103035} & \frac{16395446499}{40742620607} & -\frac{99757356861}{203713103035} & \frac{26770440759}{203713103035} & \frac{2467702816}{10721742265} & \frac{11632892698}{203713103035} & -\frac{30848462707}{203713103035} & \frac{3042447147}{203713103035} \\
-\frac{74008954}{3134047739} & -\frac{2169888633}{40742620607} & -\frac{4053804427}{40742620607} & \frac{4874154765}{40742620607} & -\frac{4349067980}{40742620607} & \frac{3634590188}{40742620607} & \frac{195062702}{2144348453} & -\frac{469567929}{40742620607} & -\frac{926331297}{40742620607} & -\frac{1221610838}{40742620607} \\
\frac{239765981}{3134047739} & \frac{17661126586}{203713103035} & \frac{60948870672}{203713103035} & -\frac{8711085182}{40742620607} & \frac{62978493878}{203713103035} & -\frac{12358170402}{203713103035} & -\frac{1419405818}{10721742265} & -\frac{12553388579}{203713103035} & \frac{31097066916}{203713103035} & -\frac{5825205336}{203713103035} \\
\frac{153069150}{3134047739} & \frac{4228351328}{203713103035} & \frac{32680318171}{203713103035} & -\frac{4551698694}{40742620607} & \frac{28277713354}{203713103035} & -\frac{20658574316}{203713103035} & -\frac{564797499}{10721742265} & \frac{130624778}{203713103035} & \frac{18915310378}{203713103035} & \frac{286984762}{203713103035} \\
\frac{86854607}{3134047739} & -\frac{64708557}{203713103035} & \frac{18276747571}{203713103035} & -\frac{2331953340}{40742620607} & \frac{21325207739}{203713103035} & -\frac{11479047526}{203713103035} & -\frac{708058399}{10721742265} & -\frac{3859090862}{203713103035} & \frac{6143195823}{203713103035} & \frac{7665741127}{203713103035} \\
\frac{84711069}{3134047739} & \frac{2041415721}{40742620607} & \frac{5533800772}{40742620607} & -\frac{3120400038}{40742620607} & \frac{4453203683}{40742620607} & -\frac{2490245417}{40742620607} & -\frac{159017671}{2144348453} & \frac{2076805993}{40742620607} & \frac{1591605402}{40742620607} & -\frac{956914256}{40742620607} \\
-\frac{115733957}{3134047739} & -\frac{916054792}{40742620607} & -\frac{1171020887}{40742620607} & -\frac{309781915}{40742620607} & -\frac{135778185}{40742620607} & -\frac{1372889107}{40742620607} & \frac{7348981}{2144348453} & \frac{809222740}{40742620607} & \frac{172501490}{40742620607} & -\frac{716590790}{40742620607} \\
-\frac{285726486}{3134047739} & -\frac{15441589322}{203713103035} & -\frac{55992257474}{203713103035} & \frac{8792979720}{40742620607} & -\frac{51532000881}{203713103035} & \frac{15442993054}{203713103035} & \frac{1128412236}{10721742265} & \frac{2784154348}{203713103035} & -\frac{17109379672}{203713103035} & -\frac{1441829408}{203713103035}
\end{bmatrix}$$

A few entries of a few solutions

$$A^{-1} = \begin{bmatrix}
-\frac{378816900}{3134047739} & -\frac{20495829114}{203713103035} & -\frac{67053094413}{203713103035} & \frac{9396074080}{40742620607} & -\frac{58841813322}{203713103035} & \frac{8641632698}{203713103035} & \frac{1176300782}{10721742265} & \frac{17807806326}{203713103035} & -\frac{23405165014}{203713103035} & \frac{10100538629}{203713103035} \\
-\frac{305542579}{3134047739} & -\frac{11872538116}{203713103035} & -\frac{49238615442}{203713103035} & \frac{8998738354}{40742620607} & -\frac{48926872543}{203713103035} & \frac{17364341402}{203713103035} & \frac{1603975448}{10721742265} & \frac{2562596724}{203713103035} & -\frac{20657616816}{203713103035} & \frac{1957476176}{203713103035} \\
-\frac{595667827}{3134047739} & -\frac{34850589482}{203713103035} & -\frac{93065264584}{203713103035} & \frac{16395446499}{40742620607} & -\frac{99757356861}{203713103035} & \frac{26770440759}{203713103035} & \frac{2467702816}{10721742265} & \frac{11632892698}{203713103035} & -\frac{30848462707}{203713103035} & \frac{3042447147}{203713103035} \\
-\frac{74008954}{3134047739} & -\frac{2169888633}{40742620607} & -\frac{4053804427}{40742620607} & \frac{4874154765}{40742620607} & -\frac{4349067980}{40742620607} & \frac{3634590188}{40742620607} & \frac{195062702}{2144348453} & -\frac{469567929}{40742620607} & -\frac{926331297}{40742620607} & -\frac{1221610838}{40742620607} \\
\frac{239765981}{3134047739} & \frac{17661126586}{203713103035} & \frac{60948870672}{203713103035} & -\frac{8711085182}{40742620607} & \frac{62978493878}{203713103035} & -\frac{12358170402}{203713103035} & -\frac{1419405818}{10721742265} & -\frac{12553388579}{203713103035} & \frac{31097066916}{203713103035} & -\frac{5825205336}{203713103035} \\
\frac{153069150}{3134047739} & \frac{4228351328}{203713103035} & \frac{32680318171}{203713103035} & -\frac{4551698694}{40742620607} & \frac{28277713354}{203713103035} & -\frac{20658574316}{203713103035} & -\frac{564797499}{10721742265} & \frac{130624778}{203713103035} & \frac{18915310378}{203713103035} & \frac{286984762}{203713103035} \\
\frac{86854607}{3134047739} & -\frac{64708557}{203713103035} & \frac{18276747571}{203713103035} & -\frac{2331953340}{40742620607} & \frac{21325207739}{203713103035} & -\frac{11479047526}{203713103035} & -\frac{708058399}{10721742265} & -\frac{3859090862}{203713103035} & \frac{6143195823}{203713103035} & \frac{7665741127}{203713103035} \\
\frac{84711069}{3134047739} & \frac{2041415721}{40742620607} & \frac{5533800772}{40742620607} & -\frac{3120400038}{40742620607} & \frac{4453203683}{40742620607} & -\frac{2490245417}{40742620607} & -\frac{159017671}{2144348453} & \frac{2076805998}{40742620607} & \frac{1591605402}{40742620607} & -\frac{956914256}{40742620607} \\
-\frac{115733957}{3134047739} & -\frac{916054792}{40742620607} & -\frac{1171020887}{40742620607} & -\frac{309781915}{40742620607} & -\frac{135778185}{40742620607} & -\frac{1372889107}{40742620607} & \frac{7348981}{2144348453} & \frac{809222740}{40742620607} & \frac{172501490}{40742620607} & -\frac{716590790}{40742620607} \\
-\frac{285726486}{3134047739} & -\frac{15441589322}{203713103035} & -\frac{55992257474}{203713103035} & \frac{8792979720}{40742620607} & -\frac{51532000881}{203713103035} & \frac{15442993054}{203713103035} & \frac{1128412236}{10721742265} & \frac{2784154848}{203713103035} & -\frac{17109379672}{203713103035} & -\frac{1441829408}{203713103035}
\end{bmatrix}$$

Step 1. $$X^T A^{-1} Y = PQ^{-1} = \begin{bmatrix} 64 & 47 & -24 & 122 \\ 20 & 36 & -36 & 140 \\ 44 & 66 & -38 & 213 \\ -13 & 18 & -3 & 66 \end{bmatrix} \begin{bmatrix} 0 & 36 & 183 & 785 \\ 363 & 319 & 379 & -41 \\ -116 & -299 & 672 & -195 \\ 382 & -387 & 0 & 344 \end{bmatrix}^{-1}$$

A few entries of a few solutions

$$A^{-1} = \begin{bmatrix}
-\frac{378816900}{3134047739} & -\frac{20495829114}{203713103035} & -\frac{67053094413}{203713103035} & \frac{9396074080}{40742620607} & -\frac{58841813322}{203713103035} & \frac{8641632698}{203713103035} & \frac{1176300782}{10721742265} & \frac{17807806326}{203713103035} & -\frac{23405165014}{203713103035} & \frac{10100538629}{203713103035} \\
-\frac{305542579}{3134047739} & -\frac{11872538116}{203713103035} & -\frac{49238615442}{203713103035} & \frac{8998738354}{40742620607} & -\frac{48926872543}{203713103035} & \frac{17364341402}{203713103035} & \frac{1603975448}{10721742265} & \frac{2562596724}{203713103035} & -\frac{20657616816}{203713103035} & \frac{1957476176}{203713103035} \\
-\frac{595667827}{3134047739} & -\frac{34850589482}{203713103035} & -\frac{93065264584}{203713103035} & \frac{16395446499}{40742620607} & -\frac{99757356861}{203713103035} & \frac{26770440759}{203713103035} & \frac{2467702816}{10721742265} & \frac{11632892698}{203713103035} & -\frac{30848462707}{203713103035} & \frac{3042447147}{203713103035} \\
-\frac{74008954}{3134047739} & -\frac{2169888633}{40742620607} & -\frac{4053804427}{40742620607} & \frac{4874154765}{40742620607} & -\frac{4349067980}{40742620607} & \frac{3634590188}{40742620607} & \frac{195062702}{2144348453} & -\frac{469567929}{40742620607} & -\frac{926331297}{40742620607} & -\frac{1221610838}{40742620607} \\
\frac{239765981}{3134047739} & \frac{17661126586}{203713103035} & \frac{60948870672}{203713103035} & -\frac{8711085182}{40742620607} & \frac{62978493878}{203713103035} & -\frac{12358170402}{203713103035} & -\frac{1419405818}{10721742265} & -\frac{12553388579}{203713103035} & \frac{31097066916}{203713103035} & -\frac{5825205336}{203713103035} \\
\frac{153069150}{3134047739} & \frac{4228351328}{203713103035} & \frac{32680318171}{203713103035} & -\frac{4551698694}{40742620607} & \frac{28277713354}{203713103035} & -\frac{20658574316}{203713103035} & -\frac{564797499}{10721742265} & \frac{130624778}{203713103035} & \frac{18915310378}{203713103035} & \frac{286984762}{203713103035} \\
\frac{86854607}{3134047739} & -\frac{64708557}{203713103035} & \frac{18276747571}{203713103035} & -\frac{2331953340}{40742620607} & \frac{21325207739}{203713103035} & -\frac{11479047526}{203713103035} & -\frac{708058399}{10721742265} & -\frac{3859090862}{203713103035} & \frac{6143195823}{203713103035} & \frac{7665741127}{203713103035} \\
\frac{84711069}{3134047739} & \frac{2041415721}{40742620607} & \frac{5533800772}{40742620607} & -\frac{3120400038}{40742620607} & \frac{4453203683}{40742620607} & -\frac{2490245417}{40742620607} & -\frac{159017671}{2144348453} & \frac{2076805998}{40742620607} & \frac{1591605402}{40742620607} & -\frac{956914256}{40742620607} \\
-\frac{115733957}{3134047739} & -\frac{916054792}{40742620607} & -\frac{1171020887}{40742620607} & -\frac{309781915}{40742620607} & -\frac{135778185}{40742620607} & -\frac{1372889107}{40742620607} & \frac{7348981}{2144348453} & \frac{809222740}{40742620607} & \frac{172501490}{40742620607} & -\frac{716590790}{40742620607} \\
-\frac{285726486}{3134047739} & -\frac{15441589322}{203713103035} & -\frac{55992257474}{203713103035} & \frac{8792979720}{40742620607} & -\frac{51532000881}{203713103035} & \frac{15442993054}{203713103035} & \frac{1128412236}{10721742265} & \frac{2784154148}{203713103035} & -\frac{17109379672}{203713103035} & -\frac{1441829408}{203713103035}
\end{bmatrix}$$

Step 1. $$X^T A^{-1} Y = PQ^{-1} = \begin{bmatrix} 64 & 47 & -24 & 122 \\ 20 & 36 & -36 & 140 \\ 44 & 66 & -38 & 213 \\ -13 & 18 & -3 & 66 \end{bmatrix} \begin{bmatrix} 0 & 36 & 183 & 785 \\ 363 & 319 & 379 & -41 \\ -116 & -299 & 672 & -195 \\ 382 & -387 & 0 & 344 \end{bmatrix}^{-1}$$

Step 2. $$\det Q = \det A = -20371310335$$

Characteristic polynomial of

$$A = \begin{bmatrix} 4 & 1 & 1 & 0 \\ 3 & 1 & 4 & 2 \\ 4 & 4 & 2 & 2 \\ 2 & 0 & 0 & 2 \end{bmatrix}$$

Characteristic polynomial of

$$A = \begin{bmatrix} 4 & 1 & 1 & 0 \\ 3 & 1 & 4 & 2 \\ 4 & 4 & 2 & 2 \\ 2 & 0 & 0 & 2 \end{bmatrix}$$

$$x - A$$

$$\det \begin{bmatrix} x-4 & -1 & -1 & 0 \\ -3 & x-1 & -4 & -2 \\ -4 & -4 & x-2 & -2 \\ -2 & 0 & 0 & x-2 \end{bmatrix} \quad n \times n$$

Characteristic polynomial of

$$A = \begin{bmatrix} 4 & 1 & 1 & 0 \\ 3 & 1 & 4 & 2 \\ 4 & 4 & 2 & 2 \\ 2 & 0 & 0 & 2 \end{bmatrix}$$

$x - A$

$$\det \begin{bmatrix} x-4 & -1 & -1 & 0 \\ -3 & x-1 & -4 & -2 \\ -4 & -4 & x-2 & -2 \\ -2 & 0 & 0 & x-2 \end{bmatrix} \quad n \times n$$

Plan A

Krylov

$$\det \; [x^4 - 9\,x^3 + 5\,x^2 + 48\,x - 96] \quad 1 \times 1$$

Characteristic polynomial of

$$A = \begin{bmatrix} 4 & 1 & 1 & 0 \\ 3 & 1 & 4 & 2 \\ 4 & 4 & 2 & 2 \\ 2 & 0 & 0 & 2 \end{bmatrix}$$

$$x - A$$

$$\det \begin{bmatrix} x-4 & -1 & -1 & 0 \\ -3 & x-1 & -4 & -2 \\ -4 & -4 & x-2 & -2 \\ -2 & 0 & 0 & x-2 \end{bmatrix} \quad n \times n$$

$$\downarrow$$

Plan K

Block Krylov

$$\det \begin{bmatrix} x^2 + 17/2\,x - 8 & \frac{71\,x}{4} - 20 \\ -9\,x - 4 & x^2 - \frac{35\,x}{2} + 2 \end{bmatrix} \quad n^\sigma \times n^\sigma$$

$$\downarrow$$

$$\det\ [x^4 - 9\,x^3 + 5\,x^2 + 48\,x - 96] \quad 1 \times 1$$

Block Krylov

$C, B \in \mathsf{K}^{n \times m}$

$C^t B, C^t AB, \ldots, C^t A^{\delta-1} B, C^t A^{\delta} B$

Block Krylov

$$C, B \in \mathsf{K}^{n\times m}$$

$$C^tB, C^tAB, \ldots, C^tA^{\delta-1}B, C^tA^{\delta}B$$

$$(C^tA^iB).M_0 + (C^tA^{i+1}B).M_1 + \ldots + (C^tA^{i+\delta}B).M_\delta$$

$M(x)$?

⇨ Minimal approximants

Block Krylov

$$C, B \in \mathsf{K}^{n\times m}$$

$$C^tB, C^tAB, \ldots, C^tA^{\delta-1}B, {\color{red}C^tA^{\delta}B}$$

Matrix fraction reconstruction

$$\sum_i (C^tA^iB)x^{-i-1} = N(x)/M(x)$$

Baby steps / giant steps

$A(x) \in \mathsf{R}[x]^{n\times n}$ $\quad\quad$ $c^t b, c^t A b, \ldots, c^t A^{n-1} b, c^t A^n b$?

$A(x) \in \mathsf{R}[x]^{n\times n}$ $\qquad c^t b, c^t Ab, \ldots, c^t A^{n-1} b, c^t A^n b$?

Baby steps

1.1. $A(x)^i b, \quad 1 \leq i \leq \sqrt{n}$

1.2. $P(x) = A(x)^{\sqrt{n}}$

$A(x) \in \mathsf{R}[x]^{n\times n}$ $c^t b, c^t Ab, \ldots, c^t A^{n-1} b, c^t A^n b$?

Baby steps 1.1. $A(x)^i b, \quad 1 \leq i \leq \sqrt{n}$

1.2. $P(x) = A(x)^{\sqrt{n}}$

Giant steps 1.3. $c^t P(x)^j, \quad 1 \leq j \leq 2\sqrt{n}$

1.4. $2n$ products $\Longrightarrow \quad \alpha_k = c^t A(x)^k b$

Relation 2. Find the linear recurrence relation for the α_k

Resultant of bivariate polynomials $\deg_x = 1,\ \deg_y = n$ Sylvester of degree one	$\tilde{O}(n^2) \longrightarrow$	$\tilde{O}(n^{1.58})$	$2 - 1/\omega$
Modular composition $\deg g = n$	$\tilde{O}(n^{1.63}) \longrightarrow$	$\tilde{O}(n^{1.46})$	$(\omega + 2)/3$
Truncated power series composition $g = y^n$	$\tilde{O}(n^{1.5}) \longrightarrow$	$\tilde{O}(n^{1.46})$	$(\omega + 2)/3$

Open problem

$\deg_x = 1, \deg_y = n$, resultant algorithm in $\tilde{O}(\mathsf{M}(n))$ arithmetic operations?