Computation of normal forms for polynomial and maybe Ore matrices

George Labahn

Symbolic Computation Group
University of Waterloo, Canada

Workshop on Computer Algebra and Combinatorics
Vienna November 13-17, 2017

Hermite Normal Forms

Given nonsingular $\mathbf{A} \in \mathbb{K}[D]^{n\times n}$. Compute $\mathbf{U}$ and $\mathbf{H}$:

(i) $\mathbf{U}$ unimodular, i.e. invertible in $\mathbb{K}[D]^{n\times n}$

(iii) $\mathbf{U} \cdot \mathbf{A} = \mathbf{H}$

(iii) $\mathbf{H}$ in (row) Hermite form , i.e.

$$\mathbf{H} = \begin{bmatrix} h_{11} & h_{12} & \cdots & \cdots & h_{1n} \\ 0 & h_{22} & h_{23} & & h_{2n} \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & h_{n-1,n} \\ 0 & \cdots & \cdots & 0 & h_{nn} \end{bmatrix}$$

h_{ii} monic

$\deg h_{ji} < \deg h_{ii}$.

Popov Normal Form

Given nonsingular $\mathbf{A} \in \mathbb{K}[D]^{n \times n}$. Compute $\mathbf{U}$ and $\mathbf{P}$:

(i) $\mathbf{U}$ unimodular,

(iii) $\mathbf{U} \cdot \mathbf{A} = \mathbf{P}$

(iii) $\mathbf{P}$ in (row) Popov form , i.e. after possibly permuting rows

$$\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} & p_{13} & \cdots & p_{1n} \\ p_{21} & p_{22} & p_{23} & & p_{2n} \\ \vdots & \vdots & p_{33} & \ddots & \vdots \\ \vdots & \vdots & & \ddots & p_{n-1,n} \\ p_{n1} & p_{n,2} & p_{n,3} & \cdots & p_{nn} \end{bmatrix}$$

lcoeff $(\mathbf{P})$ special

More on Normal forms

- Hermite : solving systems of linear equations
- Popov :
  - convert Transfer function representation to linear system representation in linear systems theory
  - also called *Polynomial Echelon Form* in Kailath
- Also shifted Popov form : one rescales the row degrees
- Also two sided Smith and Jacobson Forms (Mark's talk)

Example: Conversion to first order

Higher order system of linear differential equations

$$
\begin{array}{rcrcrcl}
y_1''(t) + (t+2)y_1(t) & + & t^2 y_2''(t) + y_2(t) & + & y_3'(t) + y_3(t) & = & 0 \\
y_1''(t) - 3y_1(t) & + & 2t^2 y_2''(t) + y_2'(t) + y_2(t) & + & y_3'''''(t) - y_3'''(t) + 2t^2 y_3(t) & = & 0 \\
y_1'(t) + y_1(t) & + & y_2''(t) + 2t y_2'(t) - y_2(t) & + & y_3''''(t) & = & 0.
\end{array}
$$

Example: Conversion to first order

Higher order system of linear differential equations

$$\begin{array}{rcrcrcl} y_1''(t) + (t+2)y_1(t) & + & t^2 y_2''(t) + y_2(t) & + & y_3'(t) + y_3(t) & = & 0 \\ y_1''(t) - 3y_1(t) & + & 2t^2 y_2''(t) + y_2'(t) + y_2(t) & + & y_3'''''(t) - y_3'''(t) + 2t^2 y_3(t) & = & 0 \\ y_1'(t) + y_1(t) & + & y_2''(t) + 2t y_2'(t) - y_2(t) & + & y_3''''(t) & = & 0. \end{array}$$

Represent system in operator form

$$\begin{bmatrix} D^2 + (t+2) & t^2 D^2 + 1 & D + 1 \\ D^2 - 3 & 2tD^2 + D + 1 & D^5 - D^3 + 2t^2 \\ D + 1 & D^2 + 2tD + 1 & D^4 \end{bmatrix} \cdot \begin{bmatrix} y_1(t) \\ y_2(t) \\ y_3(t) \end{bmatrix} = \mathbf{0}.$$

Example

Higher order system of linear differential equations

$$\begin{array}{rcrcrcl} y_1''(t) + (t+2)y_1(t) & + & t^2 y_2''(t) + y_2(t) & + & y_3'(t) + y_3(t) & = & 0 \\ y_1'(t) + 3y_1(t) & + & y_2'''(t) + 2y_2'(t) - y_2(t) & + & y_3'''(t) - 2t^2 y_3(t) & = & 0 \\ y_1'(t) + y_1(t) & + & y_2''(t) + 2ty_2'(t) - y_2(t) & + & y_3''''(t) & = & 0. \end{array}$$

Represent system in operator form

$$\begin{bmatrix} D^2 + (t+2) & t^2 D^2 + 1 & D + 1 \\ D + 3 & D^3 + 2D - 1 & D^3 - 2t^2 \\ D + 1 & D^2 + 2tD + 1 & D^4 \end{bmatrix} \cdot \begin{bmatrix} y_1(t) \\ y_2(t) \\ y_3(t) \end{bmatrix} = \mathbf{0}.$$

Example

Higher order system of linear differential equations

$$\begin{array}{rcrcrcl} y_1''(t) + (t+2)y_1(t) & + & t^2 y_2''(t) + y_2(t) & + & y_3'(t) + y_3(t) & = & 0 \\ y_1'(t) + 3y_1(t) & + & y_2'''(t) + 2y_2'(t) - y_2(t) & + & y_3'''(t) - 2t^2 y_3(t) & = & 0 \\ y_1'(t) + y_1(t) & + & y_2''(t) + 2ty_2'(t) - y_2(t) & + & y_3''''(t) & = & 0. \end{array}$$

Represent system in operator form

$$\begin{bmatrix} D^2 + (t+2) & t^2 D^2 + 1 & D + 1 \\ D + 3 & D^3 + 2D - 1 & D^3 - 2t^2 \\ D + 1 & D^2 + 2tD + 1 & D^4 \end{bmatrix} \cdot \begin{bmatrix} y_1(t) \\ y_2(t) \\ y_3(t) \end{bmatrix} = \mathbf{0}.$$

$$\text{(row) Lcoeff} = \begin{bmatrix} 1 & t^2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Example

Higher order system of linear differential equations

$$\begin{array}{rcrcrcl} y_1''(t) + (t+2)y_1(t) & + & t^2 y_2''(t) + y_2(t) & + & y_3'(t) + y_3(t) & = & 0 \\ y_1'(t) + 3y_1(t) & + & y_2'''(t) + 2y_2'(t) - y_2(t) & + & y_3'''(t) - 2t^2 y_3(t) & = & 0 \\ y_1'(t) + y_1(t) & + & y_2''(t) + 2ty_2'(t) - y_2(t) & + & y_3''''(t) & = & 0. \end{array}$$

Represent system in operator form

$$\begin{bmatrix} D^2 + (t+2) & t^2 D^2 + 1 & D + 1 \\ D + 3 & D^3 + 2D - 1 & D^3 - 2t^2 \\ D + 1 & D^2 + 2tD + 1 & D^4 \end{bmatrix} \cdot \begin{bmatrix} y_1(t) \\ y_2(t) \\ y_3(t) \end{bmatrix} = \mathbf{0}.$$

$$\text{(row) Lcoeff} = \begin{bmatrix} 1 & t^2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{(col) Lcoeff} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Example

Change to new higher order system

$$\begin{array}{rcrcrcl} y_1''(t) + (t+2)y_1(t) & + & t^2y_2''(t) + y_2(t) & + & y_3'(t) + y_3(t) & = & 0 \\ y_1'(t) + 3y_1(t) & + & y_2'''(t) + 2y_2'(t) - y_2(t) & + & y_3'''(t) - 2t^2y_3(t) & = & 0 \\ y_1'(t) + y_1(t) & + & y_2''(t) + 2ty_2'(t) - y_2(t) & + & y_3''''(t) & = & 0. \end{array}$$

Represent system in operator form

$$\begin{bmatrix} D^2 + (t+2) & t^2D^2 + 1 & D + 1 \\ D + 3 & D^3 + D + 1 & D^3 - 2t^2 \\ D + 1 & D^2 + 2tD + 1 & D^4 \end{bmatrix} \cdot \begin{bmatrix} y_1(t) \\ y_2(t) \\ y_3(t) \end{bmatrix} = \mathbf{0}.$$

Hence can rewrite as

$$y_1''(t) = -(t+2)y_1(t) - t^2y_2''(t) - y_2(t) - y_3'(t) - y_3(t)$$

$$y_2'''(t) = -y_1'(t) - 3y_1(t) - 2y_2'(t) + y_2(t) - y_3'''(t) + 2t^2y_3(t)$$

$$y_3''''(t) = -y_1'(t) - y_1(t) - y_2''(t) - 2ty_2'(t) - y_2(t)$$

Hermite and Popov are connected:

Monomials on vectors $\mathbb{K}^{1\times n}[z]$:

$$z^{\alpha} e_j = [0, \ldots, 0, z^{\alpha}, 0, \ldots, 0]$$

Ordering on monomials of $\mathbb{K}^{1\times n}[z]$:

- Position over Term (POT):

$$z^{\alpha} e_i < z^{\beta} e_j \quad \Longleftrightarrow \quad i < j \quad \text{or } i = j \text{ and } \alpha < \beta$$

If M submodule of $\mathbb{K}^{1\times n}[z]$ then can speak of Gröbner bases.

Hermite and Popov are connected:

Monomials on vectors $\mathbb{K}^{1\times n}[z]$:

$$z^{\alpha}e_j = [0, \ldots, 0, z^{\alpha}, 0, \ldots, 0]$$

Ordering on monomials of $\mathbb{K}^{1\times n}[z]$:

- Position over Term (POT):

$$z^{\alpha}e_i < z^{\beta}e_j \quad \Longleftrightarrow \quad i < j \quad \text{or } i = j \text{ and } \alpha < \beta$$

If M submodule of $\mathbb{K}^{1\times n}[z]$ then can speak of Gröbner bases.

POT reduced Gröbner bases for $M \iff M$ in Hermite Form.

Hermite and Popov are connected:

Monomials on vectors $\mathbb{K}^{1\times n}[z]$:

$$z^\alpha e_j = [0,\ldots,0,z^\alpha,0,\ldots,0]$$

Ordering on monomials of $\mathbb{K}^{1\times n}[z]$:

- Term over Position (TOP):

$$z^\alpha e_i < z^\beta e_j \quad \Longleftrightarrow \quad \alpha < \beta \ \text{ or } i = j \text{ and } i < j$$

If M submodule of $\mathbb{K}^{1\times n}[z]$ then can speak of Gröbner bases.

TOP reduced Gröbner bases for $M \iff M$ in Popov Form.

Hermite and Popov are connected:

Monomials on vectors $\mathbb{K}^{1\times n}[z]$:

$$z^{\alpha} e_j = [0, \ldots, 0, z^{\alpha}, 0, \ldots, 0]$$

Ordering on monomials of $\mathbb{K}^{1\times n}[z]$:

- Term over Position (TOP):

$$z^{\alpha} e_i < z^{\beta} e_j \quad \Longleftrightarrow \quad \alpha < \beta \quad \text{or } i = j \text{ and } i < j$$

If M submodule of $\mathbb{K}^{1\times n}[z]$ then can speak of Gröbner bases.

TOP reduced Gröbner bases for $M \Longleftrightarrow M$ in Popov Form.

Hermite to Popov via FGLM: PhD thesis J. Middeke (2011)

Computation in Polynomial Domains

Polynomial Matrices

- Fast, deterministic algorithms for Hermite and Popov
- Complexity : $O^{\sim}(n^{\omega}\lceil s \rceil)$ where s bounded by average
  : of row and column degrees of $\mathbf{A}$
  : output size $O(n^2 s)$, $\Longrightarrow$ good complexity.

Polynomial Matrices

- Fast, deterministic algorithms for Hermite and Popov
- Complexity : $O\tilde{}\,(n^{\omega}\lceil s\rceil)$ where s bounded by average
  : of row and column degrees of $\mathbf{A}$
  : output size $O(n^2 s)$, $\Longrightarrow$ good complexity.

- G. Labahn, V. Neiger and W. Zhou, Fast, deterministic computation of determinants and Hermite normal forms of polynomial matrices, To appear in Journal of Complexity
- V. Neiger and Thi Xuan Vu, Computing Canonical Bases of Modules of Univariate Relations, Proceedings of ISSAC'17, (2017).

Previous work : Hermite Form

- Polynomial-time over $\mathbb{Q}[x]$: Kannan 1985.
- $O\tilde{}(n^4 d)$: Hafner-McCurley 1991 deterministic
- $O\tilde{}(n^{\omega+1} d)$: Hafner-McCurley (1991), Villard (1996) Storjohann and L. (1996) deterministic
- $O\tilde{}(n^3 d^2)$: Mulders and Storjohann (2003) deterministic
- $O\tilde{}(n^3 d)$: Gupta and Storjohann (2012) probabilistic
- $O\tilde{}(n^\omega d)$: Gupta and Storjohann (2012) probabilistic
- $O\tilde{}(n^\omega s)$: L.-Neiger-Zhou deterministic

Techniques

(1) Triangularize
   - Finding Diagonals
   - Complexity

(2) Normalize to Hermite Form

(3) Normalize to (shifted) Popov Form

Finding Diagonal Elements

Given nonsingular $\mathbf{A}$: Partition $\mathbf{U}$ and $\mathbf{A}$ and reduce via

$$\mathbf{U} \cdot \mathbf{A} = \begin{bmatrix} \mathbf{U}_u \\ \mathbf{U}_d \end{bmatrix} \begin{bmatrix} \mathbf{A}_\ell & \mathbf{A}_r \end{bmatrix} = \begin{bmatrix} \mathbf{B}_1 & * \\ 0 & \mathbf{B}_2 \end{bmatrix}.$$

Finding Diagonal Elements

Given nonsingular $\mathbf{A}$: Partition $\mathbf{U}$ and $\mathbf{A}$ and reduce via

$$\mathbf{U} \cdot \mathbf{A} = \begin{bmatrix} \mathbf{U}_u \\ \mathbf{U}_d \end{bmatrix} \begin{bmatrix} \mathbf{A}_\ell & \mathbf{A}_r \end{bmatrix} = \begin{bmatrix} \mathbf{B}_1 & * \\ 0 & \mathbf{B}_2 \end{bmatrix}.$$

Here

(i) $\mathbf{U}_d$ a left kernel basis of $\mathbf{A}_\ell$

(ii) $\mathbf{B}_1$ $(= \mathbf{U}_u \cdot \mathbf{A}_\ell)$ is nonsingular and a row basis of $\mathbf{A}_\ell$.

(iii) $\mathbf{B}_2 = \mathbf{U}_d \cdot \mathbf{A}_r$,

Recurse on $\mathbf{B}_1$ and $\mathbf{B}_2$ to get diagonal elements

Finding Diagonal Elements

Given nonsingular $\mathbf{A}$: Partition $\mathbf{U}$ and $\mathbf{A}$ and reduce via

$$\mathbf{U} \cdot \mathbf{A} = \begin{bmatrix} \mathbf{U}_u \\ \mathbf{U}_d \end{bmatrix} \begin{bmatrix} \mathbf{A}_\ell & \mathbf{A}_r \end{bmatrix} = \begin{bmatrix} \mathbf{B}_1 & * \\ 0 & \mathbf{B}_2 \end{bmatrix}.$$

Here

(i) $\mathbf{U}_d$ a left kernel basis of $\mathbf{A}_\ell$

(ii) $\mathbf{B}_1$ $(= \mathbf{U}_u \cdot \mathbf{A}_\ell)$ is nonsingular and a row basis of $\mathbf{A}_\ell$.

(iii) $\mathbf{B}_2 = \mathbf{U}_d \cdot \mathbf{A}_r$,

Recurse on $\mathbf{B}_1$ and $\mathbf{B}_2$ to get diagonal elements

Important to control size (measured by row degrees).

Finding Diagonal Elements

Given nonsingular $\mathbf{A}$: Partition $\mathbf{U}$ and $\mathbf{A}$ and reduce via

$$\mathbf{U} \cdot \mathbf{A} = \begin{bmatrix} \mathbf{U}_u \\ \mathbf{U}_d \end{bmatrix} \begin{bmatrix} \mathbf{A}_\ell & \mathbf{A}_r \end{bmatrix} = \begin{bmatrix} \mathbf{B}_1 & * \\ 0 & \mathbf{B}_2 \end{bmatrix}.$$

Here

(i) $\mathbf{U}_d$ a left kernel basis of $\mathbf{A}_\ell$

(ii) $\mathbf{B}_1$ $(= \mathbf{U}_u \cdot \mathbf{A}_\ell)$ is nonsingular and a row basis of $\mathbf{A}_\ell$.

(iii) $\mathbf{B}_2 = \mathbf{U}_d \cdot \mathbf{A}_r$,

Recurse on $\mathbf{B}_1$ and $\mathbf{B}_2$ to get diagonal elements

Important to control size (measured by row degrees).

Cannot actually compute all of $\mathbf{U}$ - it's too big.

Approach for Hermite

- Triangularize $\mathbf{A}$ (fast for all 3 steps)
  - Gives diagonal entries of $\mathbf{H}$ which can be large
- Reduce remaining off-diagonal entries (fast)
- Remember: Avoid computing unimodular multiplier $\mathbf{U}$

Size measures : Shifted Degrees

- The row degree of a row vector $\mathbf{p}$ is

$$\operatorname{rdeg} \mathbf{p} \quad = \quad \max_{1 \le i \le n} \left[\deg p^{(i)} \right].$$

Size measures : Shifted Degrees

- The row degree of a row vector $\mathbf{p}$ is

$$\operatorname{rdeg} \mathbf{p} \quad = \quad \max_{1 \le i \le n} \left[\deg p^{(i)} \right].$$

- The $\vec{s}$-row degree of $\mathbf{p}$ is

$$\operatorname{rdeg}_{\vec{s}} \mathbf{p} \quad = \quad \max_{1 \le i \le n} \left[\deg p^{(i)} + s_i \right] \quad = \quad \operatorname{rdeg} \mathbf{p} \cdot x^{\vec{s}}.$$

- e.g. $\operatorname{rdeg} \begin{bmatrix} x & x^2 \end{bmatrix} = 2, \;\; \operatorname{rdeg}_{[3,1]} \begin{bmatrix} x & x^2 \end{bmatrix} = \operatorname{rdeg} \begin{bmatrix} x^4 & x^3 \end{bmatrix} = 4$

Size measures : Shifted Degrees

- The row degree of a row vector $\mathbf{p}$ is

$$\operatorname{rdeg} \mathbf{p} \quad = \quad \max_{1 \le i \le n} \left[\deg p^{(i)} \right].$$

- The $\vec{s}$-row degree of $\mathbf{p}$ is

$$\operatorname{rdeg}_{\vec{s}} \mathbf{p} \quad = \quad \max_{1 \le i \le n} \left[\deg p^{(i)} + s_i \right] \quad = \quad \operatorname{rdeg} \mathbf{p} \cdot x^{\vec{s}}.$$

- e.g. $\operatorname{rdeg} \begin{bmatrix} x & x^2 \end{bmatrix} = 2, \quad \operatorname{rdeg}_{[3,1]} \begin{bmatrix} x & x^2 \end{bmatrix} = \operatorname{rdeg} \begin{bmatrix} x^4 & x^3 \end{bmatrix} = 4$

- For any matrix $\mathbf{A}$: $\quad \operatorname{rdeg}_{-\vec{s}} \mathbf{A} \le 0$ same as $\operatorname{cdeg} \mathbf{A} \le \vec{s}$

Minimal Kernel Bases

Given $\mathbf{F} \in \mathbb{K}[z]^{m\times n}, \quad m \leq n$:

A *Left Kernel Basis* for $\mathbf{F}$ is a $\mathbb{K}[z]$ module basis for

$$\{ \mathbf{p} \in \mathbb{K}[x]^m \mid \mathbf{p} \cdot \mathbf{F} = 0 \}$$

Can represent basis as matrix $\mathbf{M} \in \mathbb{K}[z]^{*\times m}$.

Minimal Kernel Bases

Given $\mathbf{F} \in \mathbb{K}[z]^{m \times n}, \quad m \leq n$:

A *Left Kernel Basis* for $\mathbf{F}$ is a $\mathbb{K}[z]$ module basis for

$$\{ \mathbf{p} \in \mathbb{K}[x]^m \mid \mathbf{p} \cdot \mathbf{F} = 0 \}$$

Can represent basis as matrix $\mathbf{M} \in \mathbb{K}[z]^{* \times m}$.

Minimal Kernel Basis if matrix $\mathbf{M}$ is row reduced,

Shifted $\vec{s}$-Minimal Kernel Basis if $\mathbf{M} \cdot z^{\vec{s}}$ is row reduced.

Row Bases

Given $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$ with $m \geq n$.

A *Row Basis* for $\mathbf{F}$ is a $\mathbb{K}[x]$ module basis for

$$\{ \mathbf{q} \in \mathbb{K}[x]^n \;\mid\; \exists\, \mathbf{p} \in \mathbb{K}[x]^m \quad \text{with} \quad \mathbf{q} = \mathbf{p} \cdot \mathbf{F} \}$$

Row Bases

Given $\mathbf{F} \in \mathbb{K}[x]^{m\times n}$ with $m \geq n$.

A *Row Basis* for $\mathbf{F}$ is a $\mathbb{K}[x]$ module basis for

$$\{\ \mathbf{q} \in \mathbb{K}[x]^n \ \mid\ \exists\ \mathbf{p} \in \mathbb{K}[x]^m \quad \text{with} \quad \mathbf{q} = \mathbf{p}\cdot\mathbf{F}\ \}$$

Again

(i) Represent row basis as full rank matrix $\mathbf{T} \in \mathbb{K}[x]^{r\times n}$.

(ii) Can find unimodular matrix $\mathbf{U}$ with $\mathbf{U}\cdot\mathbf{F} = \begin{bmatrix}\mathbf{T}\\ \mathbf{0}\end{bmatrix}$.

Costs

$\mathbf{F} \in \mathbb{K}[x]^{n\times n}$, $\vec{s} \in \mathbb{Z}^m$ bounds row degrees, $\sum \vec{s} \leq \xi$

Theorem: (Zhou,L,Storjohann) ISSAC (2012)

$\vec{s}$-Minimal left kernel basis computation costs $O^{\sim}(m^{\omega} s)$.

Note: depends on fast order bases computation Zhou-L. (2009)

Costs

$\mathbf{F} \in \mathbb{K}[x]^{n \times n}$, $\vec{s} \in \mathbb{Z}^m$ bounds row degrees, $\sum \vec{s} \leq \xi$

Theorem: (Zhou,L,Storjohann) ISSAC (2012)

$\vec{s}$-Minimal left kernel basis computation costs $O^{\sim}(m^{\omega} s)$.

Note: depends on fast order bases computation Zhou-L. (2009)

Theorem: (Zhou, L (ISSAC 2013)

Row basis computation costs $O^{\sim}(m^{\omega} s)$.

Note: depends on fast Nullspace bases computation.

Complexity

$\mathbf{F} \in \mathbb{K}[x]^{n \times m}$, $\vec{s} \in \mathbb{Z}^n$ bounds row degrees, $\sum \vec{s} \leq \xi$

Theorem

For $\mathbf{M}$ *a* $\vec{s}$*-minimal kernel basis of* $\mathbf{F}$*:* $\sum \operatorname{rdeg}_{\vec{s}} \mathbf{M} \leq \sum \vec{s}$

Theorem

(i) $\mathbf{A} \in \mathbb{K}[x]^{n \times m}$, $m \leq n$, $\vec{s} \in \mathbb{Z}^n$ *bounding row degrees of* $\mathbf{A}$

(ii) $\mathbf{B} \in \mathbb{K}[x]^{k \times n}$ *with* $k \in O(n)$, $\sum \operatorname{rdeg}_{\vec{s}} \mathbf{B} \leq \sum \vec{s} \in O(\xi)$

Multiply $\mathbf{B}$ *and* $\mathbf{A}$ *:* $O^{\sim}(m^2 n^{\omega-2} s) \subset O^{\sim}(n^{\omega} s)$, $s = \xi / n$.

Complexity

$\mathbf{F} \in \mathbb{K}[x]^{n\times m}$, $\vec{s} \in \mathbb{Z}^n$ bounds row degrees, $\sum \vec{s} \leq \xi$

Theorem

For $\mathbf{M}$ *a* $\vec{s}$*-minimal kernel basis of* $\mathbf{F}$*:* $\sum \operatorname{rdeg}_{\vec{s}} \mathbf{M} \leq \sum \vec{s}$

Theorem

(i) $\mathbf{A} \in \mathbb{K}[x]^{n\times m}$, $m \leq n$, $\vec{s} \in \mathbb{Z}^n$ *bounding row degrees of* $\mathbf{A}$

(ii) $\mathbf{B} \in \mathbb{K}[x]^{k\times n}$ *with* $k \in O(n)$, $\sum \operatorname{rdeg}_{\vec{s}} \mathbf{B} \leq \sum \vec{s} \in O(\xi)$

Multiply $\mathbf{B}$ *and* $\mathbf{A}$: $O^{\sim}(m^2 n^{\omega-2} s) \subset O^{\sim}(n^{\omega} s)$, $s = \xi/n$.

Theorem

$\mathbf{A} \in \mathbb{K}[x]^{n\times n}$. *Diagonals costs* $O^{\sim}(n^{\omega}\lceil s\rceil)$ *where* $s = \frac{\sum \operatorname{cdeg} \mathbf{A}}{n}$.

Determinants

Diagonals not enough - need to worry about unimodular part.

Determinants

Diagonals not enough - need to worry about unimodular part.

$$\det \mathbf{A} = \frac{\det \mathbf{B}_1 \cdot \det \mathbf{B}_2}{\det \mathbf{U}}$$

Determinants

Diagonals not enough - need to worry about unimodular part.

$$\det \mathbf{A} = \frac{\det \mathbf{B}_1 \cdot \det \mathbf{B}_2}{\det \mathbf{U}}$$

For $\det \mathbf{U} = \det [\ \mathbf{U}_\ell\ \mathbf{U}_r]$ we do:

1. $\det \mathbf{U} = \det \mathbf{U} \bmod z = \det U = \det [U_\ell, U_r]$
2. $\mathbf{V} = \mathbf{U}^{-1} = \begin{bmatrix} \mathbf{V}_u \\ \mathbf{V}_d \end{bmatrix}$
3. $\mathbf{U}_r$ and $\mathbf{V}_u$ determined in column bases computation
4. Find $U_\ell{}^*$ such that $U^* = [U_\ell{}^*, U_r]$ is unimodular
5. Let $V_u = \mathbf{V}_u \bmod z$. Then $\det \mathbf{U} = \frac{\det U^*}{\det V_u U_\ell{}^*}$

Rest : Reduction of Off-diagonals

Know : $\vec{\delta}$ diagonal degrees of $\mathbf{H}$. Set $\mu = \max(\vec{\delta})$

$$\mathbf{A} \cdot \mathbf{x}^{\vec{\mu}-\vec{\delta}} \xrightarrow{\text{reduce}} \mathbf{R} \cdot \mathbf{x}^{\vec{\mu}-\vec{\delta}} \xrightarrow{\text{normalize}} \mathbf{H} = \operatorname{lc}_{-\vec{\delta}}(\mathbf{R})^{-1} \cdot \mathbf{R}$$

where $\mathbf{R}$ is any $-\vec{\delta}$-row reduced form of $\mathbf{A}$.

Rest : Reduction of Off-diagonals

Know : $\vec{\delta}$ diagonal degrees of $\mathbf{H}$. Set $\mu = \max(\vec{\delta})$

$$\mathbf{A} \cdot \mathbf{x}^{\vec{\mu}-\vec{\delta}} \xrightarrow{\text{reduce}} \mathbf{R} \cdot \mathbf{x}^{\vec{\mu}-\vec{\delta}} \xrightarrow{\text{normalize}} \mathbf{H} = \operatorname{lc}_{-\vec{\delta}}(\mathbf{R})^{-1} \cdot \mathbf{R}$$

where $\mathbf{R}$ is any $-\vec{\delta}$-row reduced form of $\mathbf{A}$.

Problem : Shift $\vec{\mu} - \vec{\delta}$ might be too large

Rest : Reduction of Off-diagonals

Know : $\vec{\delta}$ diagonal degrees of $\mathbf{H}$. Set $\mu = \max(\vec{\delta})$

$$\mathbf{A} \cdot \mathbf{x}^{\vec{\mu}-\vec{\delta}} \xrightarrow{\text{reduce}} \mathbf{R} \cdot \mathbf{x}^{\vec{\mu}-\vec{\delta}} \xrightarrow{\text{normalize}} \mathbf{H} = \mathrm{lc}_{-\vec{\delta}}(\mathbf{R})^{-1} \cdot \mathbf{R}$$

where $\mathbf{R}$ is any $-\vec{\delta}$-row reduced form of $\mathbf{A}$.

Problem : Shift $\vec{\mu} - \vec{\delta}$ might be too large

Answer : Partial linearization of Storjohann (2007): $\mathbf{A} \to \mathcal{L}(\mathbf{A})$

Smooths shifts, keeps properties of $\mathbf{A}$ while enlarging a bit.

Partial Linearization

Consider $\mathbf{H}$ with diagonal degrees $(2, 37, 7, 18)$.

$$\mathbf{H} = \begin{bmatrix} (2) & [36] & [6] & [17] \\ & (37) & [6] & [17] \\ & & (7) & [17] \\ & & & (18) \end{bmatrix},$$

$[d]$: degree at most d and (d) : monic , degree exactly d.

$\delta = 1 + \lfloor (2 + 37 + 7 + 18)/4 \rfloor = 17.$ Construct by “expanding columns”:

$$\widetilde{\mathbf{H}} = \begin{bmatrix} (2) & [16] & [16] & [2] & [6] & [16] & 0 \\ & [16] & [16] & (3) & [6] & [16] & [0] \\ & & & & (7) & [16] & [0] \\ & & & & & [16] & (1) \end{bmatrix}.$$

$\mathbf{H}$ and $\widetilde{\mathbf{H}}$ are related by $\mathbf{H} = \widetilde{\mathbf{H}} \cdot \mathcal{E}_{\vec{\delta}}$ where

$$\mathcal{E}_{\vec{\delta}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & x^{17} & 0 & 0 \\ 0 & x^{34} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & x^{17} \end{bmatrix}$$

Insert elementary rows in $\widetilde{\mathbf{H}}$ by

$$\mathcal{L}_{\vec{\delta}}(\mathbf{H}) = \begin{bmatrix} (2) & [16] & [16] & [2] & [6] & [16] & [0] \\ & x^{17} & -1 & & & & \\ & & x^{17} & -1 & & & \\ & [16] & [16] & (3) & [6] & [16] & [0] \\ & & & & (7) & [16] & [0] \\ & & & & & x^{17} & -1 \\ & & & & & [16] & (1) \end{bmatrix}$$

Column degrees $\vec{d} = (2, 17, 17, 3, 7, 17, 1)$ - maximum 17.

Main property kept : shifted row reduction.

$$\begin{array}{ccccc} \mathbf{A}\mathbf{x}^{\vec{\mu}-\vec{\delta}} & \xrightarrow{\text{reduce}} & \mathbf{R}\mathbf{x}^{\vec{\mu}-\vec{\delta}} & \xrightarrow{\text{normalize}} & \mathbf{H} = \mathrm{lc}_{-\vec{\delta}}(\mathbf{R})^{-1}\mathbf{R} \\ \Big| & & & & \Big| \\ \text{partial linearization} & & & & \text{partial linearization} \\ \downarrow & & & & \downarrow \\ \mathcal{L}_{\vec{\delta}}(\mathbf{A})\mathbf{x}^{\vec{m}-\vec{d}} & \xrightarrow{\text{reduce}} & \hat{\mathbf{R}}\mathbf{x}^{\vec{m}-\vec{d}} & \xrightarrow{\text{normalize}} & \mathcal{L}_{\vec{\delta}}(\mathbf{H}) = \mathrm{lc}_{-\vec{d}}(\hat{\mathbf{R}})^{-1}\hat{\mathbf{R}} \end{array}.$$

Theorem

Let $\mathbf{A} \in \mathbb{K}[x]^{n\times n}$ nonsingular with $\vec{\delta}$ the degrees of the diagonal entries of the Hermite form.

Then the Hermite form is computed using $O\tilde{~}(n^{\omega}d)$ field operations.

Improving the Complexity

Repeat : partial linearization (this time with rows) :

(i) Enlarge : $\mathbf{A} \to \mathcal{L}^c(\mathbf{A})$

- size of $\mathcal{L}^c(\mathbf{A})$ at most twice size of $\mathbf{A}$
- degree $\mathcal{L}^c(\mathbf{A})$ at most average of $\mathbf{A}$

(ii) Compute Hermite form of $\mathcal{L}^c(\mathbf{A})$

(iii) $\mathbf{H}$ is found in upper left corner of Hermite form of $\mathcal{L}^c(\mathbf{A})$

Theorem

$\mathbf{A} \in \mathbb{K}[x]^{n\times n}$ *nonsingular. Hermite form computed:* $O^{\sim}(n^{\omega}\lceil s\rceil)$.

Results specific to Ore domain

- M. Giesbrecht and M. Sub Kim, (2013) Domain $\mathbf{A} \in \mathcal{F}(t)[D_t]^{n\times n}$
  - Hermite: Polynomial $\mathcal{F}$ operations in n, $\deg_D \mathbf{A}$, and $\deg_t \mathbf{A}$ (also polynomial in the coefficient bit-length when $\mathcal{F} = \mathcal{Q}$).

- M. Barkatou, C. El Bacha, E. Pflügell, G.L. (2013)
  - Two-sided block Popov form for $\mathbf{A} \in \mathcal{F}[[t]][D_t]^{n\times n}$

- B. Beckermann, H. Cheng and G.L, (2006)
  - Fraction-free row reduction Ore matrices

    Order bases for Ore matrices

- M. Khochtali and A. Storjohann, (ISSAC 2017)
  - Fraction-free Popov for Ore matrices

Thanks

- To the organizers for the invitation
- To the audience for listening

Complexity

Complexity

Proof.

If cost : $g(n)$ then recurrence relation: (with $s = \frac{\xi}{n}$)

$$g(n) \in O\tilde{}(n^{\omega}\lceil s \rceil) + g(\lceil n/2 \rceil) + g(\lfloor n/2 \rfloor)$$

Complexity

Proof.

If cost : $g(n)$ then recurrence relation: (with $s = \frac{\xi}{n}$)

$$\begin{aligned} g(n) &\in O\tilde{\ }(n^{\omega}\lceil s\rceil) + g(\lceil n/2\rceil) + g(\lfloor n/2\rfloor) \\ &\in O\tilde{\ }(n^{\omega-1}\xi + n^{\omega}) + g(\lceil n/2\rceil) + g(\lfloor n/2\rfloor) \end{aligned}$$

Complexity

Proof.

If cost : $g(n)$ then recurrence relation: (with $s = \frac{\xi}{n}$)

$$\begin{aligned} g(n) &\in O\tilde{}(n^{\omega}\lceil s\rceil) + g(\lceil n/2\rceil) + g(\lfloor n/2\rfloor) \\ &\in O\tilde{}(n^{\omega-1}\xi + n^{\omega}) + g(\lceil n/2\rceil) + g(\lfloor n/2\rfloor) \\ &\in O\tilde{}(n^{\omega-1}\xi + n^{\omega}) + 2g(\lceil n/2\rceil) \\ &\in O\tilde{}(n^{\omega-1}\xi + n^{\omega}) = O\tilde{}(n^{\omega}\lceil s\rceil). \end{aligned}$$

□