Efficient algorithms for computing univariate relations

Séminaire Géométrie et Algèbre Effectives

Vincent Neiger

XLIM – Université de Limoges

IRMAR, Rennes, October 27, 2017

Outline

- Univariate relations
- Canonical bases of relations
- Main result
- Hermite-Padé approximation
- Rational interpolation & Multivariate interpolation
- General univariate relations
- Conclusion

Hermite-Padé approximation

Over $\mathbb{K} = \mathbb{F}_7$,

$$\begin{bmatrix} p_1 & p_2 & p_3 & p_4 \end{bmatrix} \begin{bmatrix} 5X^3 + 4X^2 + 6X + 4 \\ 2X^3 + X^2 + X + 3 \\ 2X + 1 \\ 4X^3 + X^2 + 4X \end{bmatrix} = 0 \bmod X^4$$

trivial relation $\rightsquigarrow$ $\mathbf{p} = \begin{bmatrix} X^4 & 0 & 0 & 0 \end{bmatrix}$

relation of small degree $\rightsquigarrow$ $\mathbf{p} = \begin{bmatrix} X+5 & 1 & 5 & 1 \end{bmatrix}$

basis of relations $\rightsquigarrow$ $\mathbf{P} = \begin{bmatrix} X+2 & 0 & 6 & 0 \\ X^2 & X^2 & 0 & 0 \\ X+2 & 3X+2 & X & 0 \\ X+5 & 1 & 5 & 1 \end{bmatrix}$

Bivariate interpolation

$\mathcal{I} \subseteq \mathbb{F}_{97}[X,Y] =$
polynomials vanishing at $\{(24,80),(31,73),(15,73),(32,35),(83,66),(27,46),(20,91),(59,64)\}$

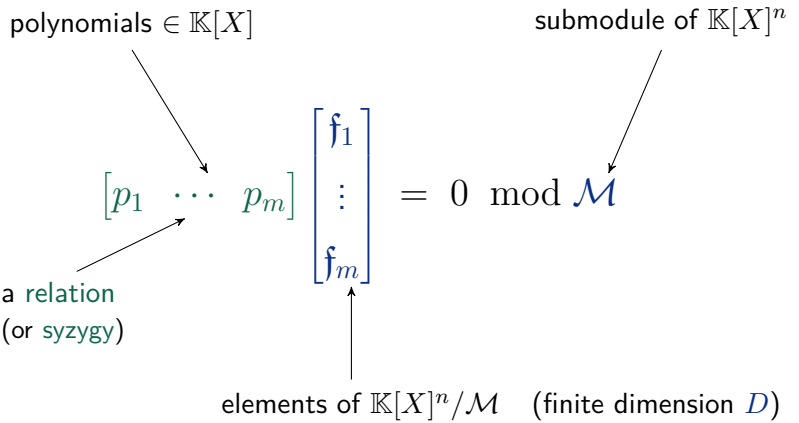
$$\left.\begin{array}{l} M = (X-24)\cdots(X-59) \\ L = \text{Lagrange interpolant} \end{array}\right\} \longrightarrow \quad \mathcal{I} = \langle M(X), Y - L(X)\rangle$$

Degree constraints: $p(X,Y) = \underbrace{p_0(X)}_{\deg\leqslant 4} + \underbrace{p_1(X)}_{\deg\leqslant 2} Y + \underbrace{p_2(X)}_{\deg\leqslant 0} Y^2$

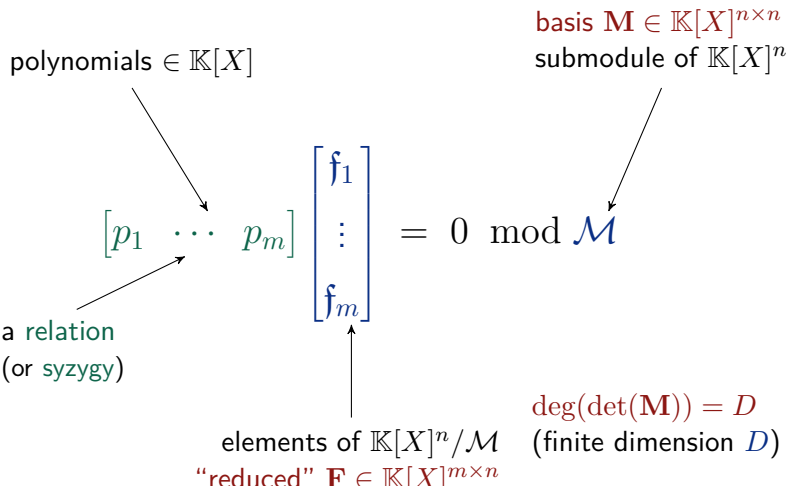
Relation: $p(X,Y) \in \mathcal{I} \quad \Leftrightarrow \quad [p_0 \quad p_1 \quad p_2] \begin{bmatrix} 1 \\ L \\ L^2 \end{bmatrix} = 0 \bmod M(X)$

$\rightsquigarrow \quad p(X,Y) = (2X^4 + 56X^3 + 42X^2 + 48X + 15) + (72X^2 + 12X + 30)Y + Y^2$

Relations / matrix equations



Relations / matrix equations



Basis of relations

Relations form a submodule $\mathcal{R} = \{\mathbf{p} \in \mathbb{K}[X]^m \mid \mathbf{pF} = 0 \bmod \mathbf{M}\}$

- compute a basis of $\mathcal{R}$
- with nice properties
  (minimal degrees, canonical, helps for computing mod $\mathcal{R}$, ...)

Hermite basis:

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

Popov basis:

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

Shifted Popov basis

- connects Popov and Hermite forms
- useful to find relations with degree constraints
- average column degree D/m

Shifted Popov basis

- connects Popov and Hermite forms
- useful to find relations with degree constraints
- average column degree D/m

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

Fastest algorithm

Problem:

Input: nonsingular basis $\mathbf{M} \in \mathbb{K}[X]^{n \times n}$
elements $\mathbf{F} \in \mathbb{K}[X]^{m \times n}$
shift $\mathbf{s} \in \mathbb{Z}^m$

Output: the $\mathbf{s}$-Popov basis of $\{\mathbf{p} \in \mathbb{K}[X]^m \mid \mathbf{pF} = 0 \bmod \mathbf{M}\}$

Result 1 (with C.-P. Jeannerod, E. Schost, G. Villard)

$$\mathbf{M} = \begin{bmatrix} M_1 & & & \\ & M_2 & & \\ & & \ddots & \\ & & & M_n \end{bmatrix}$$

with known roots and multiplicities

cost: $\widetilde{\mathcal{O}}(m^{\omega-1}D)$

assuming $\mathbf{F}$ is reduced modulo $\mathbf{M}$:
$\operatorname{cdeg}(\mathbf{F}) < (\deg(M_1), \ldots, \deg(M_n))$

Fastest algorithm

Problem:

Input: nonsingular basis $\mathbf{M} \in \mathbb{K}[X]^{n \times n}$
elements $\mathbf{F} \in \mathbb{K}[X]^{m \times n}$
shift $\mathbf{s} \in \mathbb{Z}^m$

Output: the $\mathbf{s}$-Popov basis of $\{\mathbf{p} \in \mathbb{K}[X]^m \mid \mathbf{pF} = 0 \bmod \mathbf{M}\}$

Result 2 (with Vu T. X.)

$$\mathbf{M} = \begin{bmatrix} M_1 & * & \cdots & * \\ & M_2 & \cdots & * \\ & & \ddots & \\ & & & M_n \end{bmatrix}$$

in Hermite form

cost: $\widetilde{\mathcal{O}}(m^{\omega-1}D + n^\omega D/m)$

assuming $\mathbf{F}$ is reduced modulo $\mathbf{M}$:
$\operatorname{cdeg}(\mathbf{F}) < (\deg(M_1), \ldots, \deg(M_n))$

Basis of relations

$$\mathbf{pF} \;=\; 0 \bmod \mathbf{M}$$

Hermite-Padé approximation

$$\mathbf{pF} \;=\; 0 \bmod X^D$$

Multivariate interpolation

$$p(x_i, y_i) \;=\; 0 \text{ for } 1 \leqslant i \leqslant D$$

Normal forms of matrices

$$\mathbf{M} \in \mathbb{K}[X]^{m \times m} \xrightarrow{\text{unimodular}} \mathbf{P}$$

Basis of relations

$$\mathbf{pF} \;=\; 0 \bmod \mathbf{M}$$

Hermite-Padé approximation

$$\mathbf{pF} \;=\; 0 \bmod X^D$$

Multivariate interpolation

$$p(x_i, y_i) \;=\; 0 \text{ for } 1 \leqslant i \leqslant D$$

Normal forms of matrices

$$\mathbf{M} \in \mathbb{K}[X]^{m \times m} \xrightarrow{\text{unimodular}} \mathbf{P}$$

A ubiquitous tool

- guess linear differential equations:
  $p_0 + p_1 S + p_2 S^{(2)} + \cdots + p_m S^{(m)} = 0$

- factor differential operators [Van Hoeij, 1997]

- reconstruct algebraic equations:
  find $p(X, Y) \in \mathbb{K}[X, Y]$ such that $p(X, S(X)) = 0$

- find generator for linearly recurrent matrix sequence
  $\rightsquigarrow$ block Wiedemann algorithm

- polynomial matrix computations:
  kernels, inversion, basis reduction, Hermite form, determinant, ...

- solve block-Hankel linear systems [Bostan - Jeannerod - Schost, 2008]

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

shift: $\mathbf{s} = [0, 0, 0, 0]$

$$\mathbf{F} = \begin{bmatrix} 1 \\ 1 + X \\ X + X^2 \\ X^2 + X^3 \end{bmatrix}$$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants
$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \end{bmatrix}$$

current order: $D = 0$ current shift: $\mathbf{s} = [0, 0, 0, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} 1 \\ 1 + X \\ X + X^2 \\ X^2 + X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} 1 & & & & \\ -1 & 1 & & & \\ & & 1 & & \\ & & & 1 & \end{bmatrix}$$

current order: $D = 0$ current shift: $\mathbf{s} = [0, 0, 0, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} 1 \\ X \\ X + X^2 \\ X^2 + X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants
$$\begin{bmatrix} X & & & & \\ -1 & 1 & & & \\ & & 1 & & \\ & & & 1 & \end{bmatrix}$$

current order: $D = 1$ current shift: $\mathbf{s} = [1, 0, 0, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} X \\ X \\ X + X^2 \\ X^2 + X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants
$$\begin{bmatrix} X & & & & \\ -1 & 1 & & & \\ & & 1 & & \\ & & & 1 & \end{bmatrix}$$

current order: $D = 1$ current shift: $\mathbf{s} = [1, 0, 0, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} X \\ X \\ X + X^2 \\ X^2 + X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ -1 & 1 & & \\ 1 & -1 & 1 & \\ & & & 1 \end{bmatrix}$$

current order: $D = 1$ current shift: $\mathbf{s} = [1, 0, 0, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ X \\ X^2 \\ X^2 + X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ -X & X & & \\ 1 & -1 & 1 & \\ & & & 1 \end{bmatrix}$$

current order: $D = 2$ current shift: $\mathbf{s} = [1, 1, 0, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ X^2 \\ X^2 \\ X^2 + X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ -X & X & & \\ 1 & -1 & 1 & \\ & & & 1 \end{bmatrix}$$

current order: $D = 2$ current shift: $\mathbf{s} = [1, 1, 0, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ X^2 \\ X^2 \\ X^2 + X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ -X-1 & X+1 & -1 & \\ 1 & -1 & 1 & \\ -1 & 1 & -1 & 1 \end{bmatrix}$$

current order: $D = 2$ current shift: $\mathbf{s} = [1, 1, 0, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ 0 \\ X^2 \\ X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ -X-1 & X+1 & -1 & \\ X & -X & X & \\ -1 & 1 & -1 & 1 \end{bmatrix}$$

current order: $D = 3$ current shift: $\mathbf{s} = [1, 1, 1, 0]$

Residual: $$\mathbf{G} = \begin{bmatrix} 0 \\ 0 \\ X^3 \\ X^3 \end{bmatrix}$$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ -X-1 & X+1 & -1 & \\ X & -X & X & \\ -1 & 1 & -1 & 1 \end{bmatrix}$$

current order: $D = 3$ current shift: $\mathbf{s} = [1, 1, 1, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ 0 \\ X^3 \\ X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ X-1 & X+1 & -1 & \\ X+1 & -X-1 & X+1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$$

current order: $D = 3$ current shift: $\mathbf{s} = [1, 1, 1, 0]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ X^3 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ X-1 & X+1 & -1 & \\ X+1 & -X-1 & X+1 & -1 \\ -X & X & -X & X \end{bmatrix}$$

current order: $D = 4$ current shift: $\mathbf{s} = [1, 1, 1, 1]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ X^4 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ X-1 & X+1 & -1 & \\ X+1 & -X-1 & X+1 & -1 \\ -X^2 & X^2 & -X^2 & X^2 \end{bmatrix}$$

current order: $D = 5$ current shift: $\mathbf{s} = [1, 1, 1, 2]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ X^5 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ X-1 & X+1 & -1 & \\ X+1 & -X-1 & X+1 & -1 \\ -X^3 & X^3 & -X^3 & X^3 \end{bmatrix}$$

current order: $D = 6$ current shift: $\mathbf{s} = [1, 1, 1, 3]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ X^6 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ X-1 & X+1 & -1 & \\ X+1 & -X-1 & X+1 & -1 \\ -X^4 & X^4 & -X^4 & X^4 \end{bmatrix}$$

current order: $D = 7$ current shift: $\mathbf{s} = [1, 1, 1, 4]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ X^7 \end{bmatrix}$

Iterative algorithm

Early 1990s, cost $\mathcal{O}(mD^2)$ [Beckermann - Labahn] [Van Barel - Bultheel]

Example in dimensions $m = 4, n = 1, D = 8$
Module: $\mathbf{M} = [X^8]$

Basis of approximants

$$\begin{bmatrix} X+1 & -1 & & \\ X-1 & X+1 & -1 & \\ X+1 & -X-1 & X+1 & -1 \\ -X^5 & X^5 & -X^5 & X^5 \end{bmatrix}$$

current order: $D = 8$ current shift: $\mathbf{s} = [1, 1, 1, 5]$

Residual: $\mathbf{G} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ X^8 \end{bmatrix}$

Divide-and-conquer via multiplication

$$\mathbf{pF} = 0 \bmod \begin{bmatrix} X^d & & \\ & \ddots & \\ & & X^d \end{bmatrix}$$

Target cost:
$$\widetilde{\mathcal{O}}(m^{\omega-1}D) = \widetilde{\mathcal{O}}(m^{\omega-1}nd)$$

Approach: [Beckermann-Labahn, 1994] [Giorgi-Jeannerod-Villard, 2003]

- $\mathbf{P}^{(1)}$:= $\mathbf{s}$-reduced for $\mathbf{F}$ and $d/2$
- $\mathbf{G}$ and $\mathbf{t}$:= update $\mathbf{F}$ and $\mathbf{s}$
- $\mathbf{P}^{(2)}$:= $\mathbf{t}$-reduced for $\mathbf{G}$ and $d/2$
- return $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$ ← $\mathbf{s}$-reduced basis for $\mathbf{F}$ and d

$$\mathbf{G} = (X^{-d/2}\mathbf{P}^{(1)}\mathbf{F}) \bmod X^{d/2}$$

$\mathbf{P}^{(1)}$ and $\mathbf{P}^{(2)}$: $m \times m$ of degree $\leqslant d/2$
$\mathbf{P}^{(2)}\mathbf{P}^{(2)}$: $m \times m$ of degree $\leqslant d$

Cost bound: $\widetilde{\mathcal{O}}(m^{\omega-1}(m+n)d)$

$\rightsquigarrow$ achieves target if **wide matrix** $\mathbf{F}$ (i.e. $m \leqslant n$)

Degree control assuming small shifts

wide case: very efficient algorithm

$\rightsquigarrow$ obstacle in tall case: controlling the degrees in the basis

Input $\mathbf{F}$ $\qquad$ $\mathbf{0}$-reduced basis for $d = 128$

Example: $\begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1+X \\ X+X^2 \\ X^2+X^3 \end{bmatrix} \longrightarrow \begin{bmatrix} X+1 & -1 & & \\ X-1 & X+1 & -1 & \\ X+1 & X-1 & X+1 & -1 \\ X^{125} & X^{125} & -X^{125} & X^{125} \end{bmatrix}$

Assume $\mathbf{s} = (s_1, \ldots, s_m)$ **almost uniform**

$\Rightarrow$ average row degree $\mathcal{O}(nd/m)$

Under this assumption: $\widetilde{\mathcal{O}}(m^{\omega-1}nd)$ [Zhou-Labahn, 2012]

using transformations in [Storjohann, 2006] to **rely on wide case**

Degree control via normalized basis

What about arbitrary shifts? (e.g. Hermite)

Example: $\mathbf{s} = (0,0,0,0,d,d,d,d)$, same f_1, f_2, f_3, f_4 / random f_5, f_6, f_7, f_8

Degrees in $\mathbf{s}$-reduced basis:

$$\begin{bmatrix} 1 & 0 & & & & & & \\ 1 & 1 & 0 & & & & & \\ 1 & 1 & 1 & 0 & & & & \\ 125 & 125 & 125 & 125 & & & & \\ 124 & 124 & 124 & 124 & 0 & & & \\ 124 & 124 & 124 & 124 & & 0 & & \\ 124 & 124 & 124 & 124 & & & 0 & \\ 124 & 124 & 124 & 124 & & & & 0 \end{bmatrix}$$

size $m^2 d$

Degrees in $\mathbf{s}$-Popov basis:

$$\begin{bmatrix} 1 & 0 & & & & & & \\ 0 & 1 & 0 & & & & & \\ 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 125 & & & & \\ 0 & 0 & 0 & 124 & 0 & & & \\ 0 & 0 & 0 & 124 & & 0 & & \\ 0 & 0 & 0 & 124 & & & 0 & \\ 0 & 0 & 0 & 124 & & & & 0 \end{bmatrix}$$

size mnd

$\mathbf{s}$-Popov basis: **aim** & **means**

average column degree $\leqslant \frac{D}{m} = \frac{nd}{m}$ **independently of** $\mathbf{s}$

Degree control via normalized basis

Degree control $\rightsquigarrow$ compute the $\mathbf{s}$-Popov basis $\mathbf{P}$

- $\mathbf{s}$-Popov not compatible with **multiplication**
- size of product beyond target cost

$\rightsquigarrow$ change how to combine $\mathbf{P}^{(1)}$ and $\mathbf{P}^{(2)}$

- $\mathbf{P}^{(1)} := \mathbf{s}$-Popov
- $\mathbf{G}$ and $\mathbf{t} := \cdots$
- $\mathbf{P}^{(2)} := \mathbf{t}$-Popov
- return $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$

diagonal degrees of $\mathbf{P}$: $\boldsymbol{\delta} = \boldsymbol{\delta}^{(1)} + \boldsymbol{\delta}^{(2)}$

knowing $\boldsymbol{\delta}$, reduce to **wide case**

General fast algorithm

Diagonal degrees $\boldsymbol{\delta}$ $\Rightarrow$ $\left\{ \begin{array}{c} \mathbf{s}\text{-Popov basis} = -\boldsymbol{\delta}\text{-Popov basis} \\ -\boldsymbol{\delta} \textbf{ almost uniform} \end{array} \right.$

1. $\mathbf{B} := -\boldsymbol{\delta}$-reduced basis (via [Storjohann, 2006] + **wide case**)
2. $\mathbf{P} :=$ normalize $\mathbf{B}$ into $-\boldsymbol{\delta}$-Popov basis (constant transformation)

Result: $\widetilde{\mathcal{O}}(m^{\omega-1}D)$

- arbitrary shift $\mathbf{s}$
- arbitrary orders
- returning $\mathbf{s}$-Popov basis

$$\mathbf{pF} = 0 \bmod \begin{bmatrix} X^{d_1} & & \\ & \ddots & \\ & & X^{d_n} \end{bmatrix}$$

$D := d_1 + \cdots + d_n$

Basis of relations

$$\mathbf{pF} \;=\; 0 \bmod \mathbf{M}$$

Hermite-Padé approximation

$$\mathbf{pF} \;=\; 0 \bmod X^D$$

Multivariate interpolation

$$p(x_i, y_i) \;=\; 0 \text{ for } 1 \leqslant i \leqslant D$$

Normal forms of matrices

$$\mathbf{M} \in \mathbb{K}[X]^{m \times m} \xrightarrow{\text{unimodular}} \mathbf{P}$$

List-decoding Reed-Solomon codes

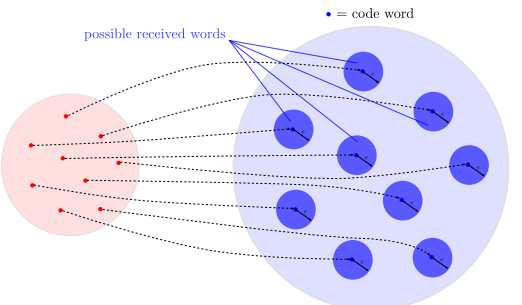
Reliable delivery of data over an unreliable communication channel

$$w = w_0 + \cdots + w_k X^k \xrightarrow{\text{encoding}} (w(x_1), \ldots, w(x_D)) \xrightarrow{\text{noise}} (y_1, \ldots, y_D)$$

Few errors during transmission: $w(x_i) = y_i$ for many i's

Retrieve w via bivariate interpolation + root finding [Guruswami-Sudan, 1999]

$$\left.\begin{array}{c} p(x_i, y_i) = 0 \\ \text{small degree } p(X, Y) \end{array}\right\} \Longrightarrow p(X, w(X)) = 0$$



Seeing interpolants as relations

Constrained **bivariate** interpolation: $p(x_i, y_i) = 0$ for all i

- Y-constraint: $\deg_Y < m \Rightarrow$ **univariate** relation

$$\begin{bmatrix} p_0 & p_1 & \cdots & p_{m-1} \end{bmatrix} \begin{bmatrix} 1 \\ L \\ \vdots \\ L^{m-1} \end{bmatrix} = 0 \bmod (X - x_1) \cdots (X - x_D)$$

- X-constraint: satisfied via s-Popov

$\rightarrow$ **Generalization of approximants:**

relations modulo $\mathbf{M} = \begin{bmatrix} M_1 & & \\ & \ddots & \\ & & M_n \end{bmatrix}$

- $M_1, \ldots, M_n$ split over $\mathbb{K}$
- known roots and multiplicities

Generalizing approximation techniques

- residual $\mathbf{G} := \mathbf{P}^{(1)}\mathbf{F} \bmod (M_1, \ldots, M_n)$ $\rightsquigarrow$ fast via CRT
- divide and conquer via multiplication
- divide and conquer via "find & use degrees"

Efficiency: generalization of the **wide case**?

Fact: degree of output at most $\operatorname{lcm}(M_1, \ldots, M_n)$

$$\bmod X^D \quad \rightarrow \quad \bmod \begin{bmatrix} X^d & & \\ & \ddots & \\ & & X^d \end{bmatrix}$$

$$\bmod (X - x_1) \cdots (X - x_D) \quad \rightarrow \quad \bmod \begin{bmatrix} \prod_i (X - x_i^{(1)}) & & \\ & \ddots & \\ & & \prod_i (X - x_i^{(n)}) \end{bmatrix}$$

Interpolation: controlling the degrees

No "wide case", yet: almost uniform shift $\Rightarrow$ small average degree

- shift modified in recursive calls
- shift may become far from uniform

$\rightsquigarrow$ intermediate bases may have large degrees

change shift processing to keep it uniform:

- all recursive calls with **uniform shift**
- correction via **change of shift**

efficiency: fast kernel basis [Zhou et al., 2012]

$\rightsquigarrow$ **fast algorithm for $\mathbf{s}$ almost uniform**

- $\mathbf{P}^{(1)} := \mathbf{0}$-reduced
- $\mathbf{G}$ and $\mathbf{t} := \cdots$
- $\mathbf{P}^{(2)} := \mathbf{0}$-reduced
- $\mathrm{Shift}(\mathbf{P}^{(2)}, \mathbf{t})$
- return $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$

Bases of interpolants: result

- arbitrary shift $\mathbf{s}$
- arbitrary diagonal with known linear factors
- returning s-Popov basis

$$\mathbf{pF} = 0 \bmod \begin{bmatrix} M_1 & & \\ & \ddots & \\ & & M_n \end{bmatrix}$$

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

Cost bound: $\widetilde{\mathcal{O}}(m^{\omega-1}D)$

Improves upon previous work:

- iterative [Kötter, 1996+2003] [Nielsen-Høholdt, 1998] [Beckermann-Labahn, 2000]
- divide and conquer [Nielsen (Rosenkilde), 2014]
- based on fast basis reduction [Cohn-Heninger, 2012+2015]

$\rightsquigarrow$ list- and soft-decoding of Reed-Solomon codes
$\rightsquigarrow$ robust Private Information Retrieval [Devet-Goldberg-Heninger, 2012]

Basis of relations

$$\mathbf{pF} \;=\; 0 \bmod \mathbf{M}$$

Hermite-Padé approximation

$$\mathbf{pF} \;=\; 0 \bmod X^D$$

Multivariate interpolation

$$p(x_i, y_i) \;=\; 0 \text{ for } 1 \leqslant i \leqslant D$$

Normal forms of matrices

$$\mathbf{M} \in \mathbb{K}[X]^{m\times m} \xrightarrow{\text{unimodular}} \mathbf{P}$$

Normal forms of polynomial matrices

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

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

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

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

Normal forms of polynomial matrices

Problem: matrix $\mathbf{M}$, shift $\mathbf{s} \longrightarrow$ $\mathbf{s}$-Popov basis of $\mathrm{RowSpace}(\mathbf{M})$

Input: $n \times n$ matrix
- of degree $\leqslant d \rightarrow$ size $n^2 d$
- of generic det. degree $\leqslant D \rightarrow$ size nD

- Popov form: $\widetilde{\mathcal{O}}(n^\omega d)$ [Giorgi et al., 2003] [Gupta et al., 2011+2012]
- Hermite form: $\widetilde{\mathcal{O}}(n^\omega d)$ Las Vegas [Gupta-Storjohann 2011]
- Hermite form: $\widetilde{\mathcal{O}}(n^{\omega-1} D)$ (with G. Labahn & W. Zhou)

Fast algorithm for arbitrary shifts?

$$\mathrm{RowSpace}(\mathbf{M}) = \{\mathbf{p} \mid \mathbf{p} = \mathbf{q}\mathbf{M} \text{ for some } \mathbf{q}\} = \{\mathbf{p} \mid \mathbf{p} \cdot \mathrm{Id} = 0 \bmod \mathbf{M}\}$$

Relations modulo arbitrary $\mathbf{M}$

Normal form problem = s-Popov relation basis for $\mathbf{F} = \mathrm{Id}$ modulo $\mathbf{M}$

if $\mathbf{M} = \begin{bmatrix} \mathbf{M}_1 & \mathbf{A} \\ \mathbf{0} & \mathbf{M}_2 \end{bmatrix}$

$\rightsquigarrow$ divide and conquer

- $\mathbf{P}^{(1)}$ for $\mathbf{F}$ and $\mathbf{M}_1$
- $[\mathbf{0} \mid \mathbf{G}] = \mathbf{P}^{(1)}\mathbf{F} \bmod \mathbf{M}$
- $\mathbf{P}^{(2)}$ for $\mathbf{G}$ and $\mathbf{M}_2$
- return $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$

Precomputation: transform $\mathbf{M}$ into Hermite form (relations unchanged)

Main obstacles:

- computing residuals $\mathbf{PF} \bmod \mathbf{M}$
  done efficiently via fast matrix division + partial linearization + high-order lifting
- base case: linear modular equation $(n = 1)$
  $\mathbf{p}\,\mathbf{f} = 0 \bmod M \quad (M \in \mathbb{K}[X], \mathbf{f} \in \mathbb{K}[X]^{m \times 1})$

roots unknown: how to divide and conquer?

Relations modulo arbitrary $\mathbf{M}$

$$\mathbf{p}\,\mathbf{f} = 0 \bmod M \Leftrightarrow \begin{bmatrix}\mathbf{p} & q\end{bmatrix}\begin{bmatrix}\mathbf{F}\\ M\end{bmatrix} = 0 \text{ for some quotient } q$$

$\Rightarrow$ difficulty: fast s-Popov kernel basis of a column vector

Base case: $\mathbf{s}$ almost uniform $\Rightarrow$ via approximant basis in $\widetilde{\mathcal{O}}(m^{\omega-1}D)$

New divide and conquer approach
based on finding a "splitting index"
$\mathbf{s} \to (\mathbf{s}^{(1)}, \mathbf{s}^{(2)})$ with half the amplitude

$$\begin{bmatrix}\mathbf{P}^{(1)} & \mathbf{0} & \mathbf{q}^{(1)}\\ * & \mathbf{P}^{(2)} & \mathbf{q}^{(2)}\\ * & * & *\end{bmatrix}\begin{bmatrix}\mathbf{F}^{(1)}\\ \mathbf{F}^{(2)}\\ M\end{bmatrix}$$

Result: $\widetilde{\mathcal{O}}(m^{\omega-1}D + n^{\omega}D/m)$

- arbitrary shift $\mathbf{s}$
- arbitrary Hermite form $\mathbf{M}$
- returning s-Popov basis

$$\mathbf{pF} = 0 \bmod \begin{bmatrix}M_1 & * & \cdots & *\\ & M_2 & \ddots & *\\ & & \ddots & *\\ & & & M_n\end{bmatrix}$$

Summary and perspectives

approximation / interpolation

- cost bound $\widetilde{\mathcal{O}}(m^{\omega-1}D)$
- solves the general case
- basis in s-Popov form

relations modulo arbitrary $\mathbf{M}$

- cost bound Hermite form + $\widetilde{\mathcal{O}}(m^{\omega-1}D + n^{\omega}D/m)$
- basis in s-Popov form

  $\rightsquigarrow$ deterministic s-Popov form of a matrix in $\widetilde{\mathcal{O}}(m^{\omega-1}D_{\mathrm{gen}})$

ongoing work and perspectives

- normal form of a rectangular/singular matrix? [with J. Rosenkilde & G. Solomatov]
- fast and deterministic Smith form?
- what about multi-level structures?