Fast computation of shifted Popov forms of polynomial matrices via systems of linear modular equations

Vincent Neiger

AriC, LIP, 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*

ISSAC 2016, Waterloo, July 21, 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
- inversion
- kernel basis, order 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 $d \quad \rightsquigarrow \quad \widetilde{\mathcal{O}}(m^\omega d)$

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

Fundamental operations

- multiplication
- inversion $\quad \widetilde{\mathcal{O}}(m^3 d)$
- kernel basis, order 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 σ/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 — $\widetilde{\mathcal{O}}(m^\omega \sigma/m)$ in specific cases
- inversion $\widetilde{\mathcal{O}}(m^3 d)$ — $\widetilde{\mathcal{O}}(m^3 \sigma/m)$
- kernel basis, order basis — $\widetilde{\mathcal{O}}(m^\omega \sigma/m)$

Transformation to normal forms

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

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

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

Shifted Popov form

Connects Popov and Hermite forms

$\mathbf{s} = (0,0,0,0)$ Popov	$\begin{bmatrix} 4 & 3 & 3 & 3 \\ 3 & 4 & 3 & 3 \\ 3 & 3 & 4 & 3 \\ 3 & 3 & 3 & 4 \end{bmatrix}$	$\begin{bmatrix} 7 & 0 & 1 & 5 \\ 0 & 1 & & 0 \\ & & 2 & \\ 6 & 0 & 1 & 6 \end{bmatrix}$
$\mathbf{s} = (0,2,4,6)$ s-Popov	$\begin{bmatrix} 7 & 4 & 2 & 0 \\ 6 & 5 & 2 & 0 \\ 6 & 4 & 3 & 0 \\ 6 & 4 & 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 8 & 5 & 1 & \\ 7 & 6 & 1 & \\ & & 2 & \\ 0 & 1 & & 0 \end{bmatrix}$
$\mathbf{s} = (0,\sigma,2\sigma,3\sigma)$ Hermite	$\begin{bmatrix} 16 & & & \\ 15 & 0 & & \\ 15 & & 0 & \\ 15 & & & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & & & \\ 3 & 7 & & \\ 1 & 5 & 3 & \\ 3 & 6 & 1 & 2 \end{bmatrix}$

- normal form
- average column degree σ/m
- and many useful properties

From reduction to reconstruction

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

Reconstruction from equations

High-order lifting [Storjohann, 2003]

Reduction of basis matrix

Popov form — **shifted** Popov form — Hermite form

Result

Problem

Input: $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ nonsingular
shift $\mathbf{s} \in \mathbb{Z}^m$

Output: the $\mathbf{s}$-Popov form $\mathbf{P}$ of $\mathbf{A}$

New fast algorithm: $\widetilde{\mathcal{O}}(m^\omega \sigma / m)$, Las Vegas randomized

Previous fastest: $\widetilde{\mathcal{O}}(m^\omega(d + \max(\mathbf{s})))$, deterministic
relying on fast non-shifted Popov form computation
worst-case $\widetilde{\mathcal{O}}(m^{\omega+2} d)$

Overview:

1. reduce to average degree
2. reduce to system of modular equations
3. solve system of modular equations

Step 1: reduce to average degree

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

with no field operation, build

- $\widetilde{\mathbf{A}} \in \mathbb{K}[X]^{\widetilde{m} \times \widetilde{m}}$
- $\mathbf{t} \in \mathbb{Z}^{\widetilde{m}}$

such that

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

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

$\rightsquigarrow$ fastest known algorithm for Popov form ($\mathbf{s} = \mathbf{0}$)
relies on shifted Popov computation

Step 2: reduce to system of modular equations

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

Reconstruction from equations

Smith form of **A** and reduced right transformation

High-order lifting [Storjohann, 2003]

Reduction of basis matrix

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

P triangular

Popov form — **shifted** Popov form — Hermite form

Step 2: reduce to system of modular equations

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

Reconstruction from equations

Smith form of **A** and reduced right transformation

High-order lifting [Storjohann, 2003]

Reduction of basis matrix

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

P triangular

Popov form — **shifted** Popov form — Hermite form

Step 2: reduce to system of 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]

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

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

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

Linear systems of 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: $\mathbf{P}$ the $\mathbf{s}$-Popov solution basis for $\mathbf{F}$ modulo $M_1, \ldots, M_n$

for $\sigma = \deg(M_1) + \cdots + \deg(M_n)$,

Order bases: $M_1 = \cdots = M_n = X^{\sigma/n}$ $\rightsquigarrow$ $\widetilde{\mathcal{O}}(m^\omega \sigma/m)$

[Giorgi et al., 2003] [Storjohann, 2006] [Zhou-Labahn, 2012] [Jeannerod et al., 2016]

Interpolation bases: $M_j =$ product of linear factors $\rightsquigarrow$ $\widetilde{\mathcal{O}}(m^\omega \sigma/m)$

[Beckermann-Labahn, 2000] [Jeannerod et al., 2015+2016]

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

Step 3: solve system of modular equations (1/3)

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:

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

Step 3: solve system of modular equations (2/3)

Reduction to order basis:

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

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

New divide-and-conquer on $\mathrm{amp}(\mathbf{s})$:

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: $\mathrm{amp}(\mathbf{s}) \in \mathcal{O}(\sigma)$, cost $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ [Jeannerod et al., 2016]

Step 3: solve system of modular equations (3/3)

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 $\mathbf{P}^{(1)}$:

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

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

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

Shifted row reduction of polynomial matrices

- $\widetilde{\mathcal{O}}(m^\omega \sigma/m)$, Las Vegas randomized
- computes **s**-Popov form for an arbitrary shift

Advertisement: deterministic $\widetilde{\mathcal{O}}(m^\omega \sigma/m)$ Hermite form and determinant
[Labahn - Neiger - Zhou `http://arxiv.org/abs/1607.04176`]

Question: what about deterministic $\widetilde{\mathcal{O}}(m^\omega \sigma/m)$ 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**	$\widetilde{\mathcal{O}}(m^{\omega}(d + \mathrm{amp}(\mathbf{s})))$	

Example: constrained bivariate interpolation

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

M of degree σ; L of degree $< \sigma$

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

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 $(\star)$

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

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

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

Degrees and target costs

measure	$\sigma \leqslant \cdot$	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 σ	σ	$\mathcal{O}(m^2 \sigma/m)$	$\widetilde{\mathcal{O}}(m^\omega \sigma/m)$

Example:

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

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

Generic determinant bound:

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

Example: constrained bivariate interpolation (1/2)

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

- points $(x_1, y_1), \ldots, (x_\sigma, y_\sigma)$ 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 $1 \leqslant i \leqslant \sigma$

(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 $(x_1, y_1), \ldots, (x_\sigma, y_\sigma)$ 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 $1 \leqslant i \leqslant \sigma$

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

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

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

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

Example: constrained bivariate interpolation (2/2)

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

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

(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 $\deg(\mathbf{R}) = \Theta(d + \operatorname{amp}(\mathbf{s}))$
with $\operatorname{amp}(\mathbf{s}) = \max(\mathbf{s}) - \min(\mathbf{s})$

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 $\mathbf{s}$