Bases of relations in one or several variables: fast algorithms and applications

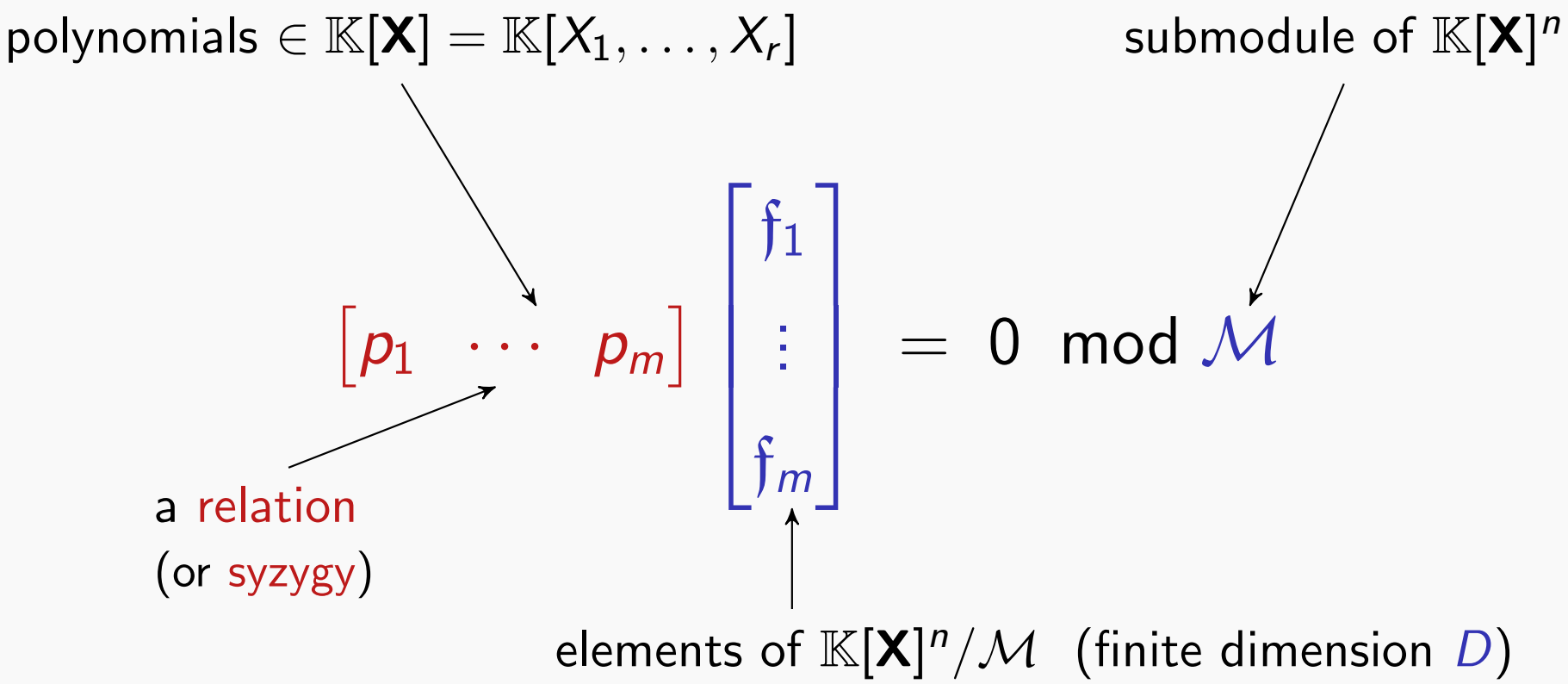
Vincent Neiger

ENS de Lyon – **C.-P. Jeannerod, G. Villard**
U. of Waterloo – **É. Schost**

PhD defense

November 30, 2016

Relations



$\rightsquigarrow$ relations form a submodule of $\mathbb{K}[\mathbf{X}]^m$

Hermite-Padé approximation

Over $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$,

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

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 with degree constraints

$\mathcal{M} =$ polynomials vanishing at $\{(24,80),(31,73),(15,73),(32,35),(83,66),(27,46),(20,91),(59,64)\}$

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

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

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

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

Basis of relations

Problem: given $\mathcal{M}$ and $\mathbf{f}$,

- compute a basis of the module of relations $\mathcal{R}$
- with nice properties: unique, minimal degrees, computing mod $\mathcal{R}$, ...

univariate

shift $\mathbf{s} = (s_1, \ldots, s_m) \in \mathbb{Z}^m$

s-Popov basis

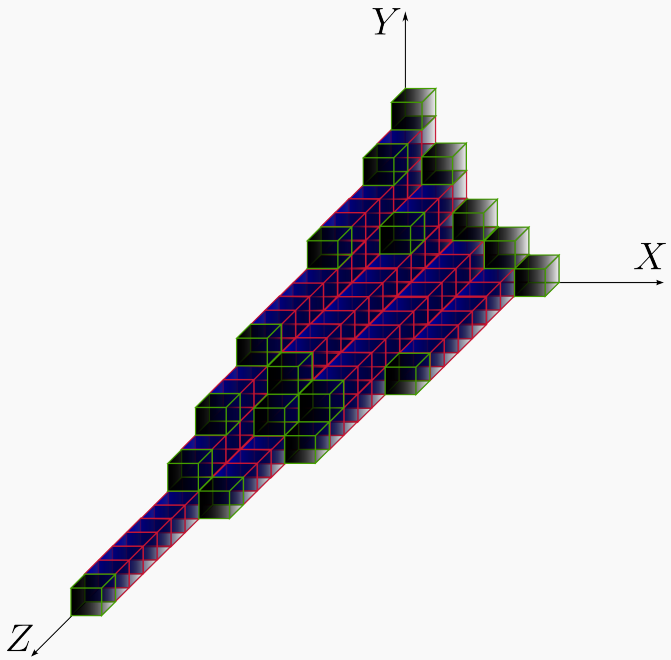
Hermite: $\begin{bmatrix} X^2+3X+2 & & \\ 5X+6 & X+1 & \\ 4X & 3 & 1 \end{bmatrix}$

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

multivariate

monomial order $\prec$ on $\mathbb{K}[\mathbf{X}]^m$

$\prec$-Gröbner basis



Basis of relations

$\mathbf{pf} \;=\; 0 \bmod \mathcal{M}$

knowing multiplication matrices

Hermite-Padé approximation

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

Multivariate interpolation

$\rightsquigarrow$ list-decoding algorithms

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

Change of monomial order

$\rightsquigarrow$ polynomial system solving

$\prec_1$-GB of $\mathcal{M} \longrightarrow \prec_2$-GB of $\mathcal{M}$

Basis of relations

$\mathbf{pf} \;=\; 0 \bmod \mathcal{M}$

knowing multiplication matrices

Hermite-Padé approximation

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

Multivariate interpolation

$\rightsquigarrow$ list-decoding algorithms

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

Normal forms of matrices

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

Change of monomial order

$\rightsquigarrow$ polynomial system solving

$\prec_1$-GB of $\mathcal{M} \longrightarrow \prec_2$-GB of $\mathcal{M}$

Basis of relations

$\mathbf{pf} \equiv 0 \bmod \mathcal{M}$

knowing multiplication matrices

Hermite-Padé approximation

$\mathbf{pf} \equiv 0 \bmod X^D$

Multivariate interpolation

$\rightsquigarrow$ list-decoding algorithms

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

Normal forms of matrices

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

Bases of relations via linear algebra

$\mathcal{V} = \mathbb{K}[X_1, \ldots, X_r]^n / \mathcal{M}$ is a $\mathbb{K}$-vector space of dimension D

Linear algebra viewpoint:

- matrix $\mathbf{E} = \begin{bmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_m \end{bmatrix} \in \mathbb{K}^{m \times D}$ (equation $\begin{bmatrix} \mathfrak{f}_1 \\ \vdots \\ \mathfrak{f}_m \end{bmatrix} \in \mathcal{V}^{m \times 1}$)
- matrix $\mathbf{M}_i \in \mathbb{K}^{D \times D}$, $1 \leqslant i \leqslant r$ (multiplying by X_i in $\mathcal{V}$)

$$[p_1 \ \cdots \ p_m] \begin{bmatrix} \mathfrak{f}_1 \\ \vdots \\ \mathfrak{f}_m \end{bmatrix} = \sum_{\mathbf{j},i} \underbrace{\alpha_{\mathbf{j},i}}_{\in \mathbb{K}} X_1^{j_1} \cdots X_r^{j_r} \mathfrak{f}_i$$

relation $=$ $\mathbb{K}$-linear relation between $\{\mathbf{e}_i \underbrace{\mathbf{M}_1^{j_1} \cdots \mathbf{M}_r^{j_r}}_{\in \mathbb{K}^{1 \times D}}\}_{\mathbf{j},i}$

Bases of relations via linear algebra

basis of relations = subset of nullspace of multi-Krylov matrix

$\prec_{\text{lex}}^{\text{top}}$ order:

$$\begin{bmatrix} \begin{bmatrix} \mathbf{E} \\ \mathbf{E}\mathbf{M}_1 \\ \vdots \\ \mathbf{E}\mathbf{M}_1^D \end{bmatrix} & & \\ \begin{bmatrix} \mathbf{E} \\ \mathbf{E}\mathbf{M}_1 \\ \vdots \\ \mathbf{E}\mathbf{M}_1^D \end{bmatrix} \mathbf{M}_2 & & \\ \vdots & & \\ \begin{bmatrix} \mathbf{E} \\ \mathbf{E}\mathbf{M}_1 \\ \vdots \\ \mathbf{E}\mathbf{M}_1^D \end{bmatrix} \mathbf{M}_2^D & & \end{bmatrix}$$

Bases of relations via linear algebra

basis of relations = subset of nullspace of multi-Krylov matrix

$\prec_{\text{lex}}^{\text{top}}$ order:

$$\begin{bmatrix} \begin{bmatrix} \mathbf{E} \\ \mathbf{E}\mathbf{M}_1 \\ \vdots \\ \mathbf{E}\mathbf{M}_1^D \end{bmatrix} \\ \begin{bmatrix} \mathbf{E} \\ \mathbf{E}\mathbf{M}_1 \\ \vdots \\ \mathbf{E}\mathbf{M}_1^D \end{bmatrix} \mathbf{M}_2 \\ \vdots \\ \begin{bmatrix} \mathbf{E} \\ \mathbf{E}\mathbf{M}_1 \\ \vdots \\ \mathbf{E}\mathbf{M}_1^D \end{bmatrix} \mathbf{M}_2^D \end{bmatrix}$$

ω: $D \times D$ matrix multiplication in $\mathcal{O}(D^\omega)$ operations

- [Keller-Gehrig, 1985]: $\text{charpoly}(\mathbf{M})$ in $\mathcal{O}(D^\omega \log(D))$ (one variable, $\mathbf{E} = \text{Id}$, output = Hermite)
- [FGLM, 1993]: general case in $\mathcal{O}(rD^3)$
- [Beckermann&Labahn, 2000]: $\mathcal{O}(mD^2)$ for structured $\mathbf{M}$ (one variable)
- [Faugère et al., 2014]: for $\prec_{\text{lex}}$ and Shape position, $\mathcal{O}(D^\omega \log(D) + r\mathsf{M}(D)\log(D))$

General case with fast matrix multiplication?

General algorithm incorporating fast linear algebra

Algorithm:

1. compute monomial basis = first independent rows
2. find $\prec$-Gröbner basis by nullspace computation

Difficulty: incorporate fast multiplication in **1.** for any $\prec$

- $X_1, \ldots, X_r \rightsquigarrow$ gather operations involving $\mathbf{M}_i$
- $X_i, X_i^2, X_i^4, \ldots \rightsquigarrow$ gather operations involving $\mathbf{M}_i^{2^j}$

$\Big\}$ as if $\prec_{\text{lex}}^{\text{top}}$

- insert new rows according to the order $\prec$

Cost bound: $\mathcal{O}(rD^\omega \log(D))$ field operations

Size of dense representations:

input	output
rD^2	$\leqslant rD^2$

Change of monomial order

Problem: $\prec_1$-GB of $\mathcal{M} \longrightarrow \prec_2$-GB of $\mathcal{M}$

$= \prec_2$-GB of relations: $\mathbf{p}1 = 0 \bmod \mathcal{M}$

Approach: [FGLM, 1993]

1. compute $\mathbf{M}_1, \ldots, \mathbf{M}_r$ from $\prec_1$-GB
2. compute the $\prec_2$-GB of relations

[FGLM, 1993] $\rightarrow \mathcal{O}(rD^3)$

$\mathcal{O}(rD^\omega \log(D))$

Result (case of ideals):
step **1.** in $\mathcal{O}(rD^\omega \log(D))$

assuming the $\prec_1$-initial ideal is Borel-fixed

$\rightsquigarrow$ extends [Faugère et al., 2014]

Change of monomial order

$\rightsquigarrow$ polynomial system solving

$\prec_1$-GB of $\mathcal{M} \longrightarrow \prec_2$-GB of $\mathcal{M}$

Basis of relations

$\mathbf{pf} \;=\; 0 \bmod \mathcal{M}$

knowing multiplication matrices

Hermite-Padé approximation

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

Multivariate interpolation

$\rightsquigarrow$ list-decoding algorithms

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

Normal forms of matrices

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

Approximant bases: divide-and-conquer via multiplication

$m \times n$ matrix of degree $< d = D/n$

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

module $\mathcal{M} = X^d \mathbb{K}[X]^n$

divide-and-conquer approach
[Beckermann-Labahn, 1994]
[Giorgi-Jeannerod-Villard, 2003]

- $\mathbf{P}^{(1)}$:= **s**-reduced for **f** and $d/2$
- **g** and **t** := update **f** and **s**
- $\mathbf{P}^{(2)}$:= **t**-reduced for **g** and $d/2$
- return $\underline{\mathbf{P}^{(2)}\mathbf{P}^{(1)}}$

s-reduced basis

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

Cost bound: $\mathcal{O}(m^\omega \mathrm{M}(d) \log(d))$

$\rightsquigarrow$ very efficient in **balanced case** ($n \approx m$)

size of input: mnd, with $n \in \mathcal{O}(m)$

Approximant bases: degree control assuming small shifts

very efficient algorithm in **balanced case**

$\rightsquigarrow$ difficulty for improvements: controlling the output degrees

Input $\mathbf{f}$ — **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 $\mathcal{O}(nd/m)$
$\Rightarrow$ output size = input size = $\mathcal{O}(mnd)$

if n is small,
$\tilde{\mathcal{O}}(m^\omega d)$ not satisfactory

Under this assumption: $\tilde{\mathcal{O}}(m^{\omega-1}nd)$ [Zhou-Labahn, 2012]
using Storjohann's transformations [Storjohann, 2006]
to **rely on balanced case**

Approximant bases: 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 **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 **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

size of **normalized** basis: $\mathcal{O}(mnd)$ **independently of the shift**

s-Popov basis: **aim** & **means**

Approximant bases: degree control via normalized basis

Degree control $\rightsquigarrow$ compute the **s**-Popov basis **P**

- **s**-Popov not compatible with **multiplication**
- size of product beyond target cost

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

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

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

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

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

Result: $\mathcal{O}(m^\omega \mathrm{M}(D/m) \log(D)^2) \subseteq \tilde{\mathcal{O}}(m^{\omega-1} D)$

- arbitrary shift **s**
- arbitrary orders
- returning **s**-Popov basis

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

$D := d_1 + \cdots + d_n$

Change of monomial order

$\rightsquigarrow$ polynomial system solving

$\prec_1$-GB of $\mathcal{M} \longrightarrow \prec_2$-GB of $\mathcal{M}$

Basis of relations

$\mathbf{pf} \equiv 0 \bmod \mathcal{M}$

knowing multiplication matrices

Hermite-Padé approximation

$\mathbf{pf} \equiv 0 \bmod X^D$

Multivariate interpolation

$\rightsquigarrow$ list-decoding algorithms

$p(x_i, y_i) = 0$ 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

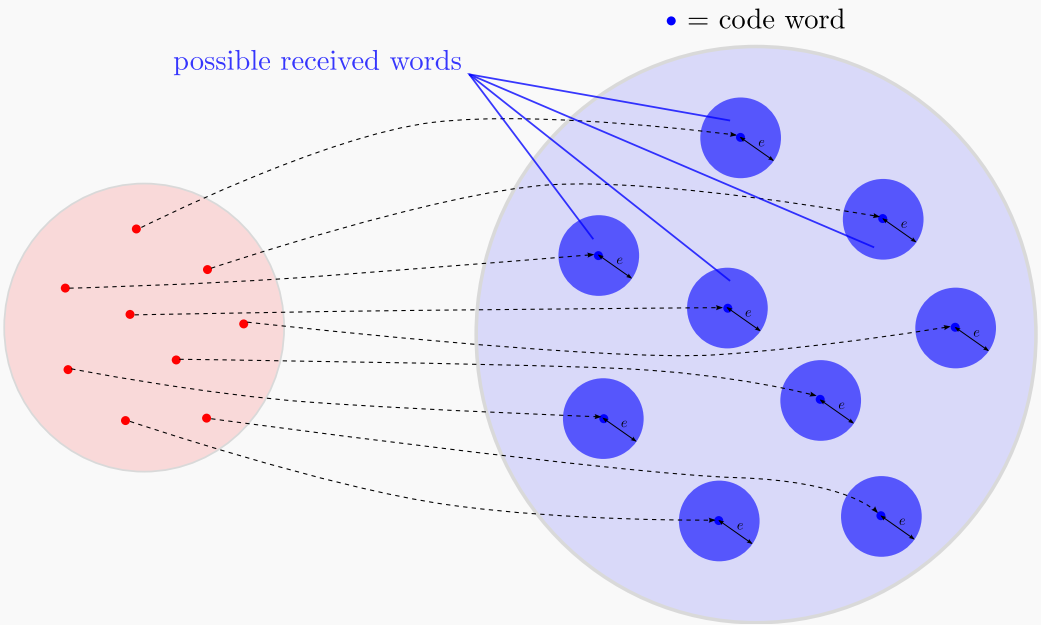
Reliable delivery of data over an unreliable communication channel

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

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

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

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



From bivariate interpolation to univariate relation

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:**

$$\text{relations modulo } \mathcal{M} = \begin{bmatrix} \mathfrak{m}_1 & & \\ & \ddots & \\ & & \mathfrak{m}_n \end{bmatrix}$$

- $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ split over $\mathbb{K}$
- roots and multiplicities are known

Interpolation: generalizing approximation techniques

Generalizations:

- update $\mathbf{g} := \mathbf{P}^{(1)}\mathbf{f} \bmod (\mathfrak{m}_1, \ldots, \mathfrak{m}_n) \rightsquigarrow$ fast via CRT
- divide and conquer via multiplication
- divide and conquer via "find & use degrees"

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

Fact: degree of output at most $\operatorname{lcm}(\mathfrak{m}_1, \ldots, \mathfrak{m}_n)$

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

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

Interpolation: controlling the degrees

No "balanced case", yet
known diagonal degrees $\Rightarrow$ almost uniform shift $\Rightarrow$ small output degrees

- 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 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: results

- arbitrary shift **s**
- arbitrary diagonal with known linear factors
- returning **s**-Popov basis

$$\mathbf{pf} = 0 \bmod \begin{bmatrix} \mathfrak{m}_1 & & \\ & \ddots & \\ & & \mathfrak{m}_n \end{bmatrix}$$

$$D := \deg(\mathfrak{m}_1) + \cdots + \deg(\mathfrak{m}_n)$$

Cost bound: $\mathcal{O}(m^{\omega-1}\mathsf{M}(D)\log(D)^3) \quad \subseteq \tilde{\mathcal{O}}(m^{\omega-1}D)$

Improves upon previous algorithms:

- iterative [Kötter, 1996+2003] [Nielsen–Høholdt, 1998]
- based on fast basis reduction [Cohn-Heninger, 2011+2012]

$\rightsquigarrow$ list- and soft-decoding of Reed-Solomon codes

$\rightsquigarrow$ robust Private Information Retrieval [Devet-Goldberg-Heninger, 2012]

Change of monomial order

$\rightsquigarrow$ polynomial system solving

$\prec_1$-GB of $\mathcal{M} \longrightarrow \prec_2$-GB of $\mathcal{M}$

Basis of relations

$\mathbf{pf} \;=\; 0 \bmod \mathcal{M}$

knowing multiplication matrices

Hermite-Padé approximation

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

Multivariate interpolation

$\rightsquigarrow$ list-decoding algorithms

$p(x_i, y_i) = 0$ 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

Problem: any basis **M** of $\mathcal{M} \longrightarrow$ **s**-Popov basis of $\mathcal{M}$

$=$ **s**-Popov basis of relations $\mathbf{p} \cdot \mathrm{Id} = 0 \bmod \mathbf{M}$

Input: $m \times m$ matrix
- of degree $\leqslant d \to$ size $m^2 d$
- of generic det. degree $\leqslant D_{\mathrm{gen}} \to$ size $m D_{\mathrm{gen}}$

Fast algorithm for arbitrary shifts?

Previous work:

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

$$\begin{bmatrix} p_1 & \cdots & p_m \end{bmatrix} \begin{bmatrix} f_{11} & \cdots & f_{1n} \\ & \vdots & \\ f_{m1} & \cdots & f_{mn} \end{bmatrix} = 0 \mod \begin{bmatrix} \mathfrak{m}_1 & & & \\ & \mathfrak{m}_2 & & \\ & & \ddots & \\ & & & \mathfrak{m}_n \end{bmatrix}$$

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

Normal forms via bases of relations

Compute the Smith form $\mathbf{U}\mathbf{M}\mathbf{V} = \mathrm{diag}(\mathfrak{m}_1, \ldots, \mathfrak{m}_n)$

$$\mathbf{p} \cdot \mathrm{Id} = 0 \bmod \mathbf{M} \iff \mathbf{p}\mathbf{V} = 0 \bmod \begin{bmatrix} \mathfrak{m}_1 & & \\ & \ddots & \\ & & \mathfrak{m}_n \end{bmatrix}$$

cost: $\tilde{\mathcal{O}}(m^{\omega-1} D_{\mathrm{gen}})$ Las Vegas [Storjohann, 2003] [Gupta et al., 2012]

$\rightsquigarrow$ it remains to compute the **s**-Popov basis of relations

generalization of approximants/interpolants:
$\mathcal{M}$ = **arbitrary diagonal matrix** (unknown roots, if any)

generalizing divide and conquer "find & use degrees"
$\Rightarrow$ remains one equation (**f** column vector)

$\mathbf{p}\,\mathbf{f} = 0 \bmod \mathfrak{m}$

arbitrary $\mathfrak{m}$: how to divide and conquer?

Basis of relations for an arbitrary diagonal matrix

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

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

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

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

$$\begin{bmatrix}\mathbf{P}^{(1)} & \mathbf{0} & \mathbf{q}^{(1)}\\ * & \mathbf{P}^{(2)} & \mathbf{q}^{(2)}\\ * & * & *\end{bmatrix}\begin{bmatrix}\mathbf{f}^{(1)}\\ \mathbf{f}^{(2)}\\ \mathfrak{m}\end{bmatrix}$$

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

- arbitrary shift **s**
- arbitrary diagonal
- returning **s**-Popov basis

$$\mathbf{p}\mathbf{f} = 0 \bmod \begin{bmatrix}\mathfrak{m}_1 & & \\ & \ddots & \\ & & \mathfrak{m}_n\end{bmatrix}$$

assumption $n \in \mathcal{O}(m)$

Summary and perspectives

Results:

	cost bound	i/o size
· $\prec$-Gröbner basis of relations · change of monomial order	$\tilde{\mathcal{O}}(rD^\omega)$	rD^2
· **s**-Popov basis of relations · normal form of $\mathbb{K}[X]$ matrix	$\tilde{\mathcal{O}}(m^{\omega-1}D)$	mD

Perspectives and open questions:

- implementation in Linbox (C++)
- fast **s**-Popov kernel basis
- deterministic Smith form
- deterministic characteristic polynomial in $\mathcal{O}(m^\omega)$
- unconditional fast change of monomial order
- exploiting double structure in bivariate interpolation