Determinant of generic polynomial structured matrices: resultant and modular composition

Work done in part with Vincent Neiger[1], Bruno Salvy, and Éric Schost

Gilles Villard

SpecFun, Saclay, April 8th, 2019

[1] See also Neiger's Grace talk, March 14, 2019, with additional practical aspects

Outline

- The problems

- Key ingredient

    - Resultant

    - Modular composition

Outline

- The problems
- Key ingredient
  - Resultant
  - Modular composition

Dense polynomial matrices : determinant

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

Degree: d

Output degree: nd

Evaluation-interpolation scheme :

Determinant in $\tilde{O}(n^{\omega} \times nd)$ operations in K

Rule of thumb:

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

(Evaluation-interpolation scheme)

Rule of thumb:

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

(Evaluation-interpolation scheme)

Dense polynomial matrices : determinant

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

Degree: d

Output degree: nd

Determinant in $O\tilde{}(n^{\omega} d) \ll O\tilde{}(n^{\omega} \times nd)$ operations in K

''Essentially'' the cost of a polynomial matrix product

[Storjohann 2003-2005]
[Labahn, Neiger, Zhou 2017]

Dense matrix fractions

Generic case

$$H(x) = P(x)Q(x)^{-1} \in \mathsf{K}[x]^{n\times n}$$

P, Q of degree d

Matrix fraction reconstruction:

Recover P, Q from $O(d)$ terms of the expansion $H(x) = \Sigma_i H_i x^i$

→ in $\tilde{O}(n^\omega d)$ operations in K

[Beckermann, Labahn 1994]
[Giorgi, Jeannerod, Villard 2003]

Structured polynomial matrices?

$A(x) \in \mathsf{K}[x]^{n\times n}$ **''structured''**

$\det\ A(x)$?

- Sylvester matrix (Toeplitz-like)
- Multiplication by $a(y)$ in $\mathsf{K}[y]/g(y)$

1. Sylvester matrix

Entries in K

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

$\deg p, q = n$

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

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

Knuth-Schönhage-Moenck recursive polynomial half-gcd

Structured determinant: $O(\mathsf{M}(n) \log n) = \tilde{O}(n)$ operations

1. Polynomial Sylvester matrix

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

$\deg_x = 1, \ \deg_y = n$

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

$\det S(x)$? Degree: $2n$

Rule of thumb $\implies \tilde{O}(n \times n) = \tilde{O}(n^2)$ operations

Best known complexity bound $\equiv$ **size of a system solution**
(n entries of degree $2n$)

2. Quotient algebra

Multiplication by $a(y)$ in $K[y]/g(y)$

$\deg g = n$

$$A : p \mapsto a \cdot p \bmod g$$

$$\begin{array}{c|ccc|}
 & a & ay & \dots & ay^{n-1} \\
\hline
1 & & & & \\
y & & & A & \\
\vdots & & & & \\
y^{n-1} & & & & \\
\hline
\end{array}
\quad \longrightarrow \quad
\begin{bmatrix} xI - A \end{bmatrix}$$

$n \times n$

Minimal polynomial ?

Characteristic polynomial generically

2. Quotient algebra

Minimal polynomial of $a(y)$ in K$[y]/g(y)$

via the projection of $1, a, a^2, \ldots, a^{2n-1}$

and Berlekamp-Massey algorithm

→ $\tilde{O}(n^2)$ operations in K

[Ly 1989] [Rifà, Borrell 1991] [Shoup 1994]

2. Quotient algebra

$h, a, g \in \mathsf{K}[y]$

Modular composition: $h(a) \bmod g$?

Modular composition $\Longrightarrow$ Minimal polynomial

Baby steps / giant steps strategy

[Paterson, Stockmeyer 1973]
[Brent, Kung 1978]
[Canny, Kaltofen, Yagati 1989]
[Shoup 1994]
[Huang, Pan 1998]
[Kaltofen 2000]
[Bostan, Flajolet, Salvy, Schost 2006]
[van der Hoeven, Lecerf 2017]
[Le Gall, Urrutia 2018]

$$\tilde{O}(n^{\omega_2/2}) \quad \Longrightarrow \quad \underline{O(n^{1.626})}$$

$$(\sqrt{n} \times \sqrt{n}) \cdot (\sqrt{n} \times n)$$

Improvements generically upon 70's bounds

Cubic matrix multiplication

Resultant
of bivariate polynomials
$\deg_x = 1,\ \deg_y = n$

Sylvester of degree one

$\tilde{O}(n^2) \longrightarrow \tilde{O}(n^{5/3})$

Modular composition
$\deg g = n$

$\tilde{O}(n^2) \longrightarrow \tilde{O}(n^{5/3})$

Truncated power series composition
$g = y^n$

$\tilde{O}(n^{1.5})$ no improvement

Improvements generically upon 70's bounds

Fast matrix multiplication

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

Improvements generically upon 70's bounds

Fast matrix multiplication

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

Outline

- The problems
- Key ingredient
  - Resultant
  - Modular composition

From 10.000 feet

Matrix view

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

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

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{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}$$

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{2784154348}{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. $$\det Q = \det A = -20371310335$$

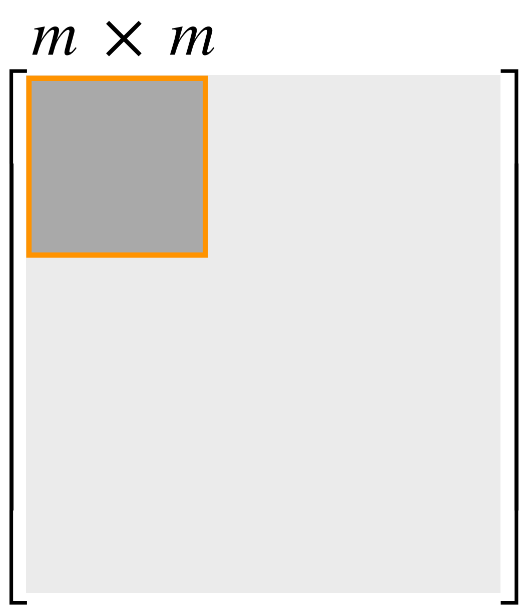
- **Be sure that the matrix fraction is ‘’small’’?**

- Compute a submatrix of the inverse without solving an entire system over $K(x)$?

$A(x) \quad n \times n \qquad \deg A = 1$

We consider a submatrix of the inverse:

$A(x)^{-1} =$



$\longrightarrow \; H(x) = P(x)\, Q(x)^{-1}$

Degrees of $P(x)$, $Q(x)$ depending on m ?

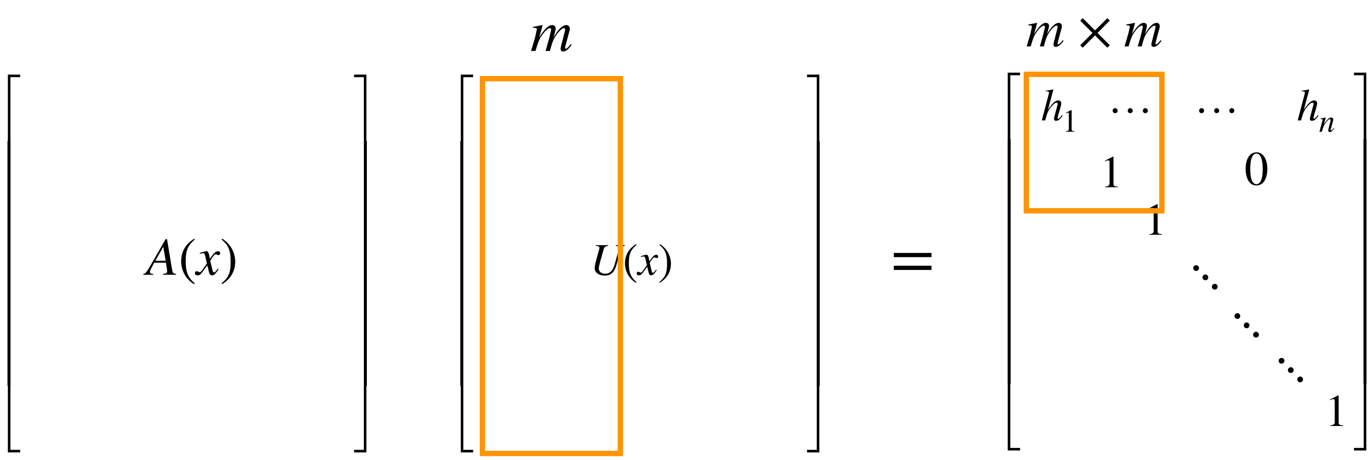
a) Hermite normal form

$$\begin{bmatrix} & & \\ & A(x) & \\ & & \end{bmatrix} \begin{bmatrix} & & \\ & U(x) & \\ & & \end{bmatrix} = \begin{bmatrix} h_1 & \cdots & \cdots & h_n \\ & 1 & & 0 \\ & & 1 & \\ & & & \ddots \\ & & & & \ddots \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}$$

$$h_1(x) = \det A(x)$$

$$\deg h_1 = n$$

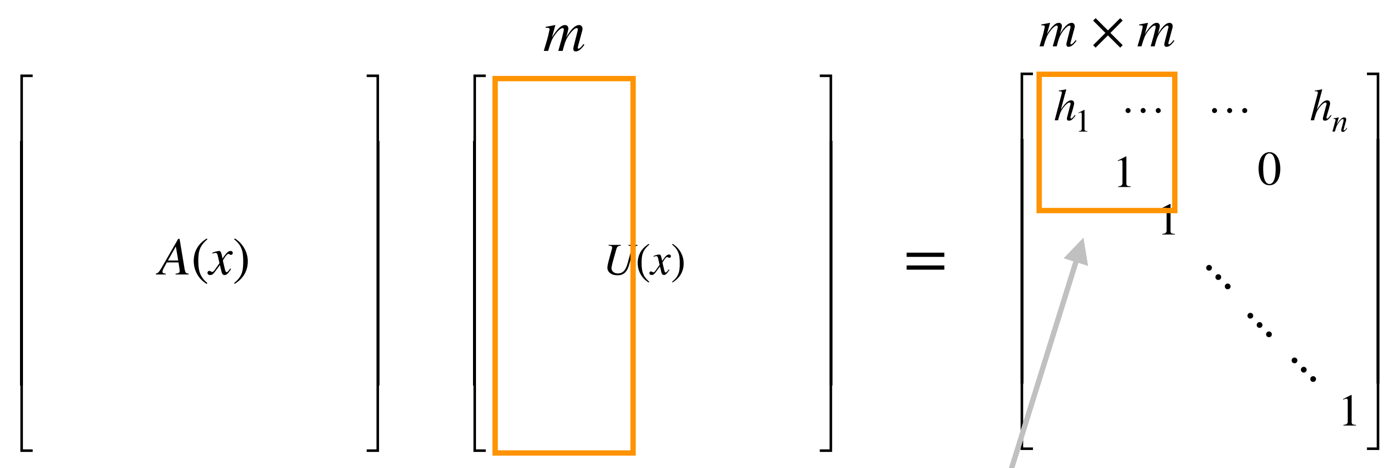
a) Hermite normal form



$$h_1(x) = \det A(x)$$

$$\deg h_1 = n$$

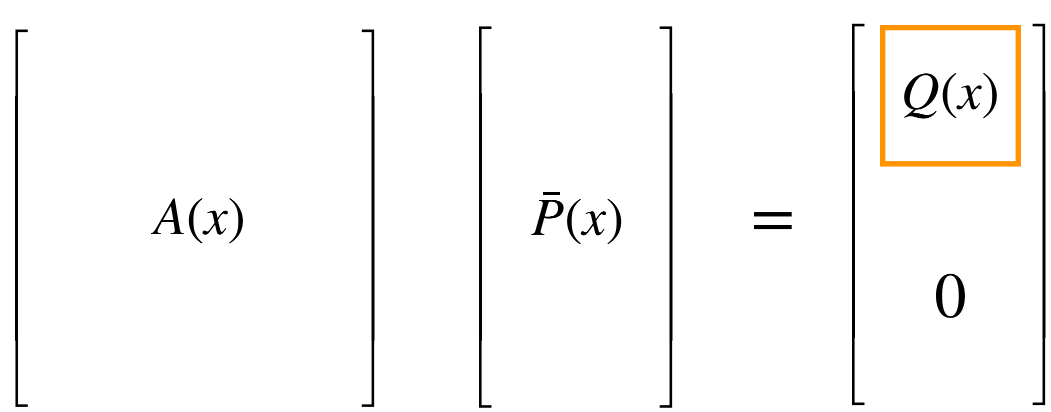
a) Hermite normal form



$$h_1(x) = \det A(x)$$

$$\deg h_1 = n$$

b) Minimal module basis: $\deg Q = n/m$



$$\Longrightarrow \quad A(x)^{-1}\begin{bmatrix} I_m \\ 0 \end{bmatrix} = \bar{P}(x)Q(x)^{-1}$$

Small size fraction

Lemma. Generically, $H(x) = R(x)Q(x)^{-1} \in \mathsf{K}(x)^{m\times m}$

with $\deg R$, $\deg Q \in O(n/m)$

and $\deg Q = \det A$

Nota. Rather than Gaussian elimination we have used a unimodular transform.

→ **Expansion limited** to order $O(n/m)$

- ✓ Be sure that the matrix fraction is ‘’small’’?

- **Compute a submatrix of the inverse without solving an entire system over $K(x)$?**

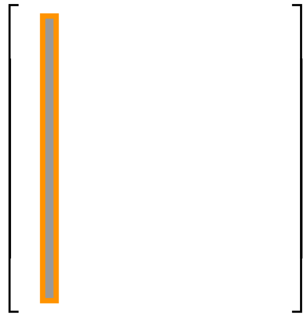
Outline

- The problems
- Key ingredient
    - Resultant
    - Modular composition

Taking advantage of the structure

- System solution:

  n entries

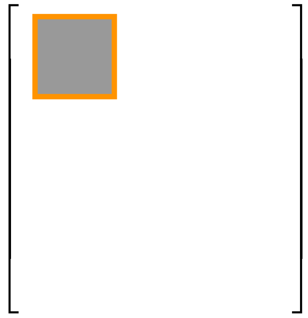
$S(x)^{-1} =$ 

$\tilde{O}(n)$ operations in K

and expansion of order $O(n)$

- **Matrix fractions:**

  Ex: $\sqrt{n} \times \sqrt{n} = n$ entries

$S(x)^{-1} =$ 

$\tilde{O}(n)$ operations in K

and expansion of order $O(\sqrt{n})$

Outline

- The problems
- Key ingredient
  - Resultant
  - Modular composition

Sylvester matrix

Toeplitz-like matrices

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

Toeplitz-like matrices

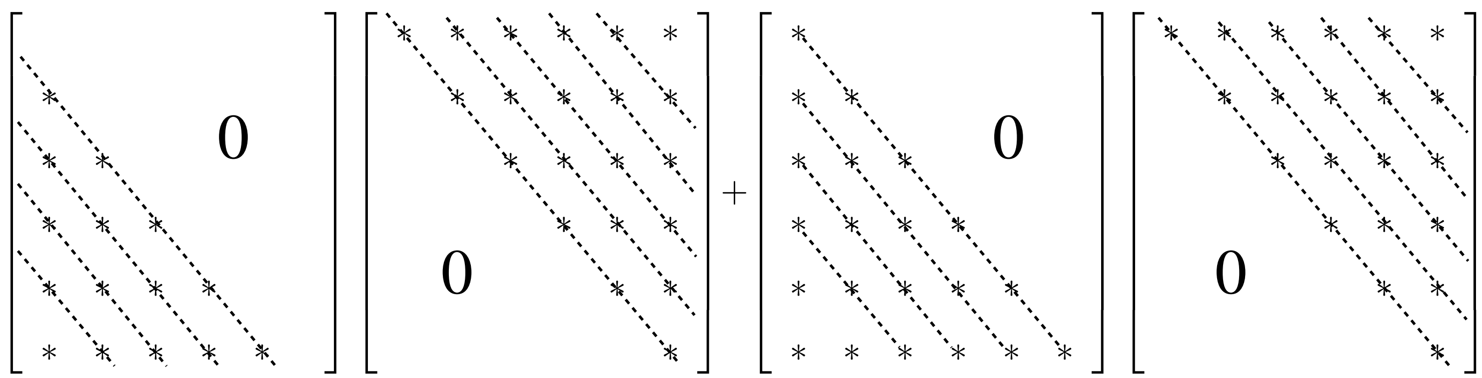
(Widely used techniques)

[Kailath, Kung, Morf 1979]
[Labahn 1992]
[Kaltofen 1994]
[Bini, Pan 1994]

Theory of displacement rank

ΣLU representation: **sum of triangular Toeplitz matrix**

$S(x) =$



✓ Be sure that the matrix fraction is ‘’small’’?

- **Compute a submatrix of the inverse without solving an entire system over $K(x)$?**

The structure is kept recursively during block Gaussian elimination *à la* Strassen

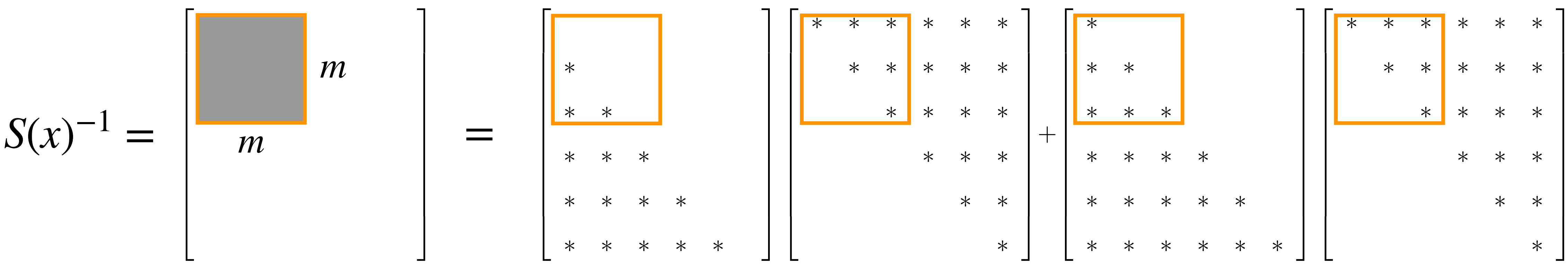
ΣLU representation of the inverse

$\tilde{O}(n)$ operations on truncated power series (half-gcd)

$$
\begin{bmatrix} \\ \\ & S(x)^{-1} & \\ \\ \\ \end{bmatrix}
=
\begin{bmatrix}
 & & & & 0 & \\
* & & & & & \\
* & * & & & & \\
* & * & * & & & \\
* & * & * & * & & \\
* & * & * & * & * &
\end{bmatrix}
\begin{bmatrix}
* & * & * & * & * & * \\
 & * & * & * & * & * \\
 & & * & * & * & * \\
 & & & * & * & * \\
 & 0 & & & * & * \\
 & & & & & *
\end{bmatrix}
+
\begin{bmatrix}
* & & & & 0 & \\
* & * & & & & \\
* & * & * & & & \\
* & * & * & * & & \\
* & * & * & * & * & \\
* & * & * & * & * & *
\end{bmatrix}
\begin{bmatrix}
* & * & * & * & * & * \\
 & * & * & * & * & * \\
 & & * & * & * & * \\
 & & & * & * & * \\
 & 0 & & & * & * \\
 & & & & & *
\end{bmatrix}
$$

Submatrix of the inverse

$m \times m$ polynomial (truncated power series) Toeplitz matrix products



Algorithm ''Structured determinant''

Input: $S(x)$ Toeplitz-like

1. Compute an expansion of a submatrix of $S(x)^{-1}$

2. Reconstruct a fraction $P(x)Q(x)^{-1} \in \mathsf{K}(x)^{m\times m}$

Output: $\det Q(x)$

Algorithm ''Structured determinant''

Input: $S(x)$ Toeplitz-like

1. Compute an expansion of a submatrix of $S(x)^{-1}$ ← $\tilde{O}(n \cdot \frac{n}{m})$

2. Reconstruct a fraction $P(x)Q(x)^{-1} \in \mathrm{K}(x)^{m \times m}$

Output: $\det Q(x)$

(Steps 2 and Output: $\tilde{O}(m^{\omega} \cdot \frac{n}{m})$)

→ Block size $m = n^{1/3}$ or $m = n^{1/\omega}$

Generic **resultant** cost: $\tilde{O}(n^{2-1/\omega})$

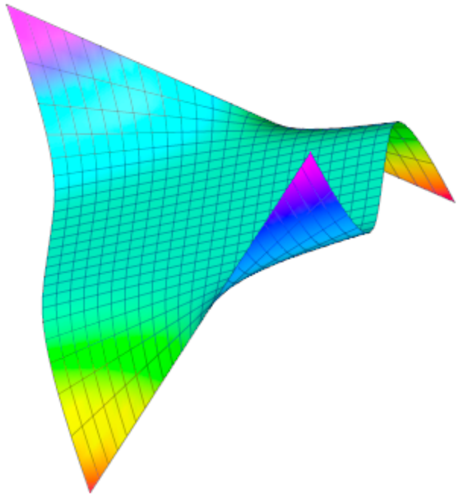
Here degree 1, analogous for degree d

Outline

- The problems
- Key ingredient
    - Resultant
    - Modular composition

From 10.000 feet

Polynomial view



Multiplication by $a(y)$ in $\mathrm{K}[y]/g(y)$ (canonical basis)

$$p \mapsto a \cdot p \bmod g$$

$$A = \begin{bmatrix} \vert & \vert & \cdots & \vert \\ a & ay & \cdots & ay^{n-1} \\ \vert & \vert & & \vert \end{bmatrix}$$

Multiplication by $a(y)$ in $\mathrm{K}[y]/g(y)$ (canonical basis)

$$p \mapsto a \cdot p \bmod g$$

$$A = \begin{bmatrix} a & ay & \dots & ay^{n-1} \end{bmatrix}$$

(See the slide on denominator minimization)

$$\begin{bmatrix} x - A \end{bmatrix} \begin{bmatrix} \bar{P}(x) \end{bmatrix} = \begin{bmatrix} Q(x) \\ 0 \end{bmatrix} \longrightarrow q_{1j}(x) + yq_{2j}(x) + \dots + y^{m-1}q_{mj}(x)$$

We have computed a **generating set** of *m* polynomials of

degree n/m in x and $m-1$ in y

of the **ideal** $\langle x - a(y), g(y) \rangle$

Modular composition

$h(a(y)) \bmod g(y)$?

Modulo the generating set

$$h(x) \longrightarrow r(x,y) = r_0(x) + yr_1(x) + \ldots + y^{m-1}r_{m-1}(x)$$

Phase 2. Evaluate $r(a(y), y) \bmod g(y)$

[Brent, Kung 1978]
[Nüsken, Ziegler 2004]

$m = n^{1/3}$

$(\omega + 2)/3$

$\tilde{O}(n^{1.46})$

Modular composition

Phase 1. Compute the generating set given by the denominator matrix

We had the exponent $\tilde{O}(n^{2-1/\omega})$ for general Toeplitz-like matrices

How to do better for the multiplication matrix?

Duality

[Shoup 94]
[Canny, Kaltofen, Yagati 1989]
[Kaltofen 2000]

$$\begin{bmatrix} \ell_0 & \ell_1 & \ell_2 & \dots & \ell_{n-1} \end{bmatrix} \cdot \begin{bmatrix} \overrightarrow{1} & \overrightarrow{a^1} & \overrightarrow{a^2} & \dots & \overrightarrow{a^{n-1}} \end{bmatrix} \cdot \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ \vdots \\ h_{n-1} \end{bmatrix}$$

Left matrix-vector product

PowerProjections

$\ell : \mathbb{A} \to \mathsf{K}$

$\ell(1), \ell(a), \ell(a^2), \ \dots, \ell(a^{2n-1})$

Right matrix-vector product

Modular Composition

$h(a) \mod g$

Duality

[Shoup 94]
[Canny, Kaltofen, Yagati 1989]
[Kaltofen 2000]

$$\begin{bmatrix}\ell_0 & \ell_1 & \ell_2 & \dots & \ell_{n-1}\end{bmatrix} \cdot \begin{bmatrix} \overrightarrow{1} & \overrightarrow{a^1} & \overrightarrow{a^2} & \dots & \overrightarrow{a^{n-1}} \end{bmatrix} \cdot \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ \vdots \\ h_{n-1} \end{bmatrix}$$

Left matrix-vector product

PowerProjections

$\ell : \mathbb{A} \to \mathsf{K}$

$\ell(1), \ell(a), \ell(a^2), \dots, \ell(a^{2n-1})$

Right matrix-vector product

Modular Composition

$h(a) \mod g$

Duality

[Shoup 94]
[Canny, Kaltofen, Yagati 1989]
[Kaltofen 2000]

PowerProjections ⟷ Modular Composition

Duality

[Shoup 94]
[Canny, Kaltofen, Yagati 1989]
[Kaltofen 2000]

PowerProjections ⟵ Modular Composition

Rich literature

Ex: *bit complexity model using Gröbner bases*

multipoint evaluation $\Longrightarrow$ bivariate resultant

[Kedlaya, Umans 2011]
[van der Hoeven, Larrieu 2018]
[van der Hoeven, Lecerf 2019]

Duality

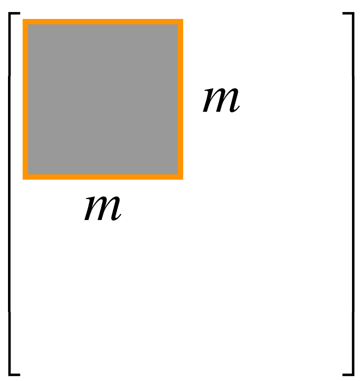
[Shoup 94]
[Canny, Kaltofen, Yagati 1989]
[Kaltofen 2000]

PowerProjections → Modular Composition

Block power projections

$$M(x) = x - A$$

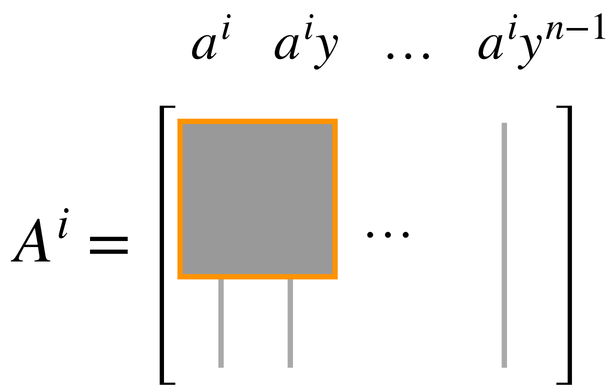
$$M(x)^{-1} = \sum_{i \geq 0} A^i x^{-i-1}$$



Submatrix of the inverse $\equiv$ submatrices of the A^i

$$X = \begin{bmatrix} I_m \\ 0 \end{bmatrix}$$

$$X^T A^i X, \; i \geq 0$$



$$m \text{ coefficients of } \left\{ \begin{array}{llll} a & ay & \dots & ay^{m-1} \\ a^2 & a^2 y & \dots & a^2 y^{m-1} \\ \dots & & & \\ a^d & a^d y & \dots & a^d y^{m-1} \end{array} \right.$$

Block power projections

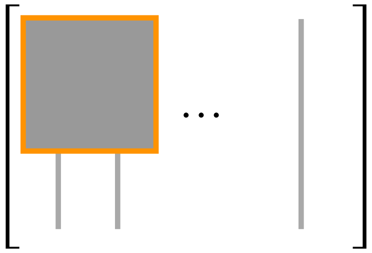
[Kaltofen, Villard 2005]

1. $U_j := X^T A^j \quad 0 \le j < r = n^\rho$ $\quad\quad \tilde{O}(n^{1+\rho})$

2. $Z := A^r$

3. $V_k := Z^k X \quad 0 \le k \le t = n^\tau$ $\quad\quad \tilde{O}(n^{1+\tau})$

$U_j V_k' s$ →

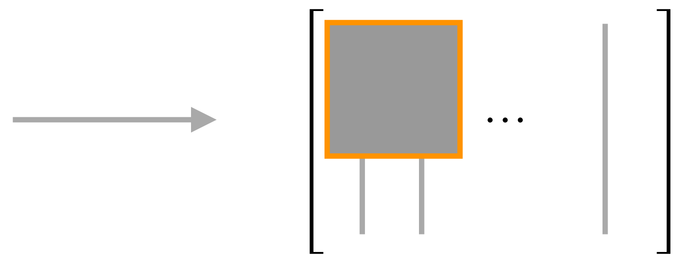


$X^T A^i X := X^T A^{j+kr} X, \; 0 \le i < 2n/m$

Block power projections

[Kaltofen, Villard 2005]

$U_j V'_k s$



$$X^T A^i X := X^T A^{j+kr} X, \; 0 \le i < 2n/m$$

Displacement rank $\gamma = O(\max\{r, s\}$

$$\tilde{O}(\gamma^{\omega-1} n)$$

- Polynomial point of view
- Structured matrices
  [Bostan, Jeannerod, Schost 2008]

$r = t = m = n^{1/3}$ $\qquad \tilde{O}(n^{1.46})$

Open question: optimal algorithms ?

Thank you !