Applications of fast kernel computation for polynomial matrices

George Labahn

Symbolic Computation Group
Cheriton School of Computer Science
University of Waterloo, Canada

Joint work with Wei Zhou

June 2013

Outline

References

Report on papers

- W. Zhou, G. Labahn and A. Storjohann, Computing Minimal Nullspace Bases, *Proceedings of ISSAC 2012*, Grenoble, France, July 22-25, 2012.
- W. Zhou and G. Labahn, Computing Column Bases for polynomial matrices, *Proceedings of ISSAC 2013*, Boston, June 26-29, 2013.
- W. Zhou and G. Labahn, A fast, deterministic algorithm for computing a Hermite Normal Form of a polynomial matrix. Submitted 2013
- W. Zhou, G. Labahn and A. Storjohann, An efficient, deterministic algorithm for inversion of a matrix polynomial. Submitted 2013.

Minimal Kernel Bases

Minimal Kernel Bases

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

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

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

Minimal Kernel Bases

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

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

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

Can represent basis as matrix $\mathbf{M} \in \mathbb{K}[x]^{n \times n}$.

Deterministic algorithm (Z-L-S 2012) :

$$O^{\sim}(n^{\omega} s) \text{ with } s = \frac{\sum \operatorname{cdeg} \mathbf{F}}{n}$$

Shifts

Given $\mathbf{F}$ and integer vector $\vec{s} = (s_1, \ldots, s_n)$.

Sometimes better to work with $x^{\vec{s}}\mathbf{F}$ where

$$x^{\vec{s}} = \mathit{diag}\left(x^{s_1}, x^{s_2}, \ldots, x^{s_n}\right) \ .$$

Shifts

Given $\mathbf{F}$ and integer vector $\vec{s} = (s_1, \ldots, s_n)$.

Sometimes better to work with $x^{\vec{s}}\mathbf{F}$ where

$$x^{\vec{s}} = \mathit{diag}\left(x^{s_1}, x^{s_2}, \ldots, x^{s_n}\right) \ .$$

Then speak of

(i) $\vec{s}$-column degree

(ii) $\vec{s}$-leading coefficient

(iii) $\vec{s}$-column reduced

Shifts

Given $\mathbf{F}$ and integer vector $\vec{s} = (s_1, \ldots, s_n)$.

Sometimes better to work with $x^{\vec{s}}\mathbf{F}$ where

$$x^{\vec{s}} = \mathit{diag}\,(x^{s_1}, x^{s_2}, \ldots, x^{s_n}) \ .$$

Then speak of

(*i*) $\vec{s}$-column degree

(*ii*) $\vec{s}$-leading coefficient

(*iii*) $\vec{s}$-column reduced

(iii) Shifted $\vec{s}$-Kernel bases (basis $\vec{s}$-column reduced)

- Called $\vec{s}$-minimal kernel basis.

Some Important Properties (ZLS ISSAC 2012)

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

Theorem

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

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

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

Theorem

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

Theorem

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

Application 1 :
Polynomial Matrix Inversion

Reduce $\mathbf{F}$ to Diagonal Form

Partition and reduce $\mathbf{F}$ via

$$\mathbf{F} \cdot \mathbf{N} = \left[\begin{array}{c} \mathbf{F}_u \\ \hline \mathbf{F}_d \end{array}\right] \cdot [\mathbf{N}_\ell, \mathbf{N}_r] = \begin{bmatrix} \mathbf{F}_u\mathbf{N}_\ell & \mathbf{F}_u\mathbf{N}_r \\ \mathbf{F}_d\mathbf{N}_\ell & \mathbf{F}_d\mathbf{N}_r \end{bmatrix} = \begin{bmatrix} \mathbf{R}_u & 0 \\ 0 & \mathbf{R}_d \end{bmatrix}$$

Notice:

- $\mathbf{N}_\ell$ a kernel basis for $\mathbf{F}_d$
- $\mathbf{N}_r$ a kernel basis for $\mathbf{F}_u$

Recurse on $\mathbf{R}_u$ and $\mathbf{R}_d$ to get diagonal $\mathbf{B}$. Cost is $O^{\sim}(n^\omega s)$

Modeled on approach used by Jeannerod and Villard (2003).

Previous to Jeannerod/Villard fastest algorithms $O^{\sim}\left(n^{\omega+1}d\right)$

Measuring Size

$\mathbf{F}$ and $\vec{s}$ bound on column degree.

(i) Partition

$$\mathbf{F} \cdot \mathbf{N} = \left[\begin{array}{c} \mathbf{F}_u \\ \hline \mathbf{F}_d \end{array}\right] \cdot [\mathbf{N}_\ell, \mathbf{N}_r] = \begin{bmatrix} \mathbf{F}_u\mathbf{N}_\ell & \mathbf{F}_u\mathbf{N}_r \\ \mathbf{F}_d\mathbf{N}_\ell & \mathbf{F}_d\mathbf{N}_r \end{bmatrix} = \begin{bmatrix} \mathbf{R}_u & 0 \\ 0 & \mathbf{R}_d \end{bmatrix}$$

(ii) Size control: $\mathbf{M}$ a $\vec{s}$-minimal kernel basis

$$\sum \operatorname{cdeg}_{\vec{s}} \mathbf{M} \leq \sum \vec{s}$$

Implies : $\sum \operatorname{cdeg}_{\vec{s}} \mathbf{N}_\ell \leq \sum \vec{s}$ and $\sum \operatorname{cdeg}_{\vec{s}} \mathbf{N}_r \leq \sum \vec{s}$

Complexity

Theorem

Inversion of $\mathbf{F} \in \mathbb{K}[x]^{n \times n}$ *costs* $O^{\sim}(n^{\omega} s)$ *field operations.*

Complexity

Theorem

Inversion of $\mathbf{F} \in \mathbb{K}[x]^{n \times n}$ *costs* $O^{\sim}(n^{\omega} s)$ *field operations.*

Proof.

Cost : $g(n)$. Then recurrence relation:

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

□

Complexity

Theorem

Inversion of $\mathbf{F} \in \mathbb{K}[x]^{n \times n}$ *costs* $O^{\sim}(n^{\omega} s)$ *field operations.*

Proof.

Cost : $g(n)$. Then recurrence relation:

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

□

Similar algorithm for determinant. Deterministic, cost $O^{\sim}(n^{\omega} s)$

Also compute largest invariant factor : lcm($b_{11}(x), \ldots, b_{nn}(x)$).

Application 2 :
Hermite Normal Form

Finding Hermite Normal Form

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

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

(ii) $\mathbf{H}$ in (column) Hermite form

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

Finding Hermite Normal Form

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

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

(ii) $\mathbf{H}$ in (column) Hermite form

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

Results :

(i) Deterministic algorithm

(ii) Complexity : $O^{\sim}(n^{\omega} d_{\max})$ where $d_{\max}$ = degree $\mathbf{H}$

Step I : Finding Diagonal Elements

Partition and reduce $\mathbf{F}$ via

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

Step I : Finding Diagonal Elements

Partition and reduce $\mathbf{F}$ via

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

Here

(i) $\mathbf{G}_1$ is nonsingular and a column basis of $\mathbf{F}_u$.

(ii) $\mathbf{U}_r$ a right kernel basis of $\mathbf{F}_u$

(iii) $\mathbf{G}_2 = \mathbf{F}_d \cdot \mathbf{U}_r$,

Step I : Finding Diagonal Elements

Partition and reduce $\mathbf{F}$ via

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

Here

(i) $\mathbf{G}_1$ is nonsingular and a column basis of $\mathbf{F}_u$.

(ii) $\mathbf{U}_r$ a right kernel basis of $\mathbf{F}_u$

(iii) $\mathbf{G}_2 = \mathbf{F}_d \cdot \mathbf{U}_r$,

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

Theorem

$\mathbf{F} \in \mathbb{K}[x]^{n \times n}$. Diagonals of HNF costs $O^{\sim}(n^\omega s)$. Here $s = \frac{\sum \operatorname{cdeg} \mathbf{F}}{n}$.

Example

$$\mathbf{F} = \begin{bmatrix} x & -x^3 & -2x^4 & 2x & -x^2 \\ 1 & -1 & -2x & 2 & -x \\ -3 & 3x^2+x & 2x^2 & -x^4+1 & 3x \\ 0 & 1 & x^2+2x-2 & x^3+2x-2 & 0 \\ 1 & -x^2+2 & -2x^3-3x+3 & 2x+2 & 0 \end{bmatrix} \in \mathbb{Z}_7[x]^{5\times 5}.$$

$$\begin{bmatrix} \mathbf{F}_u \\ \mathbf{F}_d \end{bmatrix} \cdot [\mathbf{U}_\ell, \mathbf{U}_r] = \begin{bmatrix} x & -x^3 & -2x^4 & & \\ 1 & -1 & -2x & & \\ -3 & 3x^2+x & 2x^2 & & \\ * & * & * & x^3-1 & 0 \\ * & * & * & -x & x \end{bmatrix}$$

Example

$$\mathbf{F} = \begin{bmatrix} x & -x^3 & -2x^4 & 2x & -x^2 \\ 1 & -1 & -2x & 2 & -x \\ -3 & 3x^2+x & 2x^2 & -x^4+1 & 3x \\ 0 & 1 & x^2+2x-2 & x^3+2x-2 & 0 \\ 1 & -x^2+2 & -2x^3-3x+3 & 2x+2 & 0 \end{bmatrix} \in \mathbb{Z}_7[x]^{5\times 5}.$$

$$\begin{bmatrix} \mathbf{F}_u \\ \mathbf{F}_d \end{bmatrix} \cdot [\mathbf{U}_\ell^{(2)}, \mathbf{U}_r^{(2)}] = \begin{bmatrix} x & 0 & & & \\ 1 & x^2-1 & & & \\ * & * & x^3 & & \\ * & * & * & x^3-1 & 0 \\ * & * & * & -x & x \end{bmatrix}$$

Example

$$\mathbf{F} = \begin{bmatrix} x & -x^3 & -2x^4 & 2x & -x^2 \\ 1 & -1 & -2x & 2 & -x \\ -3 & 3x^2+x & 2x^2 & -x^4+1 & 3x \\ 0 & 1 & x^2+2x-2 & x^3+2x-2 & 0 \\ 1 & -x^2+2 & -2x^3-3x+3 & 2x+2 & 0 \end{bmatrix} \in \mathbb{Z}_7[x]^{5\times 5}.$$

$$\begin{bmatrix} \mathbf{F}_u \\ \mathbf{F}_d \end{bmatrix} \cdot [\mathbf{U}_\ell^{(2)}, \mathbf{U}_r^{(2)}] = \begin{bmatrix} x & & & & \\ * & x^2-1 & & & \\ * & * & x^3 & & \\ * & * & * & x^3-1 & \\ * & * & * & * & x \end{bmatrix}$$

Step II : Finding Rest of $\mathbf{H}$

Use method of Gupta and Storjohann (2012) to get rest of $\mathbf{H}$.

(i) Convert HNF to shifted $\vec{s}$-minimal kernel basis problem

$$\mathbf{FU} = \mathbf{H} \quad \text{same as} \quad [\mathbf{F} \quad -\mathbf{I}] \begin{bmatrix} \mathbf{U} \\ \mathbf{H} \end{bmatrix} = \mathbf{0}.$$

(ii) Adjust to alternate $\vec{s}'$-minimal kernel basis problem

$$[\mathbf{F} \quad -\mathbf{E}] \begin{bmatrix} \mathbf{U} \\ \mathbf{H}' \end{bmatrix} = \mathbf{0}.$$

Easily construct $\mathbf{E}$. Easily get $\mathbf{H}$ from $\mathbf{H}'$

(iii) Find $\mathbf{Q}$ and $\mathbf{R}$ such that $\mathbf{E} = \mathbf{FQ} + \mathbf{R}$. Solve via HOL.

Then repeat (ii) but with $\mathbf{E}$ replaced by $\mathbf{R}$.

Example

Given

$$\mathbf{F} = \begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 \\ -3x^3 + x - 1 & -x & 1 \end{bmatrix} \in \mathbb{Z}_7[x]^{3\times 3}.$$

Diagonal elements of HNF : $x - 1, x + 1, x^7 + 1$.

Example

Given

$$\mathbf{F} = \begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 \\ -3x^3 + x - 1 & -x & 1 \end{bmatrix} \in \mathbb{Z}_7[x]^{3\times 3}.$$

Diagonal elements of HNF : $x-1, x+1, x^7+1$. Then $[\mathbf{F}, -\mathbf{I}] \cdot \mathbf{N} = 0$ with $\mathbf{N}$ shift reduced is

$$\begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 & -1 & 0 & 0 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 & 0 & -1 & 0 \\ -3x^3 + x - 1 & -x & 1 & 0 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2x^2 + 1 & 2x^4 \\ 1 & 2x^2 + 2 & 2x^4 + x^2 \\ 1 & 2x^2 + 1 & 2x^4 + 1 \\ x - 1 & x - 1 & -2x + 2 \\ 1 & x + 2 & -2 \\ -3x^3 & x^5 - 3x^3 - x & x^7 - x^3 + 1 \end{bmatrix} = 0$$

Example

Given

$$\mathbf{F} = \begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 \\ -3x^3 + x - 1 & -x & 1 \end{bmatrix} \in \mathbb{Z}_7[x]^{3\times 3}.$$

Diagonal elements of HNF : $x-1, x+1, x^7+1$. Then $[\mathbf{F}, -\mathbf{I}] \cdot \mathbf{N} = 0$ with $\mathbf{N}$ shift reduced is

$$\left[\begin{array}{ccc|ccc} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 & -1 & 0 & 0 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 & 0 & -1 & 0 \\ -3x^3 + x - 1 & -x & 1 & 0 & 0 & -1 \end{array}\right] \cdot \left[\begin{array}{ccc} 1 & 2x^2 + 1 & 2x^4 \\ 1 & 2x^2 + 2 & 2x^4 + x^2 \\ 1 & 2x^2 + 1 & 2x^4 + 1 \\ \hline x - 1 & x - 1 & -2x + 2 \\ 1 & x + 2 & -2 \\ -3x^3 & x^5 - 3x^3 - x & x^7 - x^3 + 1 \end{array}\right] = 0$$

Get $\mathbf{F} \cdot \mathbf{V} = \mathbf{T}$.

$$\begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 \\ -3x^3 + x - 1 & -x & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2x^2 + 1 & 2x^4 \\ 1 & 2x^2 + 2 & 2x^4 + x^2 \\ 1 & 2x^2 + 1 & 2x^4 + 1 \end{bmatrix} = \begin{bmatrix} x - 1 & x - 1 & -2x + 2 \\ 1 & x + 2 & -2 \\ -3x^3 & x^5 - 3x^3 - x & x^7 - x^3 + 1 \end{bmatrix}$$

Example

Given

$$\mathbf{F} = \begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 \\ -3x^3 + x - 1 & -x & 1 \end{bmatrix} \in \mathbb{Z}_7[x]^{3\times 3}.$$

Diagonal elements of HNF : $x-1, x+1, x^7+1$. Then $[\mathbf{F}, -\mathbf{I}] \cdot \mathbf{N} = 0$ with $\mathbf{N}$ shift reduced is

$$\left[\begin{array}{ccc|ccc} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 & -1 & 0 & 0 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 & 0 & -1 & 0 \\ -3x^3 + x - 1 & -x & 1 & 0 & 0 & -1 \end{array}\right] \cdot \left[\begin{array}{ccc} 1 & 2x^2 + 1 & 2x^4 \\ 1 & 2x^2 + 2 & 2x^4 + x^2 \\ 1 & 2x^2 + 1 & 2x^4 + 1 \\ \hline x - 1 & x - 1 & -2x + 2 \\ 1 & x + 2 & -2 \\ -3x^3 & x^5 - 3x^3 - x & x^7 - x^3 + 1 \end{array}\right] = 0$$

Find column echelon of shifted leading coefficient matrix of $\mathbf{N}$. Then get $\mathbf{F} \cdot \mathbf{U} = \mathbf{H}$.

$$\begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 \\ -3x^3 + x - 1 & -x & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2x^2 + 1 & 2x^4 \\ 1 & 2x^2 + 2 & 2x^4 + x^2 \\ 1 & 2x^2 + 1 & 2x^4 + 1 \end{bmatrix} = \begin{bmatrix} x - 1 & x - 1 & -2x + 2 \\ 1 & x + 2 & -2 \\ -3x^3 & x^5 - 3x^3 - x & x^7 - x^3 + 1 \end{bmatrix}$$

Example

Given

$$\mathbf{F} = \begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 \\ -3x^3 + x - 1 & -x & 1 \end{bmatrix} \in \mathbb{Z}_7[x]^{3\times 3}.$$

Diagonal elements of HNF : $x-1, x+1, x^7+1$. Then $[\mathbf{F}, -\mathbf{I}] \cdot \mathbf{N} = 0$ with $\mathbf{N}$ shift reduced is

$$\left[\begin{array}{ccc|ccc} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 & -1 & 0 & 0 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 & 0 & -1 & 0 \\ -3x^3 + x - 1 & -x & 1 & 0 & 0 & -1 \end{array}\right] \cdot \left[\begin{array}{ccc} 1 & 2x^2 & 2x^4 + 2 \\ 1 & 2x^2 + 2 & 1x^4 + x^2 + 2 \\ 1 & 2x^2 & 2x^4 + 3 \\ \hline x - 1 & 0 & 0 \\ 1 & x + 2 & 0 \\ -3x^3 & x^5 - x & x^7 + 1 \end{array}\right] = 0$$

Find column echelon of shifted leading coefficient matrix of $\mathbf{N}$.

Example

Given

$$\mathbf{F} = \begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 \\ -3x^3 + x - 1 & -x & 1 \end{bmatrix} \in \mathbb{Z}_7[x]^{3\times 3}.$$

Diagonal elements of HNF : $x-1, x+1, x^7+1$. Then $[\mathbf{F}, -\mathbf{I}] \cdot \mathbf{N} = 0$ with $\mathbf{N}$ shift reduced is

$$\left[\begin{array}{ccc|ccc} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 & -1 & 0 & 0 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 & 0 & -1 & 0 \\ -3x^3 + x - 1 & -x & 1 & 0 & 0 & -1 \end{array}\right] \cdot \left[\begin{array}{ccc} 1 & 2x^2 & 2x^4 + 2 \\ 1 & 2x^2 + 2 & 1x^4 + x^2 + 2 \\ 1 & 2x^2 & 2x^4 + 3 \\ \hline x - 1 & 0 & 0 \\ 1 & x + 2 & 0 \\ -3x^3 & x^5 - x & x^7 + 1 \end{array}\right] = 0$$

Find column echelon of shifted leading coefficient matrix of $\mathbf{N}$. Then get $\mathbf{F} \cdot \mathbf{U} = \mathbf{H}$.

$$\begin{bmatrix} 2x^3 - 2x^2 + 3x - 3 & -2x^3 + 2x^2 & -2x + 2 \\ x^3 + 3x^2 - x + 2 & -2x^2 + x + 1 & -x^3 - x^2 - 2 \\ -3x^3 + x - 1 & -x & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2x^2 & 2x^4 + 2 \\ 1 & 2x^2 + 1 & 2x^4 + x^2 + 2 \\ 1 & 2x^2 & 2x^4 + 3 \end{bmatrix} = \begin{bmatrix} x - 1 & 0 & 0 \\ 1 & x + 2 & 0 \\ -3x^3 & x^5 - x & x^7 + 1 \end{bmatrix}$$

Future Work

- Shifted kernel basis algorithm depending on rank
- Popov from Column basis
- Alternate domains (noncommutative)

Application 3 :
Computing Column Bases

Column Bases

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

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

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

Column Bases

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

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

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

Note:

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

(ii) Can find unimodular matrix $\mathbf{U}$ with $\mathbf{F} \cdot \mathbf{U} = [\mathbf{0}, \mathbf{T}]$.

Column Bases

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

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

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

Note:

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

(ii) Can find unimodular matrix $\mathbf{U}$ with $\mathbf{F} \cdot \mathbf{U} = [\mathbf{0}, \mathbf{T}]$.

We give deterministic algorithm with cost $O^{\sim}\left(m^{\omega-1} n s\right)$

Column Bases Decomposition

$$\mathbf{F} \cdot \mathbf{U} = \mathbf{F} \cdot [\mathbf{U_L} \ \ \mathbf{U_R}] = [\mathbf{0} \ \ \mathbf{T}]$$

$$\Longrightarrow \mathbf{F} \cdot \mathbf{U_L} = \mathbf{0} \quad \text{and} \quad \mathbf{F} = [\mathbf{0} \ \ \mathbf{T}] \cdot \begin{bmatrix} \mathbf{V_u} \\ \mathbf{V_d} \end{bmatrix} = \mathbf{T} \cdot \mathbf{V_d}$$

Column Bases Decomposition

$$\mathbf{F} \cdot \mathbf{U} = \mathbf{F} \cdot [\mathbf{U_L} \;\; \mathbf{U_R}] = [\mathbf{0} \;\; \mathbf{T}]$$

$$\Longrightarrow \mathbf{F} \cdot \mathbf{U_L} = \mathbf{0} \quad \text{and} \quad \mathbf{F} = [\mathbf{0} \;\; \mathbf{T}] \cdot \begin{bmatrix} \mathbf{V_u} \\ \mathbf{V_d} \end{bmatrix} = \mathbf{T} \cdot \mathbf{V_d}$$

$$\begin{bmatrix} \mathbf{V_u} \\ \mathbf{V_d} \end{bmatrix} [\mathbf{U_L} \;\; \mathbf{U_R}] = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

$$\mathbf{V_d} \cdot \mathbf{U_L} = \mathbf{0}$$

Column Bases Decomposition

$$\mathbf{F} \cdot \mathbf{U} = \mathbf{F} \cdot [\mathbf{U_L} \;\; \mathbf{U_R}] = [\mathbf{0} \;\; \mathbf{T}]$$

$$\Longrightarrow \mathbf{F} \cdot \mathbf{U_L} = \mathbf{0} \quad \text{and} \quad \mathbf{F} = [\mathbf{0} \;\; \mathbf{T}] \cdot \begin{bmatrix} \mathbf{V_u} \\ \mathbf{V_d} \end{bmatrix} = \mathbf{T} \cdot \mathbf{V_d}$$

$$\begin{bmatrix} \mathbf{V_u} \\ \mathbf{V_d} \end{bmatrix} [\mathbf{U_L} \;\; \mathbf{U_R}] = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

$$\mathbf{V_d} \cdot \mathbf{U_L} = \mathbf{0}$$

Theorem

Given $\mathbf{N}$ *(right) kernel of* $\mathbf{F}$ *and* $\mathbf{G}$ *(left) kernel of* $\mathbf{N}$*. Then*

$$\exists \;\; \textit{column basis} \;\; \mathbf{T} \;\; \textit{such that} \;\; \mathbf{F} = \mathbf{T} \cdot \mathbf{G}.$$

Column Bases Decomposition

Why?

$$\mathbf{F} \cdot \mathbf{U} = \mathbf{F} \cdot [\mathbf{N} \ \ \mathbf{U_R}] = [\mathbf{0} \ \ \mathbf{T}]$$

$$\Longrightarrow \mathbf{F} \cdot \mathbf{N} = \mathbf{0} \quad \text{and} \quad \mathbf{F} = [\mathbf{0} \ \ \mathbf{T}] \cdot \begin{bmatrix} \mathbf{V_u} \\ \mathbf{V_d} \end{bmatrix} = \mathbf{T} \cdot \mathbf{V_d}$$

$$\begin{bmatrix} \mathbf{V_u} \\ \mathbf{V_d} \end{bmatrix} [\mathbf{N} \ \ \mathbf{U_R}] = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

$$\mathbf{V_d} \cdot \mathbf{N} = \mathbf{0}$$

Theorem

Given $\mathbf{N}$ *(right) kernel of* $\mathbf{F}$ *and* $\mathbf{G}$ *(left) kernel of* $\mathbf{N}$*. Then*

$$\exists \ \textit{column basis} \ \ \mathbf{T} \qquad \textit{such that} \qquad \mathbf{F} = \mathbf{T} \cdot \mathbf{G}.$$

Column Bases Decomposition

Why?

$$\mathbf{F} \cdot \mathbf{U} = \mathbf{F} \cdot [\mathbf{N} \ \ \mathbf{U_R}] = [\mathbf{0} \ \ \mathbf{T}]$$

$$\Longrightarrow \mathbf{F} \cdot \mathbf{N} = \mathbf{0} \quad \text{and} \quad \mathbf{F} = [\mathbf{0} \ \ \mathbf{T}] \cdot \begin{bmatrix} \mathbf{V_u} \\ \mathbf{V_d} \end{bmatrix} = \mathbf{T} \cdot \mathbf{V_d}$$

$$\begin{bmatrix} \mathbf{V_u} \\ \mathbf{V_d} \end{bmatrix} [\mathbf{N} \ \ \mathbf{U_R}] = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

$$\mathbf{V_d} \cdot \mathbf{N} = \mathbf{0} \quad \text{and} \quad \mathbf{V_d} = \mathbf{W} \cdot \mathbf{G}$$

Theorem

Given $\mathbf{N}$ *(right) kernel of* $\mathbf{F}$ *and* $\mathbf{G}$ *(left) kernel of* $\mathbf{N}$*. Then*

$$\exists \ \textit{column basis} \ \ \mathbf{T} \quad \textit{such that} \quad \mathbf{F} = \mathbf{T} \cdot \mathbf{G}.$$

Algorithm Steps

I Compute (right) $\vec{s}$-minimal kernel basis $\mathbf{N}$ for $\mathbf{F}$

(a) Use $\vec{s}$ = bound on column degrees of $\mathbf{F}$.

(b) Use minimal kernel bases to ensure sizes are controlled

II Compute (left) - $\vec{s}$-minimal kernel basis $\mathbf{G}$ for $\mathbf{N}$

(a) Issues with using negative shift.

(b) Cannot just solve $\mathbf{N}^T \cdot \mathbf{G}^T = \mathbf{0}$.

III Compute a column basis $\mathbf{T}$ such that $\mathbf{F} = \mathbf{T} \cdot \mathbf{N}$.

(a) Method: Compute kernel basis of $[\mathbf{F}^T \ \ \mathbf{G}^T] \cdot \begin{bmatrix} I \\ \mathbf{T}^T \end{bmatrix} = \mathbf{0}$.

(b) same issues as with Step II in this part.