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*

Caramba seminar
November 10, 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 $d \quad \rightsquigarrow \quad \tilde{\mathcal{O}}(m^\omega d)$

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

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

Shifted Popov form

Connects Popov and Hermite forms

$\mathbf{s} = (0,0,0,0)$
Popov

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

$\mathbf{s} = (0,2,4,6)$
s-Popov

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

$\mathbf{s} = (0, D, 2D, 3D)$
Hermite

$$\begin{bmatrix} [16] & & & \\ [15] & [0] & & \\ [15] & & [0] & \\ [15] & & & [0] \end{bmatrix} \qquad \begin{bmatrix} [4] & & & \\ [3] & [7] & & \\ [1] & [5] & [3] & \\ [3] & [6] & [1] & [2] \end{bmatrix}$$

- 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 **s**-Popov form of $\mathbf{A}$ is the matrix $\mathbf{P} = \mathbf{UA}$ which is

s-reduced

normalized

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

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]

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

Reconstruction from equations

High-order lifting [Storjohann, 2003]

Reduction of basis matrix

$\deg(\mathbf{P}) \leqslant d$

P triangular

Popov form

shifted Popov form

Hermite form

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]

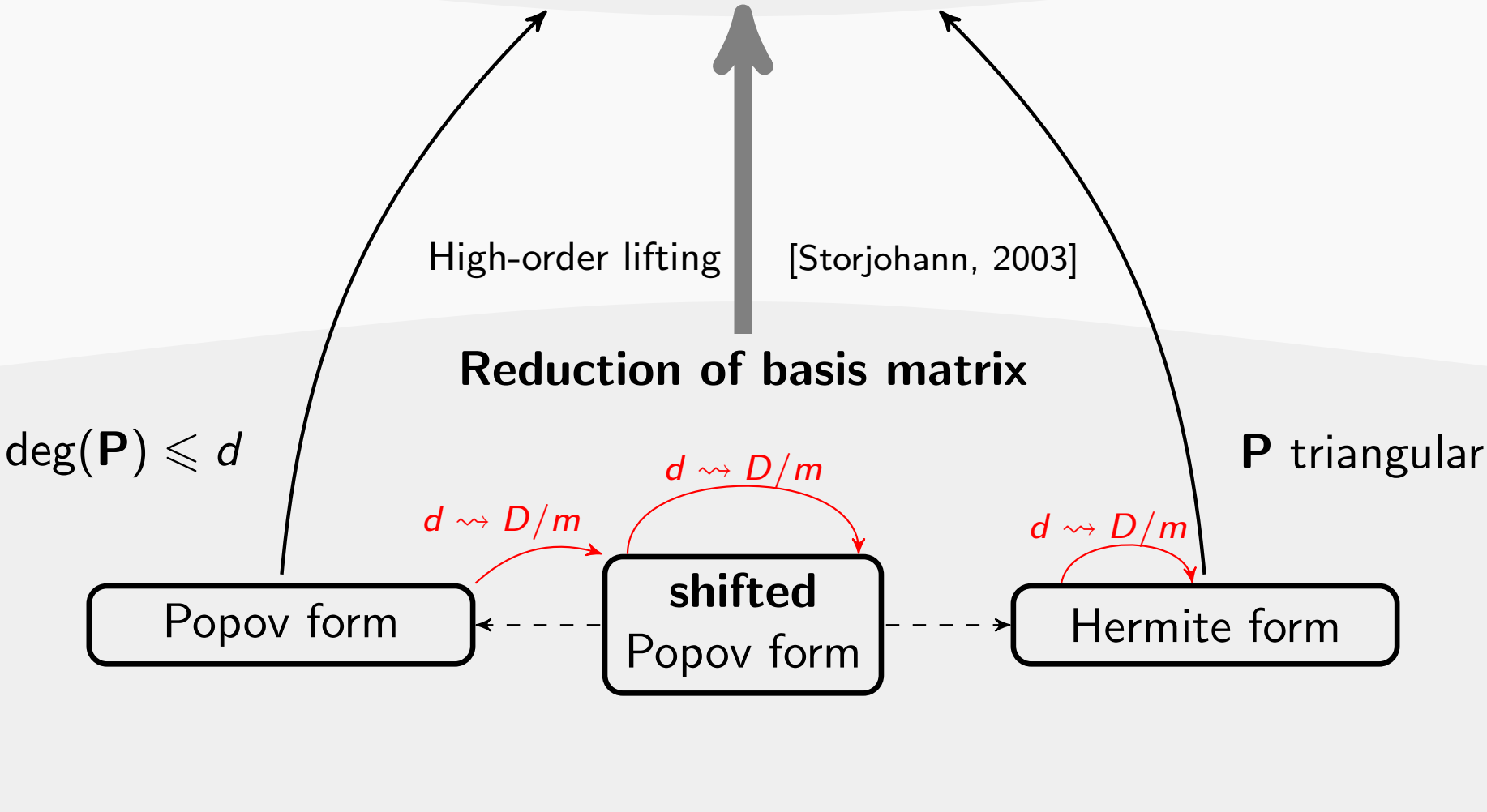
The bound D can be taken as the generic determinant degree:

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

$\rightsquigarrow D/m \leqslant$ 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])

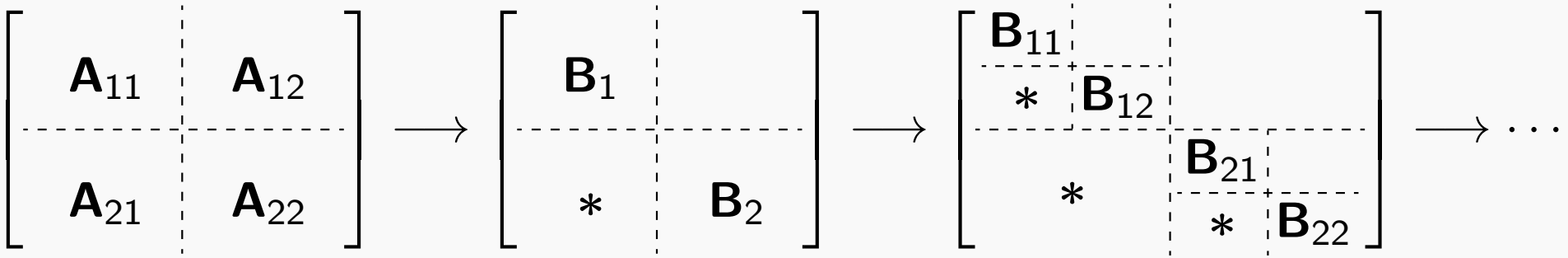
Approach:

a. Find diagonal degrees [Zhou, 2012]

b. Reduce to Popov form computation

2.a. Find diagonal degrees

Partial computation of a triangularization:



$\rightsquigarrow$ 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

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

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

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

$-\mathbf{d}$-reduction: via **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 $(\mathcal{L}(\mathbf{A}), \mathcal{L}(\mathbf{d}))$

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

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

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

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

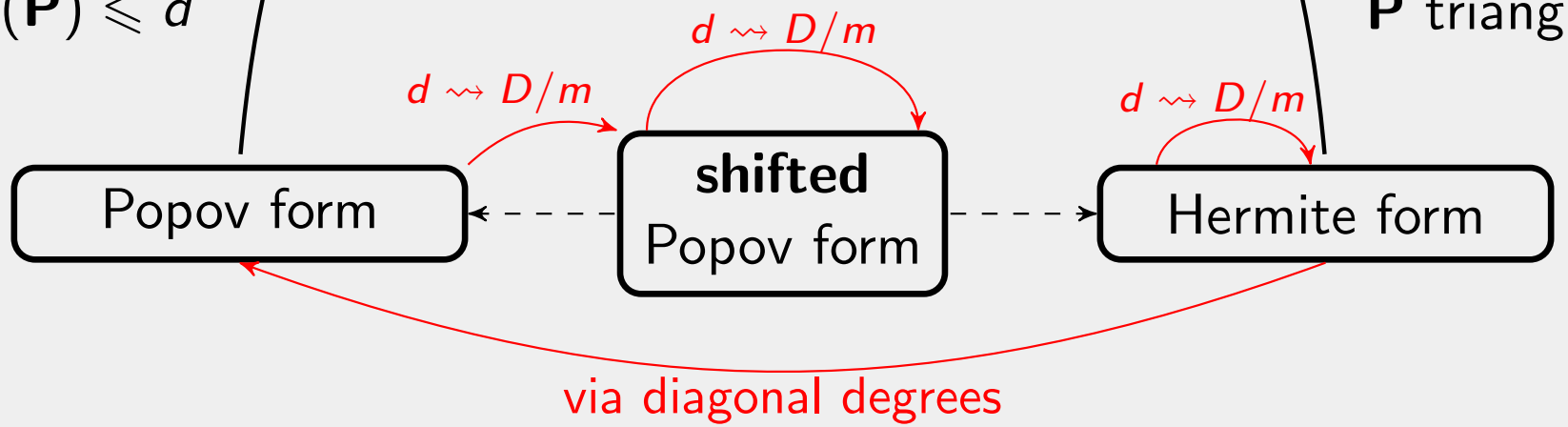
Reconstruction from equations

High-order lifting [Storjohann, 2003]

Reduction of basis matrix

$\deg(\mathbf{P}) \leqslant d$

P triangular



3. Fast **s**-Popov form for arbitrary **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

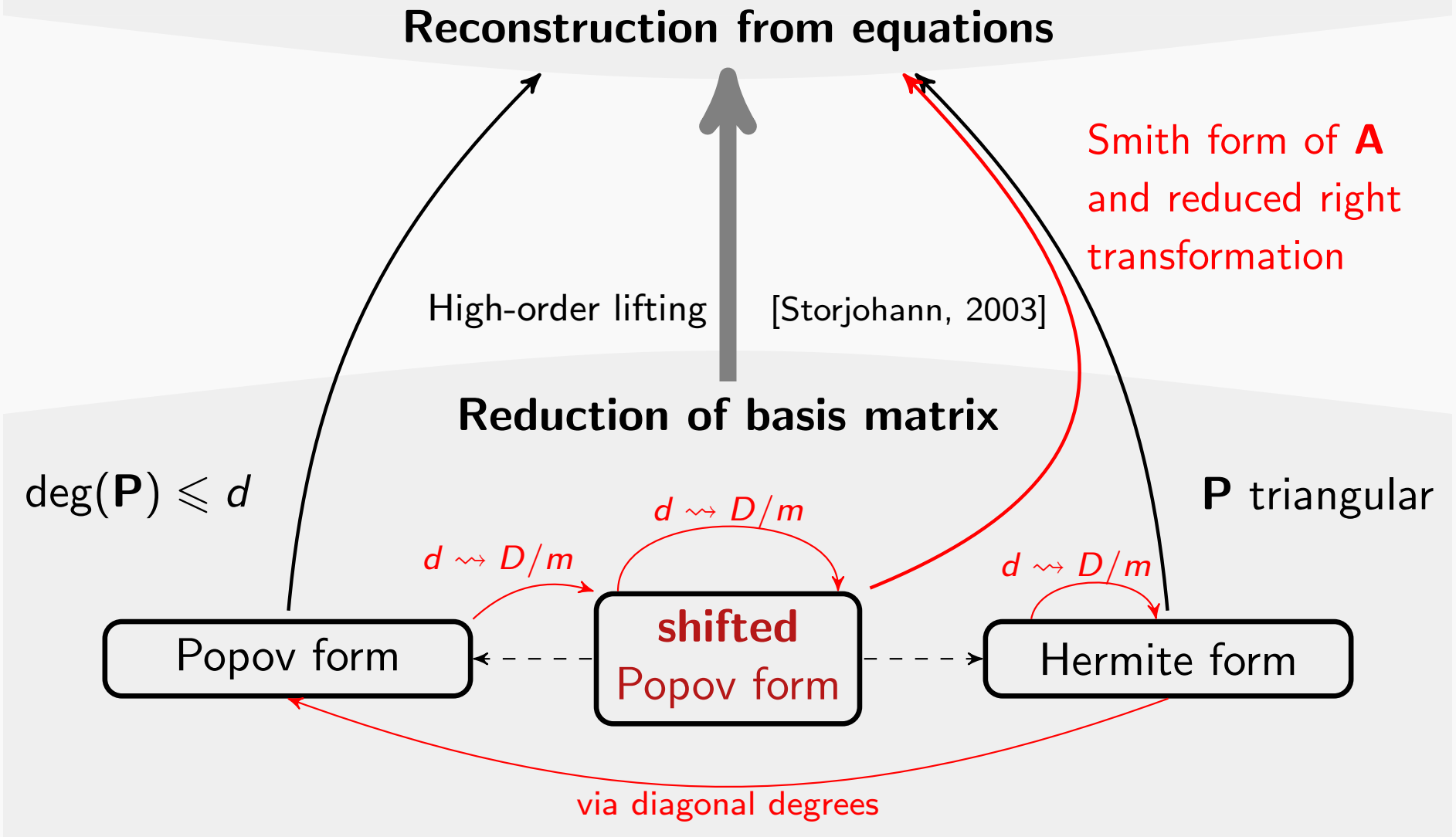
Approach:

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

b. Find **s**-Popov basis of solutions [Neiger, 2016]

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

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



3.a. Build system of linear modular equations

Compute:

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

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

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

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

$\rightsquigarrow$ **s**-Popov form of $\mathbf{A}$ = **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: $\mathbf{s} = (\mathbf{s}^{(1)}, \mathbf{s}^{(2)})$, $\mathbf{F} = \begin{bmatrix} \mathbf{F}^{(1)} \\ \mathbf{F}^{(2)} \end{bmatrix}$ 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 $\mathbf{P}^{(1)}$:

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

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

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

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

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

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 **s**-Popov solution basis for arbitrary moduli

Shifted row reduction of polynomial matrices

- $\widetilde{\mathcal{O}}(m^\omega D/m)$, Las Vegas randomized
- computes **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?