On Computing the Resultant of Generic Bivariate Polynomials

Gilles Villard

ISSAC, New York, July 17th, 2018

Outline of the talk

- Appetizer
- The problem

New algorithm:

- A key ingredient
- A central remark

Outline of the talk

- Appetizer

- The problem

New algorithm:

- A key ingredient

- A central remark

Minimal polynomial in a field extension

$$g(y) = y^4 + 10\,y^3 + 3\,y^2 + 7\,y + 4 \mod 11$$

$$\mathbb{A} = \mathsf{K}[y]/g(y)$$

$$\alpha(y) = y^4 + 4\,y^2 + 8\,y + 9 \in \mathbb{A}$$

Find the relation $\alpha(y)^2 + \alpha(y) + 4 = 0$?

Minimal polynomial in a field extension

$$\mathbb{A} = \mathsf{K}[y]/g(y) \qquad \deg g = n$$

$$\alpha(y) \in \mathbb{A}$$

$\mu(y)$ monic (and irreducible) such that $\mu(\alpha(y)) \equiv 0 \mod g(y)$

$$\alpha^{\mathbf{n}}(y) + \mu_{n-1}\,\alpha^{\mathbf{n-1}}(y) + \ldots + \mu_1\,\alpha(y) + \mu_0 \equiv 0 \mod g(y) \;\; ?$$

Generic case: $\mu(y) = \chi(y)$

Projection for saving operations:

use a K-**linear map**:

$$\pi : \mathrm{K}[y]/g(y) \to \mathrm{K}$$

Minimal polynomial in a field extension

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

1. Compute $\pi(1), \pi(\alpha), \pi(\alpha^2), \ \ldots, \pi(\alpha^{2n-1})$

   / The sequence is linearly generated over* K **/*

2. Compute the **minimal polynomial of the sequence**

   using *e.g.* a Euclidean scheme or the Berlekamp-Massey algorithm

Nota. One uses the trace and Leverrier's approach for the **characteristic polynomial**.

MinPoly / CharPoly

$$\mu(\alpha) \equiv 0 \mod g$$

$\tilde{O}(n)$

PowerProjections

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

$\pi(1), \pi(\alpha), \pi(\alpha^2), \ \ldots, \pi(\alpha^{2n-1})$

$$\mathbb{A} = \mathsf{K}[y]/g(y) \simeq \mathsf{K}^n$$

$$[\pi_0 \quad \pi_1 \quad \pi_2 \quad \dots \quad \pi_{n-1}] \cdot \begin{bmatrix} \overrightarrow{\alpha^0} & \overrightarrow{\alpha^1} & \overrightarrow{\alpha^2} & \dots & \overrightarrow{\alpha^{n-1}} \end{bmatrix}$$

Left matrix-vector product

PowerProjections

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

$\pi(1), \pi(\alpha), \pi(\alpha^2), \ \dots, \pi(\alpha^{2n-1})$

$$\mathbb{A} = \mathsf{K}[y]/g(y) \simeq \mathsf{K}^n$$

$$[\pi_0 \quad \pi_1 \quad \pi_2 \quad \dots \quad \pi_{n-1}] \cdot \begin{bmatrix} & & & & \\ \overrightarrow{\alpha^0} & \overrightarrow{\alpha^1} & \overrightarrow{\alpha^2} & \dots & \overrightarrow{\alpha^{n-1}} \\ & & & & \end{bmatrix} \cdot \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ \vdots \\ h_{n-1} \end{bmatrix}$$

Left matrix-vector product

PowerProjections

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

$\pi(1), \pi(\alpha), \pi(\alpha^2), \ \dots, \pi(\alpha^{2n-1})$

Right matrix-vector product

Modular Composition

For a polynomial h

$h(\alpha) \mod g$?

Transposition principle

[Shoup 94]

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

PowerProjections

$O(n)$

Modular Composition

$\pi : \mathbb{A} \rightarrow \mathsf{K}$

$\pi(1), \pi(\alpha), \pi(\alpha^2), \ \ldots, \pi(\alpha^{2n-1})$

For a polynomial h

$h(\alpha) \mod g$?

MinPoly / CharPoly

$\mu(\alpha) \equiv 0 \mod g$

$\tilde{O}(n)$

PowerProjections

$O(n)$

Modular Composition

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

$\pi(1), \pi(\alpha), \pi(\alpha^2), \ldots, \pi(\alpha^{2n-1})$

For a polynomial h

$h(\alpha) \mod g$?

Minimal polynomial in a field extension

Modular Composition $\Longrightarrow$ MinPoly / CharPoly

$\tilde{O}(n^2)$ operations in K

Baby steps / giant steps strategy

[Paterson, Stockmeyer 1973]

[Brent & Kung 1978]

[Shoup 1994]

[Huang, Pan 1998]

[Kaltofen 2000]

[Bostan, Flajolet, Salvy, Schost 2006]

[Le Gall, Urrutia 2018]

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

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

Improvement for generic polynomials

Particular case of the resultant approach

$\alpha(y) \in \mathbb{A}$

Multiplication endomorphism:

$A : u \mapsto \alpha u$

Characteristic polynomial

$$\begin{bmatrix} \quad A \quad \end{bmatrix} \longrightarrow \det \begin{bmatrix} \quad x I - A \quad \end{bmatrix} ?$$

$n \times n$

Outline of the talk

- Appetizer
- The problem

New algorithm:

- A key ingredient
- A central remark

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

$$\det A(x)\,?$$

Ex: *Toeplitz, Sylvester matrix, Frobenius matrix algebra, etc.*

Entries in K

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

$\deg p, q = n$

Sylvester matrix

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

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

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

[Bini, Pan 1994]

[von zur Gathen, Gerhard 1999]

Rule of thumb:

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

(Evaluation-interpolation scheme)

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: $2n$

$$2n \text{ points} \implies \tilde{O}(n \times n) = \tilde{O}(n^2) \text{ operations}$$

Rule of thumb:

?

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

(Evaluation-interpolation scheme)

Dense polynomial matrices

[Storjohann 2003-2005]

[Labahn, Neiger, Zhou 2017]

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

Degree: d

Output degree: nd

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

[Beckermann, Labahn 1994]

[Giorgi *et al.* 2003]

Dense matrix fractions

Generic case

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

R, Q of degree d

Matrix fraction reconstruction:

from $O(d)$ terms of $H(x) = \Sigma_i H_i x^i$

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

The problem

To simplify: $\deg_x = 1$

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

$\det S(x)$?

Best known complexity bound $\tilde{O}(n^2)$

Size of a system solution

(n entries of degree $2n$)

New algorithm

From 10.000 feet

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

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

Determinant of A ?

Cramer's rule: $\det A = -203713103035$

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

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

Determinant of A ?

Cramer's rule: $\det A = -203713103035$

What if solving a linear system has prohibitive cost?

$$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^{-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^{-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{2076805973}{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{2784174348}{203713103035} & -\frac{17109379672}{203713103035} & -\frac{1441829408}{203713103035} \end{bmatrix}$$

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

$$A^{-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{2076805973}{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{2784174348}{203713103035} & -\frac{17109379672}{203713103035} & -\frac{1441829408}{203713103035} \end{bmatrix}$$

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

Step 2.
$$\det Q = \det A = -203713103035$$

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

- Compute a submatrix of the inverse without solving an entire system?

Outline of the talk

- Appetizer
- The problem

New algorithm:

- A key ingredient
- A central remark

$$S(x) = \begin{bmatrix} p_n(x) & & & & q_n(x) & & & \\ p_{n-1}(x) & p_n(x) & & & q_{n-1}(x) & q_n(x) & & \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\ & \vdots & & p_n(x) & & \vdots & & q_n(x) \\ p_0(x) & & & p_{n-1}(x) & q_0(x) & & & q_{n-1}(x) \\ & p_0(x) & & \vdots & & q_0(x) & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & p_0(x) & & & & q_0(x) \end{bmatrix}$$

We consider a north-western submatrix of the inverse:

$$S(x)^{-1} = \begin{bmatrix} & \\ & \end{bmatrix}_{m \times m}$$

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

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

Ex: $p(x,y) = xy^8 + y,\ q(x,y) = y^8 + x$

$$S(x) \in \mathsf{K}[x]^{16\times 16} \qquad d = 1$$

$$S(x) = \left[\begin{array}{cccccccc|cccccccc}
x & & & & & & & & 1 & & & & & & & \\
 & x & & & & & & & & 1 & & & & & & \\
 & & x & & & & & & & & 1 & & & & & \\
 & & & x & & & & & & & & 1 & & & & \\
 & & & & x & & & & & & & & 1 & & & \\
 & & & & & x & & & & & & & & 1 & & \\
 & & & & & & x & & & & & & & & 1 & \\
1 & & & & & & & x & & & & & & & & 1 \\
\hline
 & 1 & & & & & & & x & & & & & & & \\
 & & 1 & & & & & & & x & & & & & & \\
 & & & 1 & & & & & & & x & & & & & \\
 & & & & 1 & & & & & & & x & & & & \\
 & & & & & 1 & & & & & & & x & & & \\
 & & & & & & 1 & & & & & & & x & & \\
 & & & & & & & 1 & & & & & & & x & \\
 & & & & & & & & & & & & & & & x
\end{array}\right]$$

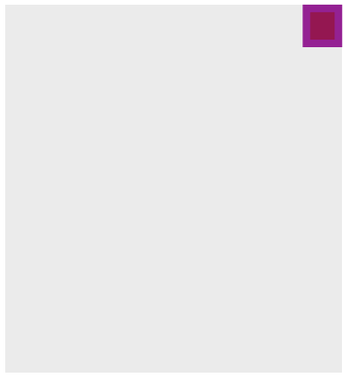
Ex: $p(x,y) = xy^8 + y^m,\ q(x,y) = y^8 + x$

$$S(x) \in \mathsf{K}[x]^{16\times 16} \qquad d = 1$$

$$m = 1$$

$$H(x) = -\frac{1}{x(x^{15}+1)}$$

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



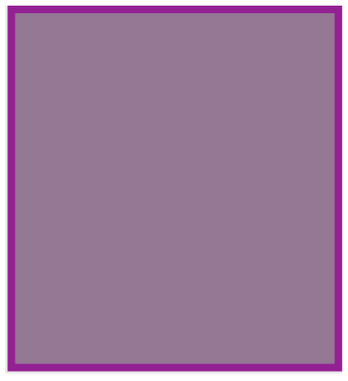
Denominator degree: 16

$$2\lceil n/m \rceil = 2\lceil 8/1 \rceil = 16$$

Ex: $p(x,y) = xy^8 + y^m,\ q(x,y) = y^8 + x$

$$S(x) \in \mathsf{K}[x]^{16\times 16} \qquad d = 1$$

$$H(x) = I \cdot S(x)^{-1}$$

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

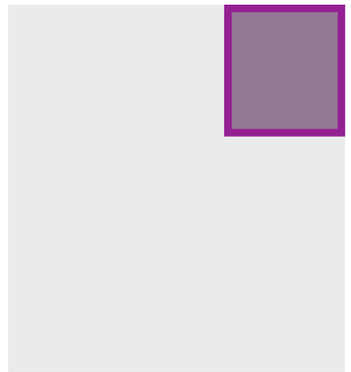
Denominator degree: 1

Ex: $p(x,y) = xy^8 + y^m,\ q(x,y) = y^8 + x$

$$S(x) \in \mathsf{K}[x]^{16\times 16} \qquad d = 1$$

$$m = 5$$

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



$$H(x) = -I \cdot \begin{bmatrix} x & 0 & 0 & x^2 & 0 \\ 0 & x & 0 & 0 & x^2 \\ x^4 & 0 & x & 0 & 0 \\ 0 & x^4 & 0 & x & 0 \\ 0 & 0 & x^4 & 0 & x \end{bmatrix}^{-1}$$

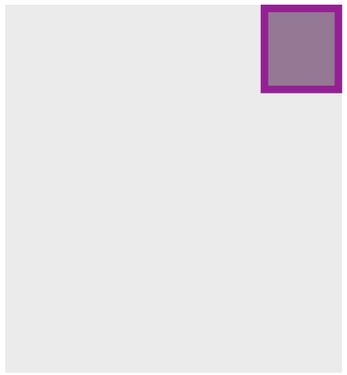
Denominator degree: 4

$$2\lceil n/m \rceil = 2\lceil 8/5 \rceil = 4$$

Ex: $p(x,y) = xy^8 + y^m,\ q(x,y) = y^8 + x$

$$S(x) \in \mathsf{K}[x]^{16\times 16} \qquad d = 1$$

$$m = 3 \qquad H(x) = -I \cdot \begin{bmatrix} x & 0 & x^4 \\ x^6 & x & 0 \\ 0 & x^6 & x \end{bmatrix}^{-1}$$

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

Denominator degree: 6

$$2\lceil n/m \rceil = 2\lceil 8/3 \rceil = 6$$

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 $\deg Q = \det S$

See also [Kaltofen, Villard 2005]

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

- System solution:

  n entries

  expansion of order $O(n)$ $\longrightarrow$ $\tilde{O}(n^2)$

- **Matrix fractions:**

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

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

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

- Compute a submatrix of the inverse without solving an entire system?

Outline of the talk

- Appetizer
- The problem

New algorithm:

- A key ingredient
- A central remark

Toeplitz-like matrices

(Widely used techniques)

Ex: $g(y) = y^6 + 3\,y^5 + 4\,y^4 + 7\,y^3 + 6\,y + 8 \bmod 11$ $\quad\quad$ $\mathbb{A} = \mathsf{K}[y]/g(y)$

$\alpha(y) = 7\,y^5 + 7\,y^4 + 3\,y^3 + 2\,y^2 + y + 9 \in \mathbb{A}$

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

Toeplitz-like matrices

(Widely used techniques)

Ex: $g(y) = y^6 + 3y^5 + 4y^4 + 7y^3 + 6y + 8 \bmod 11$ $\quad\quad$ $\mathbb{A} = \mathsf{K}[y]/g(y)$

$\alpha(y) = 7y^5 + 7y^4 + 3y^3 + 2y^2 + y + 9 \in \mathbb{A}$

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

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

Toeplitz-like matrices

(Widely used techniques)

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

Theory of displacement rank

ΣLU representation:

$$T = \begin{bmatrix} * & & & & & \\ * & * & & & & \\ * & * & * & & & \\ * & * & * & * & & \\ * & * & * & * & * & \\ * & * & * & * & * & * \end{bmatrix} \begin{bmatrix} * & * & * & * & * & * \\ & * & * & * & * & * \\ & & * & * & * & * \\ & & & * & * & * \\ & & & & * & * \\ & & & & & * \end{bmatrix} + \begin{bmatrix} * & & & & & \\ * & * & & & & \\ * & * & * & & & \\ * & * & * & * & & \\ * & * & * & * & * & \\ * & * & * & * & * & * \end{bmatrix} \begin{bmatrix} * & * & * & * & * & * \\ & * & * & * & * & * \\ & & * & * & * & * \\ & & & * & * & * \\ & & & & * & * \\ & & & & & * \end{bmatrix}$$

Ex: *Toeplitz, Sylvester matrix, Frobenius matrix algebra, etc.*

Toeplitz-like matrices

(Widely used techniques)

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

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

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

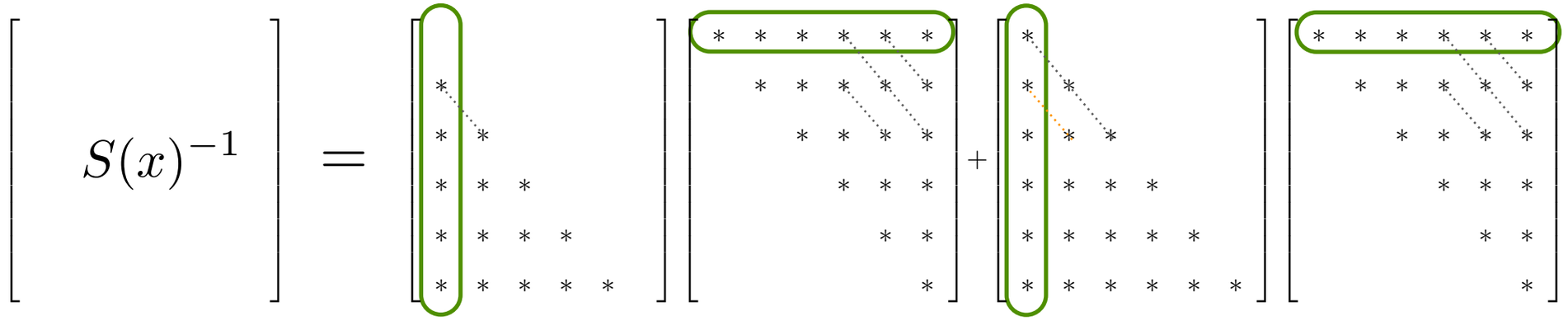
✓ Be sure that the matrix fraction is ‘’small’’?

- Compute a submatrix of the inverse without solving an entire system?

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

ΣLU representation of the inverse

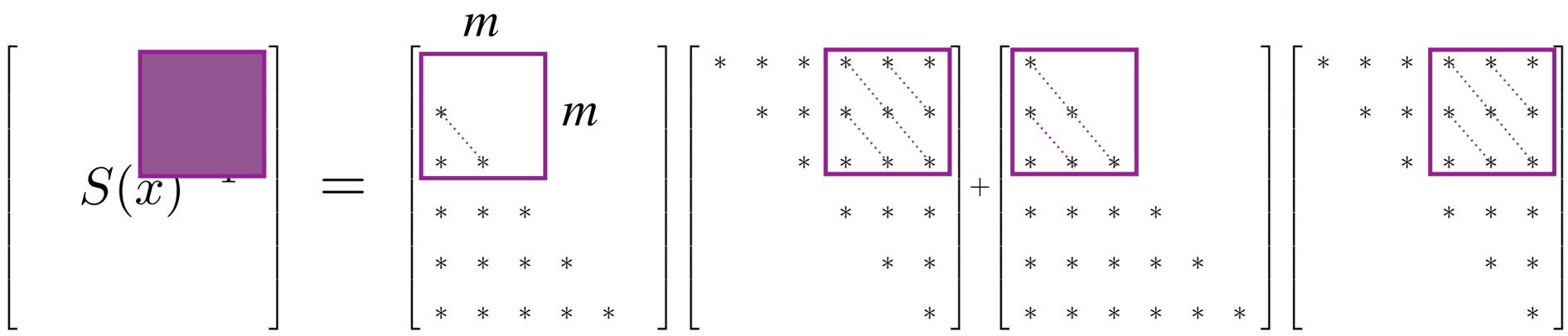
$\tilde{O}(n)$ operations on truncated power series (half-gcd)



?

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

Small polynomial Toeplitz matrix products



Determinant *via* (vector) lifting

1. Expansion of $S(x)^{-1}\,y$

2. Scalar fraction reconstruction

3. Determinant from denominators

Algorithm ‘’Structured determinant”

Input: $S(x)$ a Toeplitz-like matrix

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

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

Output: $\det Q(x)$

Nota: The matrix reconstruction and the final determinant use dense matrix computations.

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

[Beckermann, Labahn 1994] *[Giorgi et al. 2003]*

Algorithm ‘’Structured determinant”

$\tilde{O}(n \cdot \frac{n}{m})$

Input: $S(x)$ a Toeplitz-like matrix

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

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

Output: $\det Q(x)$

Nota: The matrix reconstruction and the final determinant use dense matrix computations.

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

[Beckermann, Labahn 1994] *[Giorgi et al. 2003]*

Algorithm ‘’Structured determinant”

Input: $S(x)$ a Toeplitz-like matrix

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

$\tilde{O}(n \cdot \frac{n}{m})$

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

Output: $\det Q(x)$

$\tilde{O}(m^{\omega} \cdot \frac{n}{m})$

Nota: The matrix reconstruction and the final determinant use dense matrix computations.

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

[Beckermann, Labahn 1994] [Giorgi et al. 2003]

Conclusion

Expansion: $\tilde{O}(n \cdot \frac{n}{m})$

Dense linear algebra: $\tilde{O}(m^{\omega} \cdot \frac{n}{m})$

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

- Generic **resultant** cost: $\tilde{O}(n^2)$ → $\tilde{O}(n^{5/3})$ / $O(n^{1.58})$

  Determinant of a polynomial structured matrix

  Here degree 1, analogous for degree d

- Application to Gröbner bases of generic ideals

  See also [van der Hoeven and Larrieu 2018]

Conclusion bis

Field extension

CharPoly: $O(n^{1.63}) \longrightarrow O(n^{1.58})$ better than composition ?

$\longrightarrow$ Generalization

Improvement of **modular composition** for generic polynomials

$$\text{CharPoly}_{\text{Gen}} \approx \text{Modular Composition}_{\text{Gen}} < \begin{cases} \text{CharPoly} \\ \text{Modular Composition} \end{cases} ?$$

Thank you !