September 28th, updates

The final score should be based on three evaluations:

$\longrightarrow$ Exercise score: one exercise per week will be identified during one of the two lessons, with a precise deadline for sending your script

$\longrightarrow$ Mid-term exam, Wednesday Oct. 7th: modalities to be communicated (pending ENS instructions)

$\longrightarrow$ Final exam, expected Monday Nov. 11th

Alternative to Gaussian elimination - ctd

September 28th, 2020

Overview

Matrix polynomials

Minimal bases

New elimination

Matrix polynomials

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

$$\det A(x) = \sum_{\sigma} \prod_{i=1}^{n} A_{\sigma(i),i}$$

$$\deg \det A \leq nd$$

$A \in \mathbb{Z}[x]^{n \times n}$ with entries of absolute values less than b

$$\det A = \prod_{j=1}^{n} \|A_j^*\| \leq \prod_{j=1}^{n} \|A_j\| \leq b^n n^{n/2}$$

For **input size** β:

$$\log \det A \leq n\beta + O(n \log n)$$

- Hadamard's conjecture

$a_{i,j} \in \{1, -1\}$ and the rows of A are mutually orthogonal

A Hadamard matrix of dimension n exists for every n multiple of 4

$$A = \begin{bmatrix} 54 & -79 & -5 & -79 \\ 47 & 9 & 47 & 75 \\ 90 & 45 & -54 & -85 \\ -41 & -10 & -72 & -19 \end{bmatrix}$$

$$A = \begin{bmatrix} 54 & -79 & -5 & -79 \\ 47 & 9 & 47 & 75 \\ 90 & 45 & -54 & -85 \\ -41 & -10 & -72 & -19 \end{bmatrix} \rightarrow \begin{bmatrix} 54 & -79 & -5 & -79 \\ 0 & \frac{4199}{54} & \frac{2773}{54} & \frac{7763}{54} \\ 0 & 0 & -\frac{681651}{4199} & -\frac{1175510}{4199} \\ 0 & 0 & 0 & \frac{69126727}{681651} \end{bmatrix}$$

$$A = \begin{bmatrix} 54 & -79 & -5 & -79 \\ 47 & 9 & 47 & 75 \\ 90 & 45 & -54 & -85 \\ -41 & -10 & -72 & -19 \end{bmatrix} \rightarrow \begin{bmatrix} 54 & -79 & -5 & -79 \\ 0 & \frac{4199}{54} & \frac{2773}{54} & \frac{7763}{54} \\ 0 & 0 & -\frac{681651}{4199} & -\frac{1175510}{4199} \\ 0 & 0 & 0 & \frac{69126727}{681651} \end{bmatrix}$$

$$\det A = -69126727$$

$$a_{ij}^{(k)} = \begin{vmatrix} A_{1..k,1..k} & A_{1..k,j} \\ A_{i,1..k} & a_{ij} \end{vmatrix}$$

$L_i \leftarrow L_i - \alpha L_k$

$$a_{ij}^{[k]} = a_{ij}^{[k-1]} - \frac{a_{ik}^{[k-1]}}{a_{kk}^{[k-1]}} a_{kj}^{[k-1]}$$

$$a_{ij}^{(k)} = \begin{vmatrix} A_{1..k,1..k} & A_{1..k,j} \\ A_{i,1..k} & a_{ij} \end{vmatrix}$$

$L_i \leftarrow L_i - \alpha L_k$

$$a_{ij}^{[k]} = a_{ij}^{[k-1]} - \frac{a_{ik}^{[k-1]}}{a_{kk}^{[k-1]}} a_{kj}^{[k-1]} = \frac{a_{ij}^{(k)}}{a_{kk}^{(k-1)}}$$

Gauss-Bareiss elimination (Sylvester's identities)

$$
\begin{bmatrix}
a_{11} & a_{12} & \dots & \dots & a_{1n} \\
a_{22} & a_{22} & & & \vdots \\
\vdots & & & & \vdots \\
\vdots & & & & \vdots \\
a_{n1} & \dots & \dots & \dots & a_{nn}
\end{bmatrix}
\to
\begin{bmatrix}
a_{11} & a_{12} & \dots & \dots & a_{1n} \\
0 & \frac{\Delta_{22}}{\Delta_{11}} & & & \vdots \\
\vdots & & \ddots & \color{red}{\frac{\boldsymbol{\Delta_{i,j}}}{\boldsymbol{\Delta_{i-1,i-1}}}} & \vdots \\
\vdots & 0 & & \ddots & \vdots \\
0 & \dots & \dots & 0 & \frac{\Delta_{nn}}{\Delta_{n-1,n-1}}
\end{bmatrix}
$$

$$
\Delta_{i,j} = \left| \begin{array}{ccc|c}
a_{11} & \dots & a_{1,i-1} & a_{1,j} \\
a_{21} & \dots & a_{2,i-1} & a_{2,j} \\
\vdots & & \vdots & \vdots \\
a_{i1} & \dots & a_{i,i-1} & a_{i,j}
\end{array} \right|
$$

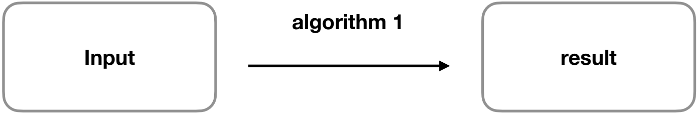
Gauss-Bareiss elimination (Sylvester's identities)

$$\begin{bmatrix} a_{11} & a_{12} & \dots & \dots & a_{1n} \\ a_{22} & a_{22} & & & \vdots \\ \vdots & & & & \vdots \\ \vdots & & & & \vdots \\ a_{n1} & \dots & \dots & \dots & a_{nn} \end{bmatrix} \to \begin{bmatrix} a_{11} & a_{12} & \dots & \dots & a_{1n} \\ 0 & \frac{\Delta_{22}}{\Delta_{11}} & & & \vdots \\ \vdots & & \ddots & \frac{\Delta_{i,j}}{\Delta_{i-1,i-1}} & \vdots \\ \vdots & 0 & & \ddots & \vdots \\ 0 & \dots & \dots & 0 & \frac{\Delta_{nn}}{\Delta_{n-1,n-1}} \end{bmatrix}$$

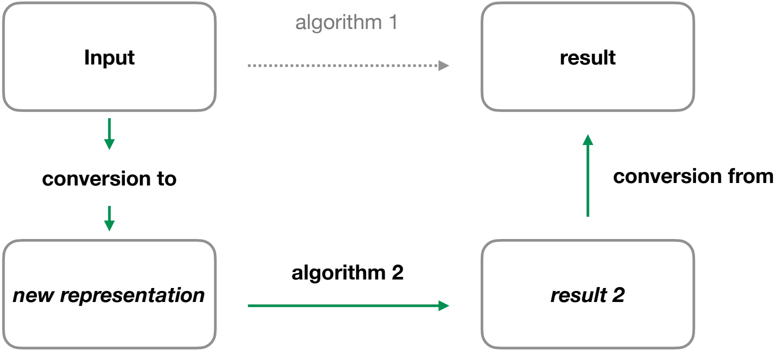
$$\Delta_{i,j} = \left| \begin{array}{ccc|c} a_{11} & \dots & a_{1,i-1} & a_{1,j} \\ a_{21} & \dots & a_{2,i-1} & a_{2,j} \\ \vdots & & \vdots & \vdots \\ a_{i1} & \dots & a_{i,i-1} & a_{i,j} \end{array} \right|$$

Size of output entries $\approx$ size of the determinant

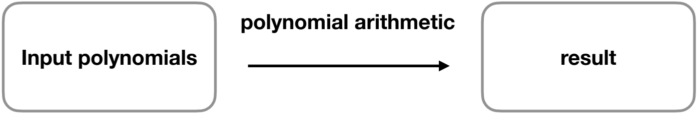
Change of representation



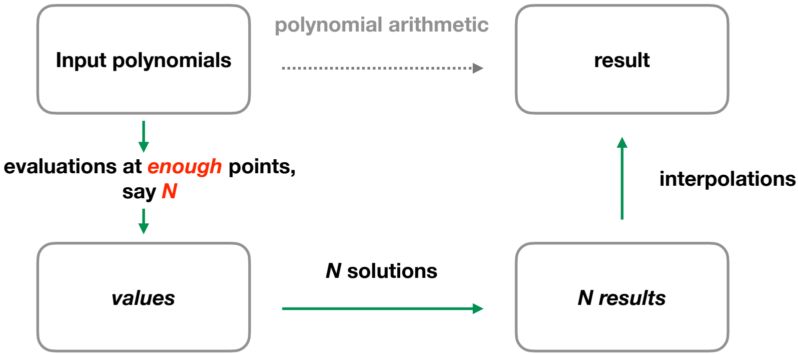
Change of representation



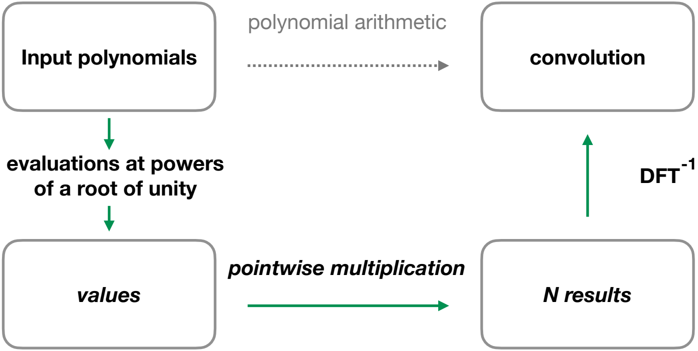
Polynomial (or rational function) problem



Polynomial (or rational function) problem



Example : DFT based polynomial multiplication



Chinese Remainder Theorem

R a Euclidean domain

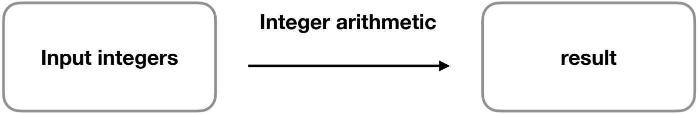
$m_1, m_2, \ldots, m_l \in$ R pairwise coprime, $\quad m = m_1 m_2 \ldots m_l$

$$\mathsf{R}/\langle m \rangle \cong \mathsf{R}/\langle m_1 \rangle \times \mathsf{R}/\langle m_2 \rangle \times \ldots \times \mathsf{R}/\langle m_l \rangle$$

Cost: $O(\mathsf{M}(\log m) \log \log m)$

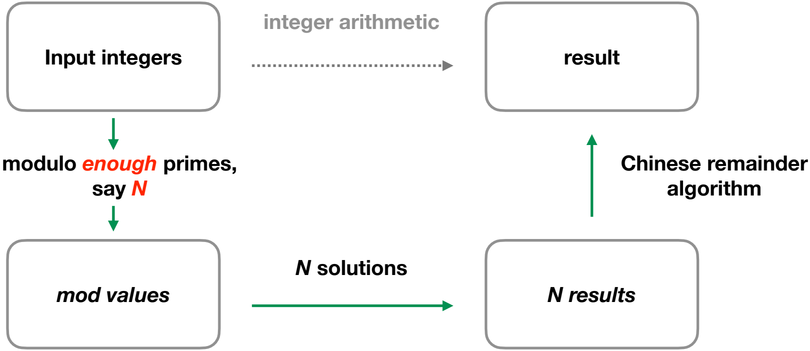
“Interpolating an integer from its values at several primes”

Integer (or rational) problem



"Interpolating an integer from its values at several primes"

Integer (or rational) problem



$\mathsf{K}[\mathbf{x}]$ or **Bit complexity**

Inputs and outputs have a **size** or a **precision**.

Impact on the problem's complexity ?

$\mathsf{K}[\mathbf{x}]$ or **Bit complexity**

Inputs and outputs have a **size** or a **precision**.

Impact on the problem's complexity ?

- $A \in \mathsf{K}[x]^{n\times n}$: $\deg \det A = O(\mathbf{n}\, d)$

K[x] or **Bit complexity**

Inputs and outputs have a **size** or a **precision**.

Impact on the problem's complexity ?

- $A \in \mathsf{K}[x]^{n \times n}$: $\deg \det A = O(\mathbf{n}\, d)$
- $A \in \mathbb{Z}^{n \times n}$: $\mathsf{size}(\det A) = O\tilde{}(\mathbf{n} \log \|A\|)$

$\mathsf{K}[\mathbf{x}]$ or **Bit complexity**

Inputs and outputs have a **size** or a **precision**.

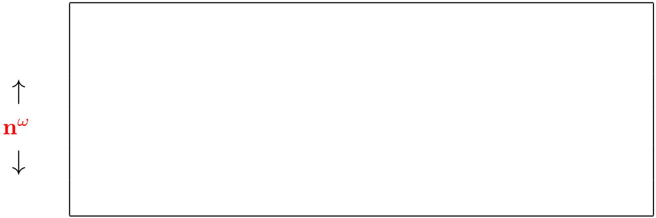
Impact on the problem's complexity ?

- $A \in \mathsf{K}[x]^{n\times n}$: $\deg \det A = O(\mathbf{n}\, d)$
- $A \in \mathbb{Z}^{n\times n}$: $\mathsf{size}(\det A) = \tilde{O}(\mathbf{n} \log \|A\|)$
- $A \in \mathbb{Z}^{n\times n}$: $O(\log \mathsf{cond}(A)) = \tilde{O}(\mathbf{n} \log \|A\|)$

Impact of data size ?

Ex. Determinant computation/Output size : $\mathbf{n}d$

Evaluation/interpolation or homomorphic scheme



Impact of data size ?

Ex. Determinant computation/Output size : $\mathbf{n}d$

Evaluation/interpolation or homomorphic scheme

$\longleftarrow$ $\boxed{\mathbf{n}d \text{ points}}$ $\longrightarrow$

$\uparrow$
$\mathbf{n}^{\omega}$
$\downarrow$

Impact of data size ?

Ex. Determinant computation/Output size : $\mathbf{n}d$

Evaluation/interpolation or homomorphic scheme

$\leftarrow$ $\mathbf{n}d$ points $\rightarrow$

$\uparrow$ $\mathbf{n}^{\omega}$ $\downarrow$

Complexity estimates:

$$O\tilde{}(n^{\omega} \times nd) = O\tilde{}(\mathbf{n}^{\omega+1}d)$$

Impact of data size ?

Ex. Determinant computation/Output size : $\mathbf{n}d$ or $O\tilde{}(\mathbf{n}\log\|A\|)$,

Evaluation/interpolation or homomorphic scheme

or $O\tilde{}(n\log\|A\|)$ bits *a priori* :

$\leftarrow$ $\mathbf{n}d$ points or $O\tilde{}(\mathbf{n}\log\|A\|)$ bits $\rightarrow$

$\uparrow$ $\mathbf{n}^\omega$ $\downarrow$

Complexity estimates:

$$O\tilde{}(n^\omega \times nd) = O\tilde{}(\mathbf{n}^{\omega+1}d)$$
$$O\tilde{}(\mathbf{n}^{\omega+1}\log\|A\|)$$

Related problem - 2

Rational reconstruction

$f(x) \in \mathsf{K}[x]$, degree n

$h(x)$

Find $p(x)$ and $q(x)$ such that for k given $1 \leq k \leq n$:

$$h(x) = \frac{p(x)}{q(x)} \bmod f(x)$$

with $\mathrm{gcd}(q,f) = 1$, $\deg p < k$, $\deg q \leq n - k$

Linear system solution

$A(x) \in \mathsf{K}[x]^{n\times n}$, $b(x) \in \mathsf{K}[x]^n$ $\quad Au = b$?

1. $\det A(0) \neq 0 \in \mathsf{K}$ or solve the shifted problem $A(x+\alpha)u(x+\alpha) = b(x+\alpha)$

Linear system solution

$A(x) \in \mathsf{K}[x]^{n\times n}$, $b(x) \in \mathsf{K}[x]^n$ $\quad Au = b$?

1. $\det A(0) \neq 0 \in \mathsf{K}$ or solve the shifted problem $A(x+\alpha)u(x+\alpha) = b(x+\alpha)$
2. Compute the truncated power series such that $A(x)\hat{u}(x) = b(x) \bmod x^{2nd+1}$

Linear system solution

$A(x) \in \mathsf{K}[x]^{n\times n}$, $b(x) \in \mathsf{K}[x]^n$ $\quad Au = b$?

1. $\det A(0) \neq 0 \in \mathsf{K}$ or solve the shifted problem $A(x+\alpha)u(x+\alpha) = b(x+\alpha)$
2. Compute the truncated power series such that $A(x)\hat{u}(x) = b(x) \bmod x^{2nd+1}$
3. Reconstruct $u(x)$ from $\hat{u}(x)$ (rational reconstruction)

Cost: $\tilde{O}(n^\omega \times nd)$

▷ $\mathbf{MM(n, d)} = O\tilde{}(n^\omega d)$: cost for multiplying $n \times n$ matrices of degree d

▷ $\mathbf{MM(n, \log \|A\|)} = O\tilde{}(n^\omega \log \|A\|)$: cost for multiplying $n \times n$ integer matrices

The determinant can be computed in

in $O(n \cdot \mathsf{MM}(n, d))$ or $O(n \cdot \mathsf{MM}(n, \log \|A\|))$ operations,

▷ $\mathbf{MM(n, d)} = O\tilde{}(n^\omega d)$: cost for multiplying $n \times n$ matrices of degree d

▷ $\mathbf{MM(n, \log \|A\|)} = O\tilde{}(n^\omega \log \|A\|)$: cost for multiplying $n \times n$ integer matrices

The determinant can be computed in

in $O(n \cdot \mathrm{MM}(n, d))$ or $O(n \cdot \mathrm{MM}(n, \log \|A\|))$ operations,

i.e. in say *n* corresponding matrix products

Fundamentals of dense linear algebra over $\mathsf{K}[x]$ or $\mathbb{Z}$

Monte Carlo rank	$O(n^\omega + n^2 \log \|A\|)$
System solution (Hensel lifting) [Moenck & Carter 79, Dixon 82]	$\tilde{O}(n^3 \log \|A\|)$
Determinant, **inversion**, **nullspace**, **rank**, . . . [Edmonds 67, Bareiss 69, Moenck & Carter 79]	$\tilde{O}(\mathbf{n} \cdot \mathsf{MM}(n, \log \|A\|))$ Deterministic
Frobenius form (minimum, **characteristic polynomial**) [Giesbrecht 93, Giesbrecht & Storjohann 02]	$\tilde{O}(\mathbf{n} \cdot \mathsf{MM}(n, \log \|A\|))$ Las Vegas
Hermite and **Smith forms**, (diophantine systems) [Kannan & Bachem 79, Domich 85, Giesbrecht 95, Storjohann 96-00]	$\tilde{O}(\mathbf{n} \cdot \mathsf{MM}(n, \log \|A\|))$ Deterministic

$$\boxed{\textbf{Bit complexity} \preceq \textbf{algebraic complexity} \times \textbf{output size}}$$

$$\boxed{\textbf{Bit complexity} \preceq \textbf{algebraic complexity} \times \textbf{output size}}$$

Is this bound pessimistic ?

Minimal bases

$A \in \mathsf{K}[x]^{m \times 2m}$

$$A(x)G(x) = \begin{bmatrix} P(x) & Q(x) \end{bmatrix} \begin{bmatrix} -P(x)^{-1}Q(x) \\ -I \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix}$$

$A \in \mathsf{K}[x]^{m \times 2m}$

$$A(x)G(x) = \begin{bmatrix} P(x) & Q(x) \end{bmatrix} \begin{bmatrix} -P(x)^{-1}Q(x) \\ -I \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix}$$

$$A(x)N(x) = \begin{bmatrix} P(x) & Q(x) \end{bmatrix} \begin{bmatrix} M_1(x) \\ M_2(x) \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix} \pmod{x^\sigma}$$

Degree $= 1$, $m = 6$

```
> RandomMatrix(n,2*n,generator=rr);
```

$$\begin{bmatrix} 2x+4 & 7x+8 & 4x+10 & 10x+4 & 5x+4 & 3x+9 & 6x+3 & 7x+7 & 9x & 5x+1 & 10x+4 & 3x \\ 10x+5 & 3x+7 & 10x+7 & 3x+3 & 9x & 2 & 6x+7 & 5x+8 & 3 & 3 & 5x+9 & 10x \\ 6x+9 & 8x+1 & 6x+7 & 2x+7 & 9x+8 & 5x+7 & 3x+4 & 2x+3 & 8x+4 & 5x & 2x+3 & 7x+1 \\ 2x+10 & x+10 & 10x+5 & 8x+9 & 8x+7 & 2x+6 & 8x+4 & 7x+7 & 2x+6 & 4x+2 & 10 & 3x+7 \\ 9x+3 & x+5 & 7 & 6x+10 & 5x+1 & 6x+7 & 3 & x+7 & 2x+7 & 7x+5 & 9x+4 & 8x+10 \\ 2x+8 & 8x+9 & 9x+2 & 7x+6 & 3x+9 & 4x+7 & 6x+5 & 4x+5 & 2x+4 & 4x+6 & 9x+3 & 6x+10 \end{bmatrix}$$

```
>
```

6×6 minors of degree $md = 6$

$$
\begin{bmatrix}
\frac{5x^6+3x^5+10x^4+4x^3+7x^2+10x+6}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{9x^6+4x^5+7x^4+6x^3+4x^2+8x}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{2x^6+2x^5+2x^4+2x^3+5x^2+2x}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{9x^6+3x^5}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{5x^6+4x^5+8x^4+5x^3+x^2+5x+7}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{x^6+5x^5+10x^4+5x^3+7x^2+5x+7}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} \\
\frac{10x^6+2x^5+5x^4+9x^3+2x^2+7x+2}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{2x^5+8x^4+3x^3+4x^2+4x+8}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{8x^6+9x^5+3x^4+6x^3+7x^2+7x+7}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{8x^6+5x^5+8x^4+2x^3+3x^2+10}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{7x^6+2x^5+3x^4+6x^3+6x^2+2x+7}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{10x^6+x^5+5x^3+6x^2+4x+5}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} \\
\frac{6x^6+10x^5+x^4+9x^3+6x^2+8x+4}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{6x^6+4x^5+5x^4+x^3+10x^2+7x+2}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{2x^6+10x^5+2x^4+x^3+10x^2+2x+7}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{x^6+x^4+9x^3+7x^2+4x+9}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{8x^6+5x^5+7x^4+4x^3+5x^2+9x+1}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{4x^6+x^4+8x^3+2x^2+6x+2}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} \\
\frac{4x^6+6x^5+5x^4+2x^3+x^2+10}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{4x^6+2x^5+10x^4+5x^3+x+8}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{5x^5+6x^4+3x^3+4x^2+2x+6}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{x^6+8x^5+9x^4+x^3+3x^2+4x+6}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{6x^6+7x^5+8x^4+7x^3+9x^2+5}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{x^6+3x^5+4x^4+8x^3+2x^2+8x+6}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} \\
\frac{2x^6+8x^5+9x^4+3x^3+9x^2+3x+8}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{x^6+6x^5+10x^4+8x^3+6x^2+2x+7}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{10x^6+5x^5+2x^4+2x^3+3x^2+7}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{3x^6+6x^5+9x^4+x^3+9x+9}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{10x^6+10x^5+2x^4+4x^3+6x^2+5x+5}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{8x^6+8x^5+10x^4+7x^3+4x^2+3x+7}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} \\
\frac{9x^6+9x^5+5x^4+9x^3+6x^2+5x+6}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{9x^6+2x^5+5x^3+4x^2+10x+4}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{9x^6+6x^5+6x^4+7x^3+10x^2+6x+1}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{8x^6+3x^5+9x^4+7x^3+10x^2+2x}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{3x^6+10x^5+9x^4+8x^3+x^2+2x+3}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} & \frac{8x^6+8x^5+8x^4+7x^3+10x^2+2x+4}{x^6+3x^5+5x^4+9x^3+7x^2+4x+1} \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
$$

“Small” nullspace basis computed via approximants at “sufficiently large” order

```
> PMbasis(M,[seq(0,i=1..2*n)],8,x) mod q: %[1..2*n,n+1..2*n];
```

$$\begin{bmatrix} 5x+10 & 9x+5 & 9x+5 & 7 & 5x+5 & x+4 \\ 10x & 7 & 9x+6 & 9x+10 & 7x+8 & 5x+8 \\ 6x+9 & 6x+3 & 4x & 7x+3 & 10x+2 & 10x \\ 4x+8 & 4x+7 & 5x+2 & 6x+5 & 5x+4 & 5x+8 \\ 2x+10 & x+1 & 2x+2 & 9x & 4x+9 & 8x+2 \\ 9x & 9x+5 & x+5 & 7x+4 & 3x+6 & 4x+1 \\ x+10 & 0 & 10x+8 & 4x & 4x+9 & 3x \\ 2 & x+1 & 5x+9 & 6 & 7x+9 & 4x+9 \\ 10 & 4 & x+4 & 2x+3 & 7x+5 & 2x+7 \\ 1 & 5 & 6 & x+8 & 10x+6 & 2x+8 \\ 7 & 9 & 5 & 5 & x+6 & 3x+5 \\ 0 & 9 & 3 & 7 & 9 & x+5 \end{bmatrix}$$

Theorem: Generically, $A \in \mathsf{K}[x]^{m \times 2m}$ of degree d has a nullspace basis of degree d

Generically: unless the entries of A form a zero of a multivariate polynomial in $\mathsf{K}[a_{11}, \ldots, a_{ij}, \ldots, a_{nn}]$

Hint: true for $A(x) = [\bar{A}(x) \;\; I]$

$A \in \mathsf{K}[x]^{m \times 2m}$

Assumption: there exists a nullspace basis of degree d

$\longrightarrow$ $B \in \mathsf{K}[x]^{(2m)\times(2m)}$ a minimal approximant basis at order $2d+1$:

$$A(x)B(x) = 0 \bmod x^{2d+1}$$

$A \in \mathsf{K}[x]^{m \times 2m}$

Assumption: there exists a nullspace basis of degree d

$\longrightarrow$ $B \in \mathsf{K}[x]^{(2m) \times (2m)}$ a minimal approximant basis at order $2d+1$:

$$A(x)B(x) = 0 \bmod x^{2d+1}$$

- If $A(x)u(x) = 0$ then $u(x)$ is in the module of the columns of $B(x)$

$A \in \mathsf{K}[x]^{m \times 2m}$

Assumption: there exists a nullspace basis of degree d

$\rightarrow$ $B \in \mathsf{K}[x]^{(2m)\times(2m)}$ a minimal approximant basis at order $2d+1$:

$$A(x)B(x) = 0 \bmod x^{2d+1}$$

- If $A(x)u(x) = 0$ then $u(x)$ is in the module of the columns of $B(x)$
- By minimality $B(x)$ has at least m columns of degree bounded by d

$A \in \mathsf{K}[x]^{m\times 2m}$

Assumption: there exists a nullspace basis of degree d

$\rightarrow$ $B \in \mathsf{K}[x]^{(2m)\times(2m)}$ a minimal approximant basis at order $2d+1$:

$$A(x)B(x) = 0 \bmod x^{2d+1}$$

- If $A(x)u(x) = 0$ then $u(x)$ is in the module of the columns of $B(x)$
- By minimality $B(x)$ has at least m columns of degree bounded by d
- If $\deg u(x) \leq d$ then $A(x)u(x) = 0 \bmod x^{2d+1} \implies B(x)u(x) = 0$

$A \in \mathsf{K}[x]^{m \times 2m}$

Assumption: there exists a nullspace basis of degree d

$\rightarrow$ $B \in \mathsf{K}[x]^{(2m)\times(2m)}$ a minimal approximant basis at order $2d+1$:

$$A(x)B(x) = 0 \bmod x^{2d+1}$$

- If $A(x)u(x) = 0$ then $u(x)$ is in the module of the columns of $B(x)$
- By minimality $B(x)$ has at least m columns of degree bounded by d
- If $\deg u(x) \leq d$ then $A(x)u(x) = 0 \bmod x^{2d+1} \implies B(x)u(x) = 0$
- $B(x)$ has exactly m columns of degree d (others are of larger degree)

$A \in \mathsf{K}[x]^{m \times 2m}$

Assumption: there exists a nullspace basis of degree d

$\rightarrow$ $B \in \mathsf{K}[x]^{(2m)\times(2m)}$ a minimal approximant basis at order $2d+1$:

$$A(x)B(x) = 0 \bmod x^{2d+1}$$

$$A(x)B(x) = 0$$

Corollary: A nullspace basis can be computed in $\tilde{O}(n^{\omega}d)$ operations in K.

New elimination

Divide and conquer

[Strassen 1969, Schönhage 1973, Bunch & Hopcroft 1974]

$$\begin{bmatrix} I & 0 \\ -BA^{-1} & I \end{bmatrix} \cdot \begin{bmatrix} A & C \\ B & D \end{bmatrix} = \begin{bmatrix} A & C \\ 0 & D - BA^{-1}C \end{bmatrix}$$

At next step :

$\hookrightarrow$ Dimension: divided by two

Divide and conquer

[Strassen 1969, Schönhage 1973, Bunch & Hopcroft 1974]

$$\begin{bmatrix} I & 0 \\ -BA^{-1} & I \end{bmatrix} \cdot \begin{bmatrix} A & C \\ B & D \end{bmatrix} = \begin{bmatrix} A & C \\ 0 & D - B\mathbf{A^{-1}}C \end{bmatrix}$$

At next step :

$\hookrightarrow$ Dimension: divided by two

$\hookrightarrow$ **Entry size : multiplied by $\mathbf{n/2}$**

Divide-double and conquer

The **dimension is divided by two** while the **entry size is at most doubled**

$$\Rightarrow \text{Cost: } \sum_{i=1}^{\log n} \left(\frac{n}{2^i}\right)^{\omega} 2^i d = O(\mathbf{n^{\omega} d})$$

degree d **degree 2d**

$$A = \begin{bmatrix} * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \end{bmatrix} \quad \rightarrow \quad BA = \begin{bmatrix} * & * & * & * & & & & \\ * & * & * & * & & & & \\ * & * & * & * & & & & \\ * & * & * & * & & & & \\ & & & & * & * & * & * \\ & & & & * & * & * & * \\ & & & & * & * & * & * \\ & & & & * & * & * & * \end{bmatrix}$$

$$\begin{bmatrix} \overline{B} \\ \underline{B} \end{bmatrix} \begin{bmatrix} A_L & A_R \end{bmatrix} = \begin{bmatrix} A'_L & 0 \\ 0 & A'_R \end{bmatrix}$$

Minimal bases diagonalization

$$A = \begin{bmatrix} * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \end{bmatrix}$$

$$BA = \begin{bmatrix} * & * & * & * & & & & \\ * & * & * & * & & & & \\ * & * & * & * & & & & \\ * & * & * & * & & & & \\ & & & & * & * & * & * \\ & & & & * & * & * & * \\ & & & & * & * & * & * \\ & & & & * & * & * & * \end{bmatrix}$$

$$B'BA = \begin{bmatrix} * & * & & & & & & \\ * & * & & & & & & \\ & & * & * & & & & \\ & & * & * & & & & \\ & & & & * & * & & \\ & & & & * & * & & \\ & & & & & & * & * \\ & & & & & & * & * \end{bmatrix}$$

$$B''B'BA = \begin{bmatrix} * & & & & & & & \\ & * & & & & & & \\ & & * & & & & & \\ & & & * & & & & \\ & & & & * & & & \\ & & & & & * & & \\ & & & & & & * & \\ & & & & & & & * \end{bmatrix} = D$$

[Jeannerod & Villard 2005] [Zhou, Labahn & Storjohann 2015]

Theorem: The inverse of a polynomial matrix of degree d can be computed in essentially optimal time $\tilde{O}(n^3 d)$

[Jeannerod & Villard 2005] [Zhou, Labahn & Storjohann 2015]

Theorem: The inverse of a polynomial matrix of degree d can be computed in essentially optimal time $\tilde{O}(n^3 d)$

Hint:

- Generically: show that minimal bases with appropriate degrees exist recursively
- General case: manage unbalanced degrees in nullspace basis

For $\xi \geq 1$, let $T(n, \xi)$ be a bound on the cost of the algorithm with input $(\mathbf{F} \in \mathbb{K}[x]^{n\times n}, \vec{s} \in \mathbb{Z}^n)$ that satisfies $\sum \vec{s} \leq \xi$.

$$T(n, \xi) \leq T(\lfloor n/2 \rfloor, \xi) + T(\lceil n/2 \rceil, \xi) + (n^{\omega}(1 + \xi/n))^{1+o(1)}.$$

$$A, A^2, \ldots, A^n \text{ ?}$$

$$A, A^2, \ldots, A^n \ ?$$

1. Inverse $(I - xA)$

$$A, A^2, \ldots, A^n \ ?$$

1. Inverse $(I - xA)$
2. Expand the entries modulo x^{n+1}

   $(I - xA)^{-1} = I + xA + x^2A^2 + \ldots + x^nA^n \bmod x^{n+1}$

Cost: $\tilde{O}(n^3)$ operations in K, essentially optimal

Exercise: For $A \in \mathsf{K}[x]^{m\times 2m}$ of degree d we are given an algorithm `ApproximantBasis(A,`δ`)` thats returns a minimal approximant basis at order $\delta \geq d$ in time $\tilde{O}(m^\omega \delta)$. For $M \in \mathsf{K}^{n\times n}$, give an algorithm for computing $M, M^2, \ldots, M^n$ in $\tilde{O}(n^3)$ operations in K. You will assume (property of genericity) that for any $A \in \mathsf{K}[x]^{m\times 2m}$ encountered for some m and d during the algorithm, there exists a nullspace basis of degree d; also assume that n is a power of 2.

Theorem of matrix polynomials $A(x) \in \mathsf{K}[x]^{n \times n}$ of degree d

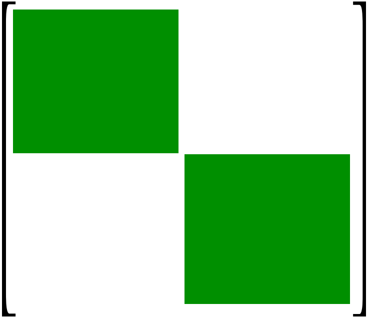
In $\tilde{O}(n^\omega d)$ (sometimes say $\tilde{O}(\mathsf{MM}(n,d))$) arithmetic operations one can compute:

- The determinant
- A linear system solution, right hand side of degree $O(nd)$
- A minimal basis of the module
- The Hermite and the Smith normal forms

Rectangular case

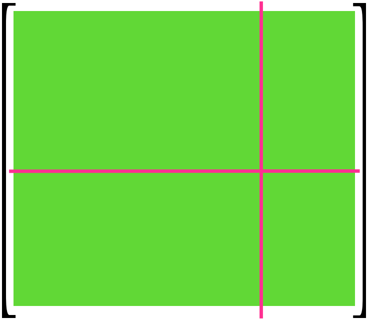
- $m \times n$, $m \leq n$, minimal basis in $\tilde{O}(m^{\omega-1}nd)$
- Nullspace basis in $\tilde{O}(mnr^{\omega-2}d)$

Divide-double & conquer : slight increase in size



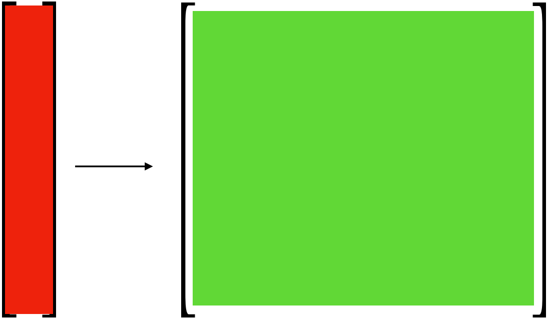
Size versus dimension

Odd slicing



Slicing + overlapping

Linearization



Theorem of integer matrices $A(x) \in \mathbb{Z}^{n \times n}$, entries of size β

In $\tilde{O}(n^\omega \beta)$ (sometimes say $\tilde{O}(\mathsf{MM}(n, \beta))$ arithmetic operations one can compute:

- The determinant
- A linear system solution, right hand side of size $O(n\beta)$
- The (certified) rank
- The Smith normal forms (non singular case)
- Matrix inverse in $\tilde{O}(n^3(\beta + \log \kappa(A)))$

Open problems

Understanding the link with corresponding matrix multiplication?

$\rightsquigarrow$ $\mathsf{K}[x]$ **and** $\mathbb{Z}$**: Characteristic polynomial**

$\rightsquigarrow$ $\mathbb{Z}$**: LLL lattice basis reduction**