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*

RAIM 2016, Banyuls-sur-Mer, June 29, 2016

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

Invariant: $\sigma = \deg(\det(\mathbf{A})) = 4 + 7 + 3 + 2 = 7 + 1 + 2 + 6$

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]
$\left.\begin{array}{l}\text{triangular}\\ \text{column normalized}\end{array}\right\}$ POT	$\left.\begin{array}{l}\text{row reduced}\\ \text{column normalized}\end{array}\right\}$ TOP
$\begin{bmatrix} 4 & & & \\ 3 & 7 & & \\ 1 & 5 & 3 & \\ 3 & 6 & 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 7 & 0 & 1 & 5 \\ 0 & 1 & & 0 \\ & & 2 & \\ 6 & 0 & 1 & 6 \end{bmatrix}$

Invariant: $\sigma = \deg(\det(\mathbf{A})) = 4+7+3+2 = 7+1+2+6$
$= \text{dimension of } \mathbb{K}[X]^{1\times m}/\mathcal{M} \text{ as a } \mathbb{K}\text{-vector space}$

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 $(\star)$

Shifted Popov form

degree shift: $\mathbf{s} = (s_1, \ldots, s_m) \in \mathbb{Z}^m$ acting as additive weights

$\rightsquigarrow$ shifted row reduced: minimizes the $\mathbf{s}$-degree of $\mathbf{p} = \begin{bmatrix} p_1 & \cdots & p_m \end{bmatrix}$

$$\mathrm{rdeg}_{\mathbf{s}}(\mathbf{p}) = \max_j(\deg(p_j) + s_j)$$

Degree constraints: $\deg(p_j) < N_j$ for all $j \Leftrightarrow \mathrm{rdeg}_{(-N_1,\ldots,-N_m)}(\mathbf{p}) < 0$

$\mathbf{s}$-Popov form $=$ $\mathbf{s}$-row reduced $+$ column normalized

Canonical form:
$\mathbf{UA} = \mathbf{P}$ for unique unimodular $\mathbf{U}$ and $\mathbf{s}$-Popov form $\mathbf{P}$

Shifted Popov form: examples

Connects Popov and Hermite forms. Examples with $m = 4, \sigma = 16$:

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

Recall: $\delta_1 + \cdots + \delta_m = \sigma = \deg(\det(\mathbf{A})) = \deg(\det(\mathbf{P}))$

$\rightsquigarrow$ for $\mathbf{P}$, average column degree: $\sigma/m \quad \Rightarrow \quad$ size: $\mathcal{O}(m\sigma)$

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 $\sigma(\mathbf{A})$	$\sigma(\mathbf{A})$	$\mathcal{O}(m^2 \sigma(\mathbf{A})/m)$	$\widetilde{\mathcal{O}}(m^\omega \sigma(\mathbf{A})/m)$

Example:

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

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

Generic determinant bound:

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

Result

Problem

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

shift $\mathbf{s} \in \mathbb{Z}^m$

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

Previous fastest algorithm: $\widetilde{\mathcal{O}}(m^\omega(d + \mathrm{amp}(\mathbf{s})))$, deterministic
[Gupta-Sarkar-Storjohann-Valeriote, 2012] + [Sarkar-Storjohann, 2011]
$\mathrm{amp}(\mathbf{s}) = \max(\mathbf{s}) - \min(\mathbf{s})$ is between 0 and $m^2 d$
$\rightsquigarrow$ worst-case $\widetilde{\mathcal{O}}(m^{\omega+2} d)$

Result

Problem

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

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

Previous fastest algorithm: $\widetilde{\mathcal{O}}(m^\omega(d + \mathrm{amp}(\mathbf{s})))$, deterministic
[Gupta-Sarkar-Storjohann-Valeriote, 2012] + [Sarkar-Storjohann, 2011]
$\mathrm{amp}(\mathbf{s}) = \max(\mathbf{s}) - \min(\mathbf{s})$ is between 0 and $m^2 d$
$\rightsquigarrow$ worst-case $\widetilde{\mathcal{O}}(m^{\omega+2} d)$

Here: $\widetilde{\mathcal{O}}(m^\omega \sigma(\mathbf{A})/m) \subseteq \widetilde{\mathcal{O}}(m^\omega d)$, probabilistic

- no dependency in $\mathbf{s}$ (except in log factors)
- takes some degree structure into account:
  $\sigma(\mathbf{A})/m \leqslant$ avg. row degree, avg. column degree

Reduction to $\deg(\mathbf{A}) \leqslant \sigma(\mathbf{A})/m$

Problem

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

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

With no field operation, one can 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 $\deg(\widetilde{\mathbf{A}}) \leqslant \lceil \sigma(\mathbf{A})/m \rceil$,
- $\mathbf{s}$-Popov form of $\mathbf{A}$ = principal submatrix of the $\mathbf{t}$-Popov form of $\widetilde{\mathbf{A}}$

thanks to partial linearization techniques [Gupta et al., 2012]

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 $\widetilde{\mathcal{O}}(d)$?

Obstacle: size of the transformation

unimodular transformation $\mathbf{U}$ may have size beyond $\mathcal{O}(m^\omega d)$

Example:

- $\mathbf{A}$ unimodular: $\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_m$
- $\mathbf{P} = \mathbf{I}_m$ for any $\mathbf{s}$
- $\mathbf{U} = \mathbf{A}^{-1}$

$$\underset{\text{degree } d}{\overset{\mathbf{A}}{\begin{bmatrix} 0 & & & & \\ d & 0 & & & \\ & d & 0 & & \\ & & \ddots & \ddots & \\ & & & d & 0 \end{bmatrix}}} \longrightarrow \underset{\text{sum of degrees } \Theta(m^3 d)}{\overset{\mathbf{U} = \mathbf{A}^{-1}}{\begin{bmatrix} 0 & & & & \\ d & 0 & & & \\ 2d & d & 0 & & \\ \vdots & \ddots & \ddots & \ddots & \\ (m-1)d & \cdots & 2d & d & 0 \end{bmatrix}}}$$

Fast Popov form

Step 1: fast row reduction
$\widetilde{\mathcal{O}}(m^\omega d)$
[Giorgi et al., 2003], probabilistic
[Gupta et al., 2012], deterministic

Step 2: fast column normalization
$\widetilde{\mathcal{O}}(m^\omega d)$
[Sarkar-Storjohann, 2011]

[Giorgi et al., 2003]:

- Expansion of $\mathbf{A}^{-1}$ is ultimately linearly recurrent
- Find $2d+1$ high-degree terms $\mathbf{B}$ in expansion of $\mathbf{A}^{-1}$
- 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 $\boldsymbol{\delta} = (\delta_1, \ldots, \delta_m)$ by triangularization from a matrix involving $\mathbf{V}$ and $\mathbf{S}$

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

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

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

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

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

Reduction to linear modular equations: example

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

$\rightsquigarrow$ for $\mathbf{p} = \begin{bmatrix} p_1 & \cdots & p_m \end{bmatrix}$,

$$\mathbf{p} \in \mathrm{RowSpace}(\mathbf{A}) \iff \begin{bmatrix} p_1 & \cdots & p_m \end{bmatrix} \begin{bmatrix} 1 \\ L \\ L^2 \\ \vdots \\ L^{m-1} \end{bmatrix} = 0 \bmod M$$

$$\iff p_1 1 + p_2 L + \cdots + p_m L^{m-1} = 0 \bmod M$$

Reduction to system of modular equations

Smith form of $\mathbf{A}$:

$$\mathbf{UAV} = \operatorname{diag}(1, \ldots, 1, \mathfrak{m}_1, \ldots, \mathfrak{m}_n)$$

Consider $\mathfrak{M} = (\mathfrak{m}_1, \ldots, \mathfrak{m}_n)$ and $[\mathbf{0} \mid \mathbf{F}] = \mathbf{V} \bmod (1, \ldots, 1, \mathfrak{M})$

$\rightsquigarrow$ $(\mathfrak{M}, \mathbf{F})$ computed in probabilistic $\widetilde{\mathcal{O}}(m^\omega d)$ [Gupta-Storjohann, 2011]

Then

$$\mathrm{RowSpace}(\mathbf{A}) \; = \; \{\mathbf{p} \in \mathbb{K}[X]^{1 \times m} \mid \mathbf{pF} = 0 \bmod \mathfrak{M}\}$$

$\rightsquigarrow$ $\mathbf{s}$-Popov form of $\mathbf{A}$ = $\mathbf{s}$-Popov basis of solutions for $(\mathfrak{M}, \mathbf{F})$

Linear systems of modular equations

Input: nonzero moduli $\mathfrak{M} = (\mathfrak{m}_1, \ldots, \mathfrak{m}_n)$
system matrix $\mathbf{F} \in \mathbb{K}[X]^{m \times n}$ with $\deg(\mathbf{F}_{*,j}) < \deg(\mathfrak{m}_j)$
shift $\mathbf{s} \in \mathbb{Z}^m$

Output: $\mathbf{P}$ the $\mathbf{s}$-Popov solution basis for $(\mathfrak{M}, \mathbf{F})$

for $\sigma = \deg(\mathfrak{m}_1) + \cdots + \deg(\mathfrak{m}_n)$,
$\deg(\det(\mathbf{P})) \leqslant \sigma$ $\Longrightarrow$

I/O size	target cost
$\mathcal{O}(m\sigma)$	$\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$

Order bases: $\mathfrak{m}_1 = \cdots = \mathfrak{m}_n = X^{\sigma/n}$ $\rightsquigarrow$ $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$

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

Interpolation bases: $\mathfrak{m}_j =$ product of known linear factors $\rightsquigarrow$ $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$

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

Here: $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ for arbitrary moduli, $n \in \mathcal{O}(m)$

Overview of the algorithm

Similarly to [Jeannerod et al., 2016] for interpolation bases,
divide-and-conquer on n (number of equations):

- recursive calls give $\mathbf{P}^{(1)}$ and $\mathbf{P}^{(2)}$ $\rightsquigarrow$ $\mathbf{P} = \mathrm{ColumnNormalize}(\mathbf{P}^{(2)}\mathbf{P}^{(1)})$
- deduce $\mathbf{s}$-pivot degrees δ of $\mathbf{P}$
- compute $\mathbf{P}$ when knowing δ [Gupta-Storjohann, 2011]

$\rightsquigarrow$ base case: one equation

Difficulty: no recurrence relations like in order/interpolation bases
$\rightsquigarrow$ compute a shifted Popov kernel basis with arbitrary shift:

$$\mathbf{pF} = 0 \bmod \mathfrak{m} \quad \Leftrightarrow \quad \text{for some } q, \quad [\,\mathbf{p} \quad q\,] \begin{bmatrix} \mathbf{F} \\ \mathfrak{m} \end{bmatrix} = 0$$

New divide-and-conquer approach on the shift

New divide-and-conquer approach on the shift

Recall $\deg(\mathbf{F}) < \deg(\mathfrak{m}) = \sigma$

Reduction to kernel basis:

$$\begin{bmatrix} \mathbf{P} & \mathbf{q} \end{bmatrix} = (\mathbf{s}, \min(\mathbf{s}))\text{-Popov kernel basis of } \begin{bmatrix} \mathbf{F} \\ \mathfrak{m} \end{bmatrix}$$

Reduction to order basis:

$$\begin{bmatrix} \mathbf{P} & \mathbf{q} \\ * & * \end{bmatrix} = (\mathbf{s}, \min(\mathbf{s}))\text{-Popov order basis for } \begin{bmatrix} \mathbf{F} \\ \mathfrak{m} \end{bmatrix} \text{ and } \mathrm{amp}(\mathbf{s}) + 2\sigma$$

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

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

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

New divide-and-conquer approach on the shift

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

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

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

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

3. recursive call to find $\delta^{(2)} \rightsquigarrow \mathbf{s}$-pivot degree $\boldsymbol{\delta} = (\boldsymbol{\delta}^{(1)}, \boldsymbol{\delta}^{(0)} + \boldsymbol{\delta}^{(2)})$

$$\mathbf{P}^{(2)} = (\mathbf{s}^{(2)} + \boldsymbol{\delta}^{(0)})\text{-Popov sol. basis for } (\mathbf{G}, \mathfrak{n})$$

4. compute $\mathbf{P}$ from $\boldsymbol{\delta}$ via order basis at order $\mathcal{O}(\sigma)$

Conclusion

Linear systems of modular equations

- $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$
- return basis of solutions
- in $\mathbf{s}$-Popov form
- deterministic

Shifted row reduction of polynomial matrices

- $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma(\mathbf{A}))$
- return $\mathbf{s}$-Popov form
- probabilistic

Example: constrained bivariate interpolation

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

$$\mathcal{M} = \left\{ Q = \sum_{0 \leqslant j < m} Q_j(X) Y^j \in \mathbb{K}[X,Y] \;\middle|\; Q(x_i, y_i) = 0 \text{ for } 1 \leqslant i \leqslant \sigma \right\}$$

Define $M = (X - x_1) \cdots (X - x_\sigma)$ and $L \in \mathbb{K}[X]$ s.t. $L(x_i) = y_i$

$$\rightsquigarrow \text{basis of } \mathcal{M}\text{:} \quad \begin{pmatrix} M \\ Y - L \\ Y^2 - L^2 \\ \vdots \\ Y^{m-1} - L^{m-1} \end{pmatrix} \quad \longleftrightarrow \quad \mathbf{A} = \begin{bmatrix} M & & & & \\ -L & 1 & & & \\ -L^2 & & 1 & & \\ \vdots & & & \ddots & \\ -L^{m-1} & & & & 1 \end{bmatrix}$$

Example: constrained bivariate interpolation

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

$$\mathcal{M} = \left\{ Q = \textstyle\sum_{0 \leqslant j < m} Q_j(X) Y^j \in \mathbb{K}[X, Y] \;\middle|\; Q(x_i, y_i) = 0 \text{ for } 1 \leqslant i \leqslant \sigma \right\}$$

Define $M = (X - x_1) \cdots (X - x_\sigma)$ and $L \in \mathbb{K}[X]$ s.t. $L(x_i) = y_i$

$$\rightsquigarrow \text{basis of } \mathcal{M}\text{:} \quad \begin{pmatrix} M \\ Y - L \\ Y^2 - L^2 \\ \vdots \\ Y^{m-1} - L^{m-1} \end{pmatrix} \quad \longleftrightarrow \quad \mathbf{A} = \begin{bmatrix} M & & & & \\ -L & 1 & & & \\ -L^2 & & 1 & & \\ \vdots & & & \ddots & \\ -L^{m-1} & & & & 1 \end{bmatrix}$$

Problem: find $Q \in \mathcal{M}$ satisfying $\deg(Q_j) < N_j$ for $0 \leqslant j < m$

Approach:

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

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

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

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

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**	$\widetilde{\mathcal{O}}(m^{\omega}(d + \mathrm{amp}(\mathbf{s})))$	

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 $\widetilde{\mathcal{O}}(d)$?