Fast computation of normal forms of polynomial matrices

Vincent Neiger

Inria – AriC, École Normale Supérieure de Lyon, France

University of Waterloo, Ontario, Canada

Partially supported by the mobility grants *Explo'ra doc* from *Région Rhône-Alpes* / *Globalink Research Award - Inria* from *Mitacs & Inria* / *Programme Avenir Lyon Saint-Étienne*

SpecFun seminar
November 7, 2016

Polynomial matrix computations

Matrices over $\mathbb{K}[X]$
matrix $m \times m$

$$\begin{bmatrix} 3X+4 & X^3+4X+1 & 4X^2+3 \\ 5 & 5X^2+3X+1 & 5X+3 \\ 3X^3+X^2+5X+3 & 6X+5 & 2X+1 \end{bmatrix}$$

Fundamental operations

- multiplication
- kernel basis
- approximant basis

Transformation to normal forms

- triangularization $\rightsquigarrow$ Hermite
- row reduction $\rightsquigarrow$ Popov
- diagonalization $\rightsquigarrow$ Smith

Polynomial matrix computations

Matrices over $\mathbb{K}[X]$
matrix $m \times m$
degree $d \rightsquigarrow \widetilde{\mathcal{O}}(m^\omega d)$

$$\begin{bmatrix} 3X+4 & X^3+4X+1 & 4X^2+3 \\ 5 & 5X^2+3X+1 & 5X+3 \\ 3X^3+X^2+5X+3 & 6X+5 & 2X+1 \end{bmatrix}$$

Fundamental operations

- multiplication
- kernel basis
- approximant basis

Transformation to normal forms

- triangularization $\rightsquigarrow$ Hermite
- row reduction $\rightsquigarrow$ Popov
- diagonalization $\rightsquigarrow$ Smith

Polynomial matrix computations

Matrices over $\mathbb{K}[X]$
matrix $m \times m$
degree $d \quad \rightsquigarrow \quad \widetilde{\mathcal{O}}(m^\omega d)$
type of average degree D/m

$$\begin{bmatrix} 3X+4 & X^3+4X+1 & 4X^2+3 \\ 5 & 5X^2+3X+1 & 5X+3 \\ 3X^3+X^2+5X+3 & 6X+5 & 2X+1 \end{bmatrix}$$

Fundamental operations

- multiplication — $\widetilde{\mathcal{O}}(m^\omega D/m)$ in specific cases
- kernel basis — $\widetilde{\mathcal{O}}(m^\omega D/m)$
- approximant basis — $\widetilde{\mathcal{O}}(m^\omega D/m)$

Transformation to normal forms

- triangularization $\rightsquigarrow$ Hermite — **?**
- row reduction $\rightsquigarrow$ Popov — **?**
- diagonalization $\rightsquigarrow$ Smith — $\widetilde{\mathcal{O}}(m^\omega D/m)$

Hermite and Popov forms

working over $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$

$$\mathbf{A} = \begin{bmatrix} 3X+4 & X^3+4X+1 & 4X^2+3 \\ 5 & 5X^2+3X+1 & 5X+3 \\ 3X^3+X^2+5X+3 & 6X+5 & 2X+1 \end{bmatrix}$$

$\rightsquigarrow$ using elementary row operations, transform $\mathbf{A}$ into

Hermite form

$$\mathbf{H} = \begin{bmatrix} X^6+6X^4+X^3+X+4 & 0 & 0 \\ 5X^5+5X^4+6X^3+2X^2+6X+3 & X & 0 \\ 3X^4+5X^3+4X^2+6X+1 & 5 & 1 \end{bmatrix}$$

Popov form

$$\mathbf{P} = \begin{bmatrix} X^3+5X^2+4X+1 & 2X+4 & 3X+5 \\ 1 & X^2+2X+3 & X+2 \\ 3X+2 & 4X & X^2 \end{bmatrix}$$

Example: constrained bivariate interpolation

As in Guruswami-Sudan list-decoding of Reed-Solomon codes

M of degree D; L of degree $< D$

$$\mathbf{A} = \begin{bmatrix} M & & & & \\ -L & 1 & & & \\ -L^2 & & 1 & & \\ \vdots & & & \ddots & \\ -L^{m-1} & & & & 1 \end{bmatrix}$$

Problem: find $\mathbf{p} = \begin{bmatrix} p_1 & \cdots & p_m \end{bmatrix} \in \mathrm{RowSpace}(\mathbf{A})$ such that

$$(\star) \qquad \deg(p_j) < N_j \quad \text{for all } j$$

Approach:

- compute the Popov form **P** of **A** with degree weights on the columns
- return row of **P** which satisfies $(\star)$

Shifted Popov form

Connects Popov and Hermite forms

$$\mathbf{s} = (0,0,0,0) \quad \text{Popov} \qquad \begin{bmatrix} [4] & [3] & [3] & [3] \\ [3] & [4] & [3] & [3] \\ [3] & [3] & [4] & [3] \\ [3] & [3] & [3] & [4] \end{bmatrix} \qquad \begin{bmatrix} [7] & [0] & [1] & [5] \\ [0] & [1] & & [0] \\ & & [2] & \\ [6] & [0] & [1] & [6] \end{bmatrix}$$

$$\mathbf{s} = (0,2,4,6) \quad \mathbf{s}\text{-Popov} \qquad \begin{bmatrix} [7] & [4] & [2] & [0] \\ [6] & [5] & [2] & [0] \\ [6] & [4] & [3] & [0] \\ [6] & [4] & [2] & [1] \end{bmatrix} \qquad \begin{bmatrix} [8] & [5] & [1] & \\ [7] & [6] & [1] & \\ & & [2] & \\ [0] & [1] & & [0] \end{bmatrix}$$

$$\mathbf{s} = (0, D, 2D, 3D) \quad \text{Hermite} \qquad \begin{bmatrix} [16] & & & \\ [15] & [0] & & \\ [15] & & [0] & \\ [15] & & & [0] \end{bmatrix} \qquad \begin{bmatrix} [4] & & & \\ [3] & [7] & & \\ [1] & [5] & [3] & \\ [3] & [6] & [1] & [2] \end{bmatrix}$$

- normal form
- controlled average column degree
- and many useful properties

Shifted Popov form

For $\mathbf{A} \in \mathbb{K}[X]^{m\times m}$ nonsingular and $\mathbf{s} \in \mathbb{Z}^m$,
the $\mathbf{s}$-Popov form of $\mathbf{A}$ is the matrix $\mathbf{P} = \mathbf{UA}$ which is

$\mathbf{s}$-reduced

normalized

$$\begin{bmatrix} [7] & [4] & [2] & [0] \\ [6] & [5] & [2] & [0] \\ [6] & [4] & [3] & [0] \\ [6] & [4] & [2] & [1] \end{bmatrix} \begin{bmatrix} [8] & [5] & [1] & \\ [7] & [6] & [1] & \\ & & [2] & \\ [0] & [1] & & [0] \end{bmatrix}$$

sum of diagonal degrees:

$$d_1 + \cdots + d_m = \deg(\det(\mathbf{P})) = \deg(\det(\mathbf{A})) \leqslant D$$

Problem and previous work

Input: $\mathbf{A} \in \mathbb{K}[X]^{m\times m}$ nonsingular; shift $\mathbf{s} \in \mathbb{Z}^m$
Output: the $\mathbf{s}$-Popov form of $\mathbf{A}$

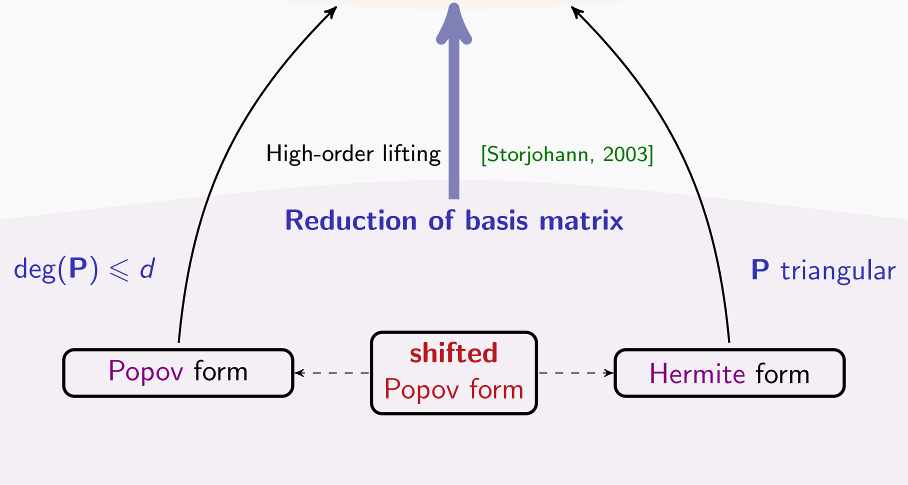
Previous fast algorithms focus on Hermite and Popov forms

Popov form: $\widetilde{\mathcal{O}}(m^\omega d)$, deterministic
[Giorgi-Jeannerod-Villard '03] [Sarkar-Storjohann '11] [Gupta-Sarkar-Storjohann-Valeriote '12]

Hermite form: $\widetilde{\mathcal{O}}(m^\omega d)$, Las Vegas randomized
[Gupta-Storjohann '11] [Gupta '11]

$$\begin{cases} p_1 f_{11} + \cdots + p_m f_{1m} & = & 0 & \bmod M_1 \\ \vdots & \vdots & & \vdots \\ p_1 f_{n1} + \cdots + p_m f_{nm} & = & 0 & \bmod M_n \end{cases}$$

Reconstruction from equations



Outline

1. reduction to average degree $d \in \mathcal{O}(D/m)$
2. Hermite form in $\widetilde{\mathcal{O}}(m^\omega D/m)$, deterministic
3. **s**-Popov form in $\widetilde{\mathcal{O}}(m^\omega D/m)$, probabilistic

1. Reduce to average degree

Example of partial linearization on the columns [Gupta et al., 2012]

$$\begin{bmatrix} (18) & & & \\ [17] & (7) & & \\ [17] & [6] & (37) & \\ [17] & [6] & [36] & (2) \end{bmatrix} \xrightarrow{\text{avg.}=16} \begin{bmatrix} (1) & [16] & & & & & \\ [0] & [16] & (7) & & & & \\ [0] & [16] & [6] & (3) & [16] & [16] & \\ [0] & [16] & [6] & [2] & [16] & [16] & (2) \end{bmatrix}$$

Elementary rows are inserted:

$$\begin{bmatrix} (1) & [16] & & & & & \\ & X^{17} & -1 & & & & \\ [0] & [16] & (7) & & & & \\ [0] & [16] & [6] & (3) & [16] & [16] & \\ & & & & X^{17} & -1 & \\ & & & & & X^{17} & -1 \\ [0] & [16] & [6] & [2] & [16] & [16] & (2) \end{bmatrix}$$

$\rightsquigarrow$ preserves determinant, Smith form, inverse...

1. Reduce to average degree

Problem: given $\mathbf{A}$ and $\mathbf{s}$, find $\mathbf{P}$

using no field operation, build

- $\mathcal{L}(\mathbf{A}) \in \mathbb{K}[X]^{\widetilde{m}\times\widetilde{m}}$
- $\mathcal{L}(\mathbf{s}) \in \mathbb{Z}^{\widetilde{m}}$

such that

- $\widetilde{m} \leqslant 3m$ and $\deg(\mathcal{L}(\mathbf{A})) \leqslant \lceil D/m \rceil$,
- $\mathbf{P}$ = submatrix of $\mathcal{L}(\mathbf{s})$-Popov form of $\mathcal{L}(\mathbf{A})$

uses partial linearization techniques from [Gupta et al., 2012]

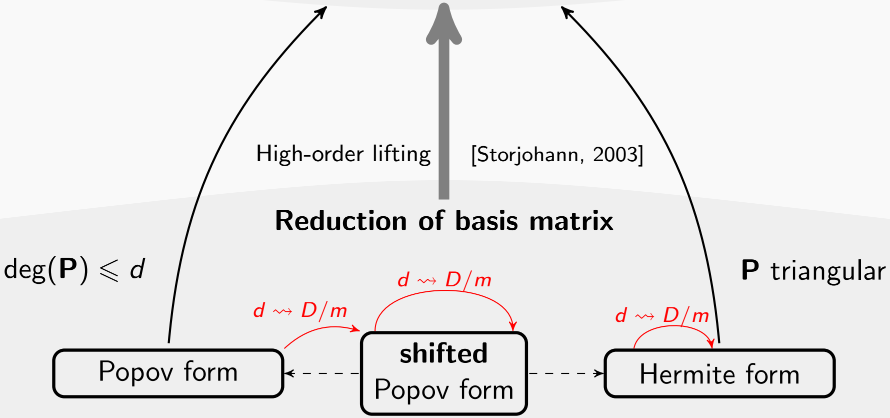
The bound D can be taken as the generic determinant degree:

$$\max_{\pi\in\mathrm{Perm}(\{1,\ldots,m\})} \sum_{1\leqslant i\leqslant m} \overline{\deg}(a_{i,\pi_i})$$

$\rightsquigarrow D/m \leqslant$ average row and column degrees

$$\begin{cases} p_1 f_{11} + \cdots + p_m f_{1m} & = & 0 \mod M_1 \\ \vdots & \vdots & \vdots \\ p_1 f_{n1} + \cdots + p_m f_{nm} & = & 0 \mod M_n \end{cases}$$

Reconstruction from equations



2. Fast deterministic Hermite form

Previous fastest: $\widetilde{\mathcal{O}}(m^\omega d)$, Las Vegas [Gupta-Storjohann, 2011]

Here: $\widetilde{\mathcal{O}}(m^\omega D/m)$, deterministic

(joint work with G. Labahn and W. Zhou [http://arxiv.org/abs/1607.04176])

Approach:

a. Find diagonal degrees [Zhou, 2012]

b. Reduce to Popov form computation

2.a. Find diagonal degrees

Partial computation of a triangularization:

$$\left[\begin{array}{c:c} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \hdashline \mathbf{A}_{21} & \mathbf{A}_{22} \end{array}\right] \longrightarrow \left[\begin{array}{c:c} \mathbf{B}_{1} & \\ \hdashline * & \mathbf{B}_{2} \end{array}\right] \longrightarrow \left[\begin{array}{c:c:c:c} \mathbf{B}_{11} & & & \\ \hdashline * & \mathbf{B}_{12} & & \\ \hdashline \multicolumn{2}{c:}{\multirow{2}{*}{$*$}} & \mathbf{B}_{21} & \\ \hdashline & & * & \mathbf{B}_{22} \end{array}\right] \longrightarrow \cdots$$

$\rightsquigarrow$ yields diagonal entries in $\widetilde{\mathcal{O}}(m^{\omega} d)$

- $\mathbf{B}_2$ = small degree row basis of $\begin{bmatrix}\mathbf{A}_{12} \\ \mathbf{A}_{22}\end{bmatrix}$ [Zhou-Labahn, 2013]
- $\mathbf{N}$ = minimal kernel basis of $\begin{bmatrix}\mathbf{A}_{12} \\ \mathbf{A}_{22}\end{bmatrix}$ [Zhou-Labahn-Sorjohann, 2012]
- $\mathbf{B}_1 = \mathbf{N}\begin{bmatrix}\mathbf{A}_{11} \\ \mathbf{A}_{21}\end{bmatrix}$

2.b. Reduce to Popov form computation

$\mathbf{H} = -\mathbf{d}$-Popov form of $\mathbf{A}$ $\qquad$ ($\mathbf{d}$ = diagonal degrees)

$$\mathbf{A} \xrightarrow{-\mathbf{d}\text{-reduction}} \mathbf{R} \xrightarrow[\text{(constant } \mathbf{U})]{\text{normalization}} \mathbf{H} = \mathbf{U}\,\mathbf{R}$$

$$\begin{bmatrix} [48] & [37] & [67] & [32] \\ [39] & [28] & [58] & [23] \\ [26] & [15] & [45] & [10] \\ [18] & [7] & [37] & [2] \end{bmatrix} \qquad \begin{bmatrix} [18] & [7] & [37] & [2] \\ [18] & [7] & [37] & [2] \\ [18] & [7] & [37] & [2] \\ [18] & [7] & [37] & [2] \end{bmatrix} \qquad \begin{bmatrix} (18) & & & \\ [17] & (7) & & \\ [17] & [6] & (37) & \\ [17] & [6] & [36] & (2) \end{bmatrix}$$

$-\mathbf{d}$-reduction: via $\mathbf{0}$-reduction $\rightsquigarrow$ worst case $\widetilde{\mathcal{O}}(m^{\omega+1} d)$

normalization: in $\widetilde{\mathcal{O}}(m^{\omega} d)$

2.b. Reduce to Popov form computation

Partial linearization: $(\mathbf{A}, \mathbf{d})$ transformed into $(\mathcal{L}(\mathbf{A}), \mathcal{L}(\mathbf{d}))$

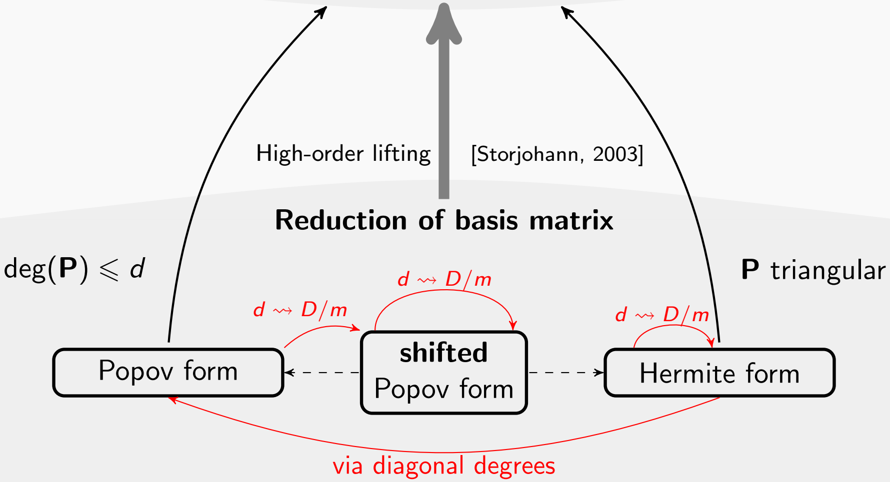
$$\left.\begin{array}{l} \mathcal{L}(\mathbf{A}) \text{ has degree } \leqslant d \\ \mathcal{L}(\mathbf{A}) \text{ has dimension } \leqslant 2m \\ \mathcal{L}(\mathbf{d}) \text{ has entries } \leqslant d \end{array}\right\} \Rightarrow -\mathcal{L}(\mathbf{d})\text{-reduction of } \mathcal{L}(\mathbf{A}) \text{ in } \widetilde{\mathcal{O}}(m^\omega d)$$

$$\begin{array}{ccccc}
\mathbf{A} & \xrightarrow{-\mathbf{d}\text{-reduction}} & \mathbf{R} & \xrightarrow[\text{(constant } \mathbf{U})]{\text{normalization}} & \mathbf{H} = \mathbf{U}\,\mathbf{R} \\
\Big| \text{ partial linearization } \downarrow & & & & \Big| \text{ partial linearization } \downarrow \\
\mathcal{L}(\mathbf{A}) & \xrightarrow{-\mathcal{L}(\mathbf{d})\text{-reduction}} & \hat{\mathbf{R}} & \xrightarrow[\text{(constant } \hat{\mathbf{U}})]{\text{normalization}} & \mathcal{L}(\mathbf{H}) = \hat{\mathbf{U}}\,\hat{\mathbf{R}}
\end{array}$$

$\mathbf{H}$ directly obtained from $\mathcal{L}(\mathbf{H})$

$$
\begin{cases}
p_1 f_{11} + \cdots + p_m f_{1m} & = & 0 \mod M_1 \\
\vdots & \vdots & \vdots \\
p_1 f_{n1} + \cdots + p_m f_{nm} & = & 0 \mod M_n
\end{cases}
$$

Reconstruction from equations



3. Fast $\mathbf{s}$-Popov form for arbitrary $\mathbf{s}$

Previous fastest: $\widetilde{\mathcal{O}}(m^\omega(d + \mathrm{amp}(\mathbf{s}))) \subseteq \widetilde{\mathcal{O}}(m^{\omega+2}d)$,
relying on non-shifted Popov form computation [Gupta et al., 2012]

Here: $\widetilde{\mathcal{O}}(m^\omega D/m)$, Las Vegas randomized

Approach:

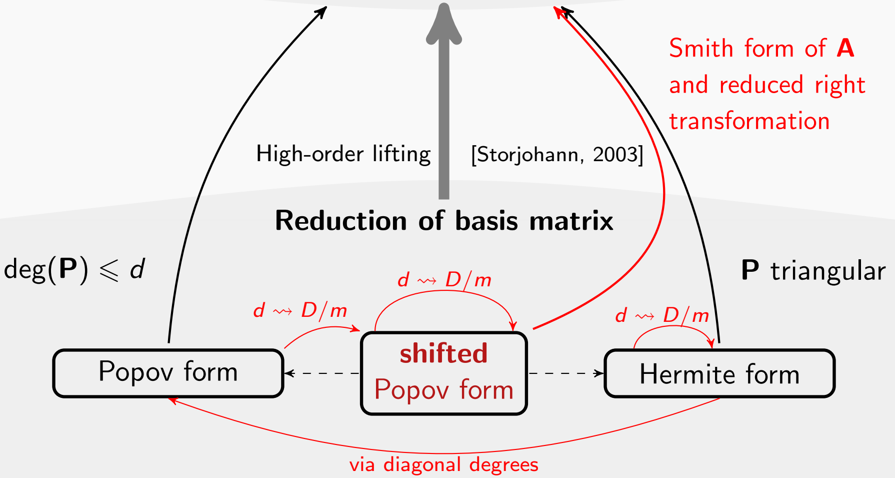
a. Build system of modular equations [Gupta-Storjohann, 2011]

b. Find $\mathbf{s}$-Popov basis of solutions [Neiger, 2016]

Note: yields fastest known algorithm for Popov form ($\mathbf{s} = \mathbf{0}$)

$$\begin{cases} p_1 f_{11} + \cdots + p_m f_{1m} & = & 0 & \bmod M_1 \\ \vdots & \vdots & & \vdots \\ p_1 f_{n1} + \cdots + p_m f_{nm} & = & 0 & \bmod M_n \end{cases}$$

Reconstruction from equations



3.a. Build system of linear modular equations

Compute:

Smith form $\quad \mathbf{UAV} = \mathrm{diag}(1, \ldots, 1, M_1, \ldots, M_n)$

reduced right transformation $\quad [\mathbf{0} \mid \mathbf{F}] = \mathbf{V} \bmod (1, \ldots, 1, M_1, \ldots, M_n)$

in probabilistic $\widetilde{\mathcal{O}}(m^\omega d)$ [Storjohann, 2003] [Gupta-Storjohann, 2011] [Gupta, 2011]

Then $\mathrm{RowSpace}(\mathbf{A})$ = all solutions $[p_1, \ldots, p_m]$ to

$$\begin{cases} p_1 f_{11} + \cdots + p_m f_{1m} = 0 \mod M_1 \\ \vdots \\ p_1 f_{n1} + \cdots + p_m f_{nm} = 0 \mod M_n \end{cases}$$

$\rightsquigarrow$ $\mathbf{s}$-Popov form of $\mathbf{A}$ = $\mathbf{s}$-Popov basis of solutions

3.b. Solve system of linear modular equations

Input:	nonzero moduli $M_1, \ldots, M_n$
	system matrix $\mathbf{F} \in \mathbb{K}[X]^{m \times n}$
	shift $\mathbf{s} \in \mathbb{Z}^m$
Output:	the $\mathbf{s}$-Popov basis of $\{\mathbf{p} \mid \mathbf{pF} = 0 \bmod (M_1, \ldots, M_n)\}$

Result: $\widetilde{\mathcal{O}}(m^\omega D/m)$ for arbitrary moduli, $n \in \mathcal{O}(m)$

where $D = \deg(M_1) + \cdots + \deg(M_n)$

Previous work: $\widetilde{\mathcal{O}}(m^\omega D/m)$ for

- Approximant bases: moduli = powers of X
- Interpolant bases: moduli given by roots and multiplicities
- Single degree-constrained solution (via structured system solving)

3.b. Solve system of linear modular equations

divide-and-conquer on the number of equations using ideas from

- [Jeannerod et al., 2016] (manage arbitrary shifts)
- [Gupta-Storjohann, 2011] (solution when diagonal degrees are known)

$\rightsquigarrow$ remains the base case: one equation

$$p_1 f_1 + \cdots + p_m f_m = 0 \bmod M$$

$\mathbf{P}$ the sought $\mathbf{s}$-Popov solution basis:

$$\mathbf{PF} = \begin{bmatrix} q_1 \\ \vdots \\ q_m \end{bmatrix} M \qquad \Leftrightarrow \qquad \begin{bmatrix} \mathbf{P} & \mathbf{q} \end{bmatrix} \begin{bmatrix} \mathbf{F} \\ M \end{bmatrix} = 0$$

3.b. Solve system of linear modular equations

Reduction to approximant basis:

$$\begin{bmatrix} \mathbf{P} & \mathbf{q} \\ * & * \end{bmatrix} \begin{bmatrix} \mathbf{F} \\ M \end{bmatrix} = 0 \mod X^{\mathrm{amp}(\mathbf{s})+2D}$$

where $\mathrm{amp}(\mathbf{s}) = \max(\mathbf{s}) - \min(\mathbf{s})$

New divide-and-conquer approach:

Recursion: $\mathbf{s} = (\mathbf{s}^{(1)}, \mathbf{s}^{(2)}), \quad \mathbf{F} = \begin{bmatrix} \mathbf{F}^{(1)} \\ \mathbf{F}^{(2)} \end{bmatrix}$ with $\mathrm{amp}(\mathbf{s}^{(i)}) \approx \mathrm{amp}(\mathbf{s})/2$

Base case: $\mathrm{amp}(\mathbf{s}) \in \mathcal{O}(D)$, cost $\widetilde{\mathcal{O}}(m^\omega D/m)$ [Jeannerod et al., 2016]

3.b. Solve system of linear modular equations

1. recursive call to find splitting index and $\mathbf{P}^{(1)}$:

$$\begin{bmatrix} \mathbf{P}^{(1)} & \mathbf{0} \\ * & * \end{bmatrix} = \mathbf{s}^{(1)}\text{-Popov sol. basis for } (\mathbf{F}^{(1)}, M) \quad \rightsquigarrow \quad \mathrm{UpdateSplit}(\mathbf{s}, \mathbf{F})$$

2. residual computation thanks to known $\mathbf{P}^{(1)}$:

$$\mathbf{A} = \begin{bmatrix} \mathbf{P}^{(1)} & \mathbf{0} & \mathbf{q}^{(1)} \\ * & \mathbf{P}^{(0)} & * \\ * & \mathbf{0} & q \end{bmatrix} = \mathbf{u}\text{-Popov app. basis for } \begin{bmatrix} \mathbf{F}^{(1)} \\ \mathbf{F}^{(2)} \\ M \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} \mathbf{0} \\ \mathbf{G} \\ N \end{bmatrix} = \mathbf{A} \begin{bmatrix} \mathbf{F}^{(1)} \\ \mathbf{F}^{(2)} \\ M \end{bmatrix}$$

3. recursive call to find $\mathbf{P}^{(2)}$

$$\mathbf{P}^{(2)} = \mathbf{v}\text{-Popov sol. basis for } (\mathbf{G}, N), \quad \text{where } \mathrm{amp}(\mathbf{v}) \approx \mathrm{amp}(\mathbf{s})/2$$

4. compute $\mathbf{P} = \begin{bmatrix} \mathbf{P}^{(1)} & \mathbf{0} \\ * & \mathbf{P}^{(2)}\mathbf{P}^{(0)} \end{bmatrix}$ using known diagonal degrees

Conclusion

Linear systems of modular equations

- $\widetilde{\mathcal{O}}(m^\omega D/m)$, deterministic ($n \in \mathcal{O}(m)$)
- return $\mathbf{s}$-Popov solution basis for arbitrary moduli

Shifted row reduction of polynomial matrices

- $\widetilde{\mathcal{O}}(m^\omega D/m)$, Las Vegas randomized
- computes $\mathbf{s}$-Popov form for an arbitrary shift
- Hermite form: deterministic

Questions:

- removing the assumption $n \in \mathcal{O}(m)$?
- deterministic $\widetilde{\mathcal{O}}(m^\omega D/m)$ Popov form?
- fast deterministic shifted Popov form?

Previous algorithms

Here, $\star$ = probabilistic algorithm, $d = \deg(\mathbf{A})$

Algorithm	Problem	Cost bound	
[Hafner-McCurley, 1991]	Hermite form	$\widetilde{\mathcal{O}}(m^4 d)$	
[Storjohann-Labahn, 1996]	Hermite form	$\widetilde{\mathcal{O}}(m^{\omega+1} d)$	
[Villard, 1996]	Popov & Hermite forms	$\widetilde{\mathcal{O}}(m^{\omega+1} d + (md)^{\omega})$	
[Alekhnovich, 2002]	weak Popov form	$\widetilde{\mathcal{O}}(m^{\omega+1} d)$	
[Mulders-Storjohann, 2003]	Popov & Hermite forms	$\mathcal{O}(m^3 d^2)$	
[Giorgi et al., 2003]	**0**-reduction	$\widetilde{\mathcal{O}}(m^{\omega} d)$	$\star$
[1] = [Sarkar-Storjohann, 2011]	Popov form of **0**-reduced	$\widetilde{\mathcal{O}}(m^{\omega} d)$	
[Gupta-Storjohann, 2011]	Hermite form	$\widetilde{\mathcal{O}}(m^{\omega} d)$	$\star$
[2] = [Gupta et al., 2012]	**0**-reduction	$\widetilde{\mathcal{O}}(m^{\omega} d)$	
[Zhou-Labahn, 2012/2016]	Hermite form	$\widetilde{\mathcal{O}}(m^{\omega} d)$	
[1] + [2]	**s**-Popov form for any **s**	$\widetilde{\mathcal{O}}(m^{\omega}(d + \mathrm{amp}(\mathbf{s})))$	

Reduction to linear modular equations: example

$$\mathbf{I}_m \begin{bmatrix} M & & & & \\ -L & 1 & & & \\ -L^2 & & 1 & & \\ \vdots & & & \ddots & \\ -L^{m-1} & & & & 1 \end{bmatrix} \begin{bmatrix} 1 & & & & \\ L & 1 & & & \\ L^2 & & 1 & & \\ \vdots & & & \ddots & \\ L^{m-1} & & & & 1 \end{bmatrix} = \begin{bmatrix} M & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

In other words, for $Q = \sum_{j<m} Q_j(X) Y^j$,

$$Q(x_i, y_i) = 0 \text{ for all } i \iff \begin{bmatrix} Q_0 & \cdots & Q_{m-1} \end{bmatrix} \begin{bmatrix} 1 \\ L \\ L^2 \\ \vdots \\ L^{m-1} \end{bmatrix} = 0 \bmod M$$

$$\iff Q(X, L) = 0 \bmod M$$

Degrees and target costs

measure	$D \leqslant \cdot$	I/O size	target cost
degree of matrix d	md	$\mathcal{O}(m^2 d)$	$\widetilde{\mathcal{O}}(m^\omega d)$
avg. row degree ρ/m	ρ	$\mathcal{O}(m^2 \rho/m)$	$\widetilde{\mathcal{O}}(m^\omega \rho/m)$
avg. column degree γ/m	γ	$\mathcal{O}(m^2 \gamma/m)$	$\widetilde{\mathcal{O}}(m^\omega \gamma/m)$
generic det. bound D	D	$\mathcal{O}(m^2 D/m)$	$\widetilde{\mathcal{O}}(m^\omega D/m)$

Example:

$$\mathbf{A} = \begin{bmatrix} M & & & & \\ -L & 1 & & & \\ -L^2 & & 1 & & \\ \vdots & & & \ddots & \\ -L^{m-1} & & & & 1 \end{bmatrix}$$

- $d = D$ — $\widetilde{\mathcal{O}}(m^\omega D)$
- $\rho/m \approx D$ — $\widetilde{\mathcal{O}}(m^\omega D)$
- $\gamma/m = D/m$ — $\widetilde{\mathcal{O}}(m^\omega D/m)$
- $D/m = D/m$ — $\widetilde{\mathcal{O}}(m^\omega D/m)$

Generic determinant bound:

$$D = \max_{\pi \in S_m} \sum_{1 \leqslant i \leqslant m} \overline{\deg}(a_{i,\pi_i}) \qquad \leqslant \min(\rho, \gamma) \leqslant md$$

Example: constrained bivariate interpolation (1/2)

As in Guruswami-Sudan list-decoding of Reed-Solomon codes: given

- points $(x_1, y_1), \ldots, (x_D, y_D)$ in $\mathbb{K}^2$ with the x_i's distinct
- and degree constraints m

find a nonzero $Q \in \mathbb{K}[X, Y]$ such that

(i) $Q(x_i, y_i) = 0$ for $1 \leqslant i \leqslant D$

(ii) $\deg_Y(Q) < m$ $\qquad (\rightsquigarrow Q = \sum_{0 \leqslant j < m} Q_j(X) Y^j)$

$(i) + (ii)$ defines a $\mathbb{K}[X]$-module $\mathcal{M}$ of rank m:
identifying $Q \longleftrightarrow [Q_0, \ldots, Q_{m-1}] \in \mathbb{K}[X]^{1 \times m}$,

$$M\mathbb{K}[X]^{1 \times m} \subseteq \mathcal{M} \subseteq \mathbb{K}[X]^{1 \times m}$$

for $M = (X - x_1) \cdots (X - x_m)$

Example: constrained bivariate interpolation (1/2)

As in Guruswami-Sudan list-decoding of Reed-Solomon codes: given

- points $(x_1, y_1), \ldots, (x_D, y_D)$ in $\mathbb{K}^2$ with the x_i's distinct
- and degree constraints m and $N_0, \ldots, N_{m-1}$,

find a nonzero $Q \in \mathbb{K}[X, Y]$ such that

(i) $Q(x_i, y_i) = 0$ for $1 \leqslant i \leqslant D$

(ii) $\deg_Y(Q) < m$ $\quad (\rightsquigarrow Q = \sum_{0 \leqslant j < m} Q_j(X) Y^j)$

(iii) $\deg(Q_j) < N_j$ for $0 \leqslant j < m$

$(i) + (ii)$ defines a $\mathbb{K}[X]$-module $\mathcal{M}$ of rank m:
identifying $Q \longleftrightarrow [Q_0, \ldots, Q_{m-1}] \in \mathbb{K}[X]^{1 \times m}$,

$$M\mathbb{K}[X]^{1 \times m} \subseteq \mathcal{M} \subseteq \mathbb{K}[X]^{1 \times m}$$

for $M = (X - x_1) \cdots (X - x_m)$

Example: constrained bivariate interpolation (2/2)

Recall that $M = (X - x_1) \cdots (X - x_D)$
Define $L \in \mathbb{K}[X]$ s.t. $L(x_i) = y_i$ and $\deg(L) < D$
$\rightsquigarrow$ basis of $\mathcal{M}$:

$$\mathcal{M} = \mathrm{Span}_{\mathbb{K}[X]} \begin{pmatrix} M \\ Y - L \\ Y^2 - L^2 \\ \vdots \\ Y^{m-1} - L^{m-1} \end{pmatrix} \quad \longleftrightarrow \quad \mathbf{A} = \begin{bmatrix} M & & & & \\ -L & 1 & & & \\ -L^2 & & 1 & & \\ \vdots & & & \ddots & \\ -L^{m-1} & & & & 1 \end{bmatrix}$$

Problem: find $Q \in \mathcal{M}$

Example: constrained bivariate interpolation (2/2)

Recall that $M = (X - x_1) \cdots (X - x_D)$
Define $L \in \mathbb{K}[X]$ s.t. $L(x_i) = y_i$ and $\deg(L) < D$
$\rightsquigarrow$ basis of $\mathcal{M}$:

$$\mathcal{M} = \mathrm{Span}_{\mathbb{K}[X]} \begin{pmatrix} M \\ Y - L \\ Y^2 - L^2 \\ \vdots \\ Y^{m-1} - L^{m-1} \end{pmatrix} \quad \longleftrightarrow \quad \mathbf{A} = \begin{bmatrix} M & & & & \\ -L & 1 & & & \\ -L^2 & & 1 & & \\ \vdots & & & \ddots & \\ -L^{m-1} & & & & 1 \end{bmatrix}$$

(iii): $\deg(Q_j) < N_j$ for $0 \leqslant j < m$

Problem: find $Q \in \mathcal{M}$ satisfying the degree constraints (iii)

Approach:

- compute the Popov form $\mathbf{P}$ of $\mathbf{A}$ with degree weights on the columns
- return row of $\mathbf{P}$ which satisfies (iii)

Hermite form example

Base field $\mathbb{Z}/7\mathbb{Z}$

$$\mathbf{A} = \begin{bmatrix} 3X+4 & X^3+4X+1 & 4X^2+3 \\ 5 & 5X^2+3X+1 & 5X+3 \\ 3X^3+X^2+5X+3 & 6X+5 & 2X+1 \end{bmatrix}$$

$$\mathbf{H} = \begin{bmatrix} X^6+6X^4+X^3+X+4 & 0 & 0 \\ 5X^5+5X^4+6X^3+2X^2+6X+3 & X & 0 \\ 3X^4+5X^3+4X^2+6X+1 & 5 & 1 \end{bmatrix}$$

$$\mathbf{U} = \begin{bmatrix} 6X^2+4X+1 & 3X^3+4X^2+3X+3 & 5X^3+3X^2+2X+2 \\ 2X+1 & X^2+5 & 4X^2+5X+3 \\ 4 & 2X+6 & X+6 \end{bmatrix}$$

$\det(\mathbf{U}) = 2$

Popov form example

Base field $\mathbb{Z}/7\mathbb{Z}$

$$\mathbf{A} = \begin{bmatrix} 3X+4 & X^3+4X+1 & 4X^2+3 \\ 5 & 5X^2+3X+1 & 5X+3 \\ 3X^3+X^2+5X+3 & 6X+5 & 2X+1 \end{bmatrix}$$

$$\mathbf{P} = \begin{bmatrix} X^3+5X^2+4X+1 & 2X+4 & 3X+5 \\ 1 & X^2+2X+3 & X+2 \\ 3X+2 & 4X & X^2 \end{bmatrix}$$

$$\mathbf{U} = \begin{bmatrix} 0 & 0 & 5 \\ 0 & 3 & 0 \\ 5 & 6X+2 & 0 \end{bmatrix}$$

$\det(\mathbf{U}) = 2$

Hermite and Popov forms

$\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ nonsingular
$\rightsquigarrow$ via elementary row operations,
transform $\mathbf{A}$ into

Hermite form [Hermite, 1851]	Popov form [Popov, 1972]
triangular	row reduced

Hermite and Popov forms

$\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ nonsingular
$\rightsquigarrow$ via elementary row operations,
transform $\mathbf{A}$ into

Hermite form [Hermite, 1851]	Popov form [Popov, 1972]
triangular column normalized	row reduced column normalized
$\begin{bmatrix} 4 & & & \\ 3 & 7 & & \\ 1 & 5 & 3 & \\ 3 & 6 & 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 7 & 0 & 1 & 5 \\ 0 & 1 & & 0 \\ & & 2 & \\ 6 & 0 & 1 & 6 \end{bmatrix}$

Hermite and Popov forms

$\mathbf{A} \in \mathbb{K}[X]^{m\times m}$ nonsingular
$\rightsquigarrow$ via elementary row operations,
transform $\mathbf{A}$ into

basis of $\mathcal{M} \subset \mathbb{K}[X]^{1\times m}$ of rank m
$\rightsquigarrow$ find the reduced Gröbner basis
of $\mathcal{M}$ for either term order

Hermite form [Hermite, 1851]	Popov form [Popov, 1972]
triangular, column normalized } POT	row reduced, column normalized } TOP
$\begin{bmatrix} 4 & & & \\ 3 & 7 & & \\ 1 & 5 & 3 & \\ 3 & 6 & 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 7 & 0 & 1 & 5 \\ 0 & 1 & & 0 \\ & & 2 & \\ 6 & 0 & 1 & 6 \end{bmatrix}$

Iterative Popov form algorithm

[Wolovich, 1974] and [Mulders-Storjohann, 2003]

Row reduction:

$$\mathbf{A} = \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 3 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 2 & 2 \end{bmatrix}$$

Column normalization:

Cost bound: $\mathcal{O}(m^3 d^2)$

Iterative Popov form algorithm

[Wolovich, 1974] and [Mulders-Storjohann, 2003]

Row reduction:

$$\mathbf{A} = \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 3 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 2 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix} = \mathbf{R}$$

Column normalization:

Cost bound: $\mathcal{O}(m^3 d^2)$

Iterative Popov form algorithm

[Wolovich, 1974] and [Mulders-Storjohann, 2003]

Row reduction:

$$\mathbf{A} = \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 3 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 2 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix} = \mathbf{R}$$

Column normalization:

Cost bound: $\mathcal{O}(m^3 d^2)$

Iterative Popov form algorithm

[Wolovich, 1974] and [Mulders-Storjohann, 2003]

Row reduction:

$$\mathbf{A} = \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 3 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 2 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix} = \mathbf{R}$$

Column normalization:

$$\mathbf{R} = \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 1 & 2 \end{bmatrix}$$

Cost bound: $\mathcal{O}(m^3 d^2)$

Iterative Popov form algorithm

[Wolovich, 1974] and [Mulders-Storjohann, 2003]

Row reduction:

$$\mathbf{A} = \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 3 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 2 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix} = \mathbf{R}$$

Column normalization:

$$\mathbf{R} = \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 1 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 2 & 5 & 1 & 1 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 1 & 2 \end{bmatrix} = \mathbf{P}$$

Cost bound: $\mathcal{O}(m^3 d^2)$

Iterative Popov form algorithm

[Wolovich, 1974] and [Mulders-Storjohann, 2003]

Row reduction:

$$\mathbf{A} = \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 3 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 3 & 2 & 2 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix} = \mathbf{R}$$

Column normalization:

$$\mathbf{R} = \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 1 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 2 & 0 & 0 \\ 2 & 5 & 1 & 1 \\ 2 & 0 & 2 & 1 \\ 2 & 2 & 1 & 2 \end{bmatrix} = \mathbf{P}$$

Cost bound: $\mathcal{O}(m^3 d^2)$

$\rightsquigarrow$ incorporate

- fast matrix multiplication $\mathcal{O}(m^\omega)$?
- fast polynomial arithmetic $\widetilde{\mathcal{O}}(d)$?

Fast Popov form algorithm

Step 1: fast row reduction

$\widetilde{\mathcal{O}}(m^\omega d)$

[Giorgi et al., 2003], probabilistic

[Gupta et al., 2012], deterministic

Step 2: fast Popov normalization

$\widetilde{\mathcal{O}}(m^\omega d)$

[Sarkar-Storjohann, 2011]

[Giorgi et al., 2003]:
expansion of $\mathbf{A}^{-1}$ is, ultimately, recurrent sequence of matrices

$$\mathbf{A}^{-1} = B_0 + B_1 X + \cdots + \underbrace{B_\nu X^\nu + \cdots + B_{\nu+2d} X^{\nu+2d}}_{\text{via high-order lifting}} + X^{\nu+2d+1}(\cdots)$$

Reconstruct $\mathbf{R}$ as $\mathbf{B} = \dfrac{*}{\mathbf{R}} \bmod X^{2d+1}$

$\rightsquigarrow$ uses $\deg(\mathbf{R}) \leqslant d$, which does not hold for arbitrary shifts
(even $\deg(\mathbf{P})$ may be md)

Obstacle: size of a shifted row reduced form

Shifted Popov form via

$$\mathbf{A} \xrightarrow{\text{Step 1: shifted row reduction}} \mathbf{R} \xrightarrow{\text{Step 2: column normalization}} \mathbf{P}$$

Obstacle: worst-case $\deg(\mathbf{R}) = \Theta(d + \mathrm{amp}(\mathbf{s}))$
with $\mathrm{amp}(\mathbf{s}) = \max(\mathbf{s}) - \min(\mathbf{s})$

Example: $\mathbf{A}$ unimodular, shift $\mathbf{s} = (0, \ldots, 0, md, \ldots, md)$
$\rightsquigarrow$ $\mathbf{s}$-row reduced form of $\mathbf{A}$

$$\mathbf{R} = \begin{bmatrix} 0 & & & & & \\ & 0 & & & & \\ & & 0 & & & \\ md & md & md & 0 & & \\ md & md & md & & 0 & \\ md & md & md & & & 0 \end{bmatrix}$$

size $\Theta(m^3 d)$ beyond target cost

Hermite form in $\widetilde{\mathcal{O}}(m^\omega d)$

[Gupta-Storjohann, 2011], [Gupta, 2011]:

Step 1: Smith form computation: $\mathbf{UAV} = \mathbf{S}$ (probabilistic)
$\rightsquigarrow$ modular equations describing $\mathrm{RowSpace}(\mathbf{A})$

Step 2: find pivot degrees $\mathbf{d} = (d_1, \ldots, d_m)$ by triangularization
from a matrix involving $\mathbf{V}$ and $\mathbf{S}$

Step 3: use $\mathbf{d}$ to find Hermite basis of solutions to the equations

[Zhou, 2012], [Zhou-Labahn, 2016]:

Step 1: find pivot degrees $\mathbf{d}$ by (partial) triangularization
(using kernel bases and column bases, deterministic)

Step 2: use $\mathbf{d}$ to find Hermite form of $\mathbf{A}$

$\mathbf{s}$-Popov form not triangular for arbitrary $\mathbf{s}$