Fast computation of interpolation bases in Popov form for arbitrary shifts

Vincent Neiger [§,†,‡]

Claude-Pierre Jeannerod[§] Éric Schost[†] Gilles Villard[§]

[§]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 22, 2016

Approximation and Interpolation

Padé-like approximation

Input: $\mathbf{F} = (f_1, \ldots, f_m)$ polynomials over $\mathbb{K}$, order σ points $x_1, \ldots, x_\sigma$
Find $\mathbf{p} = (p_1, \ldots, p_m)$ polynomials such that

$$\begin{cases} p_1 f_1 + \cdots + p_m f_m \ = \ 0 \mod X^\sigma & \mod \prod_{1 \leqslant i \leqslant \sigma} (X - x_i) \\ \text{minimal } \deg(\mathbf{p}) \end{cases}$$

Approximation and Interpolation

Padé-like approximation

Input: $\mathbf{F} = (f_1, \ldots, f_m)$ polynomials over $\mathbb{K}$, order σ points $x_1, \ldots, x_\sigma$
Find $\mathbf{p} = (p_1, \ldots, p_m)$ polynomials such that

$$\begin{cases} p_1 f_1 + \cdots + p_m f_m \ = \ 0 \mod X^\sigma & \mod \prod_{1 \leqslant i \leqslant \sigma} (X - x_i) \\ \text{minimal } \deg(\mathbf{p}) \end{cases}$$

Guruswami-Sudan list-decoding

Input: points $\{(x_i, y_i)\}_{1 \leqslant i \leqslant \sigma}$ in $\mathbb{K}^2$
Find $Q(X, Y) = Q_0 + Q_1 Y + \cdots + Q_{m-1} Y^{m-1}$ such that

- $Q(x_i, y_i) = 0$ for all i
- minimal $\deg_X(Q)$

Why would one care?

Central problem:

- Hermite-Padé approximants
  $\rightsquigarrow$ guessing linear differential equations

- order basis
  $\rightsquigarrow$ simultaneous Padé approximants [Nielsen-Storjohann, 2016]
  $\rightsquigarrow$ computation of normal forms [Neiger, 2016]
  $\rightsquigarrow$ kernel bases [Zhou-Labahn-Storjohann, 2012]

- list-decoding algorithms
  $\rightsquigarrow$ Reed-Solomon codes [Guruswami-Sudan, 1998]
  $\rightsquigarrow$ folded Reed-Solomon codes [Guruswami-Rudra, 2006]
  $\rightsquigarrow$ robust Private Information Retrieval [Devet-Goldberg-Heninger, 2012]

Example

Hermite-Padé approximation: $p_1 f_1 + \cdots + p_m f_m = 0 \mod X^\sigma$

Example with $m = 4, \sigma = 128$

$$\mathbf{f} = \begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 + X \\ X + X^2 \\ X^2 + X^3 \end{bmatrix}$$

basis of solutions:

$$\mathbf{P} = \begin{bmatrix} X+1 & -1 & & \\ X-1 & X+1 & -1 & \\ X+1 & X-1 & X+1 & -1 \\ X^{125} & X^{125} & -X^{125} & X^{125} \end{bmatrix}$$

with minimal row degrees

General interpolation problem

Several equations

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

where $M_1, \ldots, M_n$ are known through roots and multiplicities

interpolation basis = basis of the module of interpolants

$$\left\{ \mathbf{p} = (p_1, \ldots, p_m) \in \mathbb{K}[X]^m \quad | \quad \mathbf{pF} = 0 \bmod \mathbf{M} \right\}$$

Specific case of vector rational interpolation [Beckermann - Labahn, 2000]

Problem

Input: roots and multiplicities of 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 interpolation basis

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

1. minimal interpolation bases
2. global picture of existing algorithms
3. fast algorithm

Minimal interpolation bases

interpolation basis: nonsingular matrix $\mathbf{P} = \begin{bmatrix} p_{11} & \cdots & p_{1m} \\ & \vdots & \\ p_{m1} & \cdots & p_{mm} \end{bmatrix}$

s-minimal basis **P**: minimal **s**-row degrees

Shift: integers $\mathbf{s} = (s_1, \ldots, s_m)$ used as additive degree weights

$$\deg_{\mathbf{s}}(\begin{bmatrix} p_1 & \cdots & p_m \end{bmatrix}) = \max_j(\deg(p_j) + s_j)$$

Shifts can serve as degree constraints:

$$\deg(p_j) < N_j \text{ for all } j \quad \Leftrightarrow \quad \deg_{(-N_1,\ldots,-N_m)}(\mathbf{p}) < 0$$

Basis in normal form

s-Popov basis $=$ **s**-minimal $+$ column normalized

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

$\rightsquigarrow$ many useful properties

[Nielsen-Storjohann, ISSAC 2016]

Average degrees

$\tilde{\mathcal{O}}(m^\omega \sigma / m)$

[Jeannerod-Neiger-Schost-Villard, 2015]

[Storjohann, 2006]
[Zhou-Labahn, 2012]

assumptions on the shift

[Giorgi-Jeannerod-Villard, 2003]

$\tilde{\mathcal{O}}(m^\omega \sigma / n)$

Matrix multiplication

$\tilde{\mathcal{O}}(m^\omega \sigma)$

[Beckermann-Labahn, 1994]

Structure

$\mathcal{O}(m^2 \sigma^2)$

[Van Barel-Bultheel, 1992]
[Kötter-Nielsen-Høholdt, 1999]
[Beckermann-Labahn, 2000]

[Sergeyev, 1987]
[Paszkowski, 1987]
[Van Barel-Bultheel, 1991]

Dense linear algebra

[Jeannerod-Neiger-Schost-Villard, 2015] $\tilde{\mathcal{O}}(\sigma^\omega)$ with arbitrary shift Popov basis

Here: $\tilde{\mathcal{O}}(m^\omega \sigma/m)$ with arbitrary shift, Popov basis

↑

Average degrees

$\tilde{\mathcal{O}}(m^\omega \sigma/m)$

assumptions on the shift

[Jeannerod-Neiger-Schost-Villard, 2015]

[Storjohann, 2006]
[Zhou-Labahn, 2012]

[Giorgi-Jeannerod-Villard, 2003]
$\tilde{\mathcal{O}}(m^\omega \sigma/n)$

↑

Matrix multiplication

$\tilde{\mathcal{O}}(m^\omega \sigma)$

[Beckermann-Labahn, 1994]

↑

Structure

$\mathcal{O}(m^2\sigma^2)$

[Van Barel-Bultheel, 1992]
[Kötter-Nielsen-Høholdt, 1999]
[Beckermann-Labahn, 2000]

[Sergeyev, 1987]
[Paszkowski, 1987]
[Van Barel-Bultheel, 1991]

↑

Dense linear algebra

[Jeannerod-Neiger-Schost-Villard, 2015] $\tilde{\mathcal{O}}(\sigma^\omega)$ with arbitrary shift, Popov basis

Divide-and-conquer algorithm

Relying on fast polynomial matrix multiplication
(generalizing [Beckermann-Labahn, 1994] from Hermite-Padé to interpolation)

- $\mathbf{P}^{(1)} \leftarrow$ **s**-minimal for first $\sigma/2$ constraints and $\mathbf{F}$
- $\mathbf{G} \leftarrow$ update $\mathbf{F}$, $\mathbf{t} \leftarrow$ update **s**
- $\mathbf{P}^{(2)} \leftarrow$ **t**-minimal for last $\sigma/2$ constraints and $\mathbf{G}$
- return $\mathbf{P} = \mathbf{P}^{(2)}\mathbf{P}^{(1)}$

$\rightsquigarrow$ $\mathbf{P}$ is a **s**-minimal interpolation basis

$\deg(\mathbf{P}^{(1,2)}) \leqslant \sigma/2 \;\Rightarrow\; \deg(\mathbf{P}) \leqslant \sigma \quad \rightsquigarrow \quad$ Cost bound $\mathcal{O}^{\sim}(m^{\omega}\sigma)$

How to obtain $\mathcal{O}^{\sim}(m^{\omega}\sigma/m)$? ... why is it even feasible?

Overview

1. why feasible? $\rightsquigarrow$ **s**-Popov basis
2. solution when diagonal degrees are known
3. how to find diagonal degrees recursively

- $\mathbf{P}^{(1)} \leftarrow$ **s**-Popov
- ...
- $\mathbf{P}^{(2)} \leftarrow$ **t**-Popov
- return $\mathbf{P} = \mathbf{P}^{(2)}\mathbf{P}^{(1)}$

Too large output (1/2)

Hermite-Padé approximation with $m = 4, \sigma = 128$, $\mathbf{s = 0}$

$$\mathbf{F} = \begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 + X \\ X + X^2 \\ X^2 + X^3 \end{bmatrix},$$

0-minimal basis:

$$\begin{bmatrix} X+1 & -1 & & \\ X-1 & X+1 & -1 & \\ X+1 & X-1 & X+1 & -1 \\ X^{125} & X^{125} & -X^{125} & X^{125} \end{bmatrix}$$

- unbalanced row degrees $(1, 1, 1, 125)$
- average row degrees $= \sigma/m \ldots$ because $\mathbf{s = 0}$

Too large output (2/2)

Extend this to $m = 8, \sigma = 128$, $\mathbf{s} = (0, 0, 0, 0, \sigma, \sigma, \sigma, \sigma)$

with $\mathbf{F}$: same f_1, f_2, f_3, f_4 / random f_5, f_6, f_7, f_8

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

- some $\mathbf{s}$-minimal basis
- size $\Theta(m^2\sigma)$
- beyond target $\tilde{\mathcal{O}}(m^\omega\sigma/m)$

Too large output (2/2)

Extend this to $m = 8, \sigma = 128$, $\mathbf{s} = (0, 0, 0, 0, \sigma, \sigma, \sigma, \sigma)$

with $\mathbf{F}$: same f_1, f_2, f_3, f_4 / random f_5, f_6, f_7, f_8

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

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

- some **s**-minimal basis
- size $\Theta(m^2\sigma)$
- beyond target $\tilde{\mathcal{O}}(m^\omega\sigma/m)$

- the **s**-Popov basis
- diagonal entries dominant
- average column degree σ/m

When diagonal degrees are known

Input: $\mathbf{F}$, $\mathbf{s}$, and $\mathbf{d} = (d_1, \ldots, d_m)$ the diagonal degrees of $\mathbf{P}$

Central fact: $\mathbf{P}$ is also the $-\mathbf{d}$-Popov basis

Algorithm:

Step 1. $\mathbf{B} \leftarrow$ some $-\mathbf{d}$-minimal basis for $\mathbf{F}$

partial linearization [Storjohann, 2006] + small shifts algorithm

Step 2. $\mathbf{P} \leftarrow$ normalize $\mathbf{B}$ into $-\mathbf{d}$-Popov form

$\mathbf{d} = (1, 1, 1, 125, 0, 0, 0, 0)$

$$\mathbf{B} = \begin{bmatrix} 1 & 0 & & & & & & \\ 1 & 1 & 0 & & & & & \\ 1 & 1 & 1 & 0 & & & & \\ 1 & 1 & 1 & 125 & & & & \\ 0 & 0 & 0 & 124 & 0 & & & \\ 0 & 0 & 0 & 124 & & 0 & & \\ 0 & 0 & 0 & 124 & & & 0 & \\ 0 & 0 & 0 & 124 & & & & 0 \end{bmatrix} \quad \text{or} \quad \mathbf{B} = \begin{bmatrix} 1 & 1 & 1 & 125 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 125 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 125 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 125 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 125 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 125 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 125 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 125 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Finding diagonal degrees recursively

- If $\sigma \leqslant m$: compute $\mathbf{P}$ by dense linear algebra
- Else:
  - $\mathbf{P}^{(1)} \leftarrow$ **s**-Popov for first $\sigma/2$ constraints and $\mathbf{F}$
  - $\mathbf{G} \leftarrow$ update $\mathbf{F}$, $\mathbf{t} \leftarrow$ update **s**
  - $\mathbf{P}^{(2)} \leftarrow$ **t**-Popov for last $\sigma/2$ constraints and $\mathbf{G}$
  - Find the diagonal degrees **d** of $\mathbf{P}$
  - $\mathbf{B} \leftarrow -\mathbf{d}$-minimal for all σ constraints and $\mathbf{F}$
  - Return $\mathbf{P} = \mathrm{lm}_{-\mathbf{d}}(\mathbf{B})^{-1}\mathbf{B}$

cost bound: $\mathcal{O}(m^{\omega-1}\mathrm{M}(\sigma)\log(\sigma)\log(\sigma/m)^2)$

Finding diagonal degrees recursively

- If $\sigma \leqslant m$: compute $\mathbf{P}$ by dense linear algebra
- Else:
  - $\mathbf{P}^{(1)} \leftarrow$ **s**-Popov for first $\sigma/2$ constraints and $\mathbf{F}$
  - $\mathbf{G} \leftarrow$ update $\mathbf{F}$, $\mathbf{t} \leftarrow$ update **s**
  - $\mathbf{P}^{(2)} \leftarrow$ **t**-Popov for last $\sigma/2$ constraints and $\mathbf{G}$
  - Find the diagonal degrees $\mathbf{d}$ of $\mathbf{P}$
  - $\mathbf{B} \leftarrow -\mathbf{d}$-minimal for all σ constraints and $\mathbf{F}$
  - Return $\mathbf{P} = \mathrm{lm}_{-\mathbf{d}}(\mathbf{B})^{-1}\mathbf{B}$

Product $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$

- not in **s**-Popov form, degrees too large for efficient computation
- $\mathbf{P}$ is its **s**-Popov form

cost bound: $\mathcal{O}(m^{\omega-1}\mathrm{M}(\sigma)\log(\sigma)\log(\sigma/m)^2)$

Finding diagonal degrees recursively

- If $\sigma \leqslant m$: compute $\mathbf{P}$ by dense linear algebra
- Else:
  - $\mathbf{P}^{(1)} \leftarrow$ **s**-Popov for first $\sigma/2$ constraints and $\mathbf{F}$
  - $\mathbf{G} \leftarrow$ update $\mathbf{F}$, $\mathbf{t} \leftarrow$ update **s**
  - $\mathbf{P}^{(2)} \leftarrow$ **t**-Popov for last $\sigma/2$ constraints and $\mathbf{G}$
  - Find the diagonal degrees $\mathbf{d}$ of $\mathbf{P}$
  - $\mathbf{B} \leftarrow -\mathbf{d}$-minimal for all σ constraints and $\mathbf{F}$
  - Return $\mathbf{P} = \mathrm{lm}_{-\mathbf{d}}(\mathbf{B})^{-1}\mathbf{B}$

Product $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$

- not in **s**-Popov form, degrees too large for efficient computation
- $\mathbf{P}$ is its **s**-Popov form

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

cost bound: $\mathcal{O}(m^{\omega-1}\mathrm{M}(\sigma)\log(\sigma)\log(\sigma/m)^2)$

Here: $\tilde{\mathcal{O}}(m^\omega \sigma / m)$ with arbitrary shift, Popov normal form

↑

Average degrees

$\tilde{\mathcal{O}}(m^\omega \sigma / m)$

assumptions on the shift

[Jeannerod-Neiger-Schost-Villard, 2015]

[Storjohann, 2006]
[Zhou-Labahn, 2012]

[Giorgi-Jeannerod-Villard, 2003]
$\tilde{\mathcal{O}}(m^\omega \sigma / n)$

↑

Matrix multiplication

$\tilde{\mathcal{O}}(m^\omega \sigma)$

[Beckermann-Labahn, 1994]

↑

Structure

$\mathcal{O}(m^2 \sigma^2)$

[Van Barel-Bultheel, 1992]
[Kötter-Nielsen-Høholdt, 1999]
[Beckermann-Labahn, 2000]

[Sergeyev, 1987]
[Paszkowski, 1987]
[Van Barel-Bultheel, 1991]

↑

Dense linear algebra

[Jeannerod-Neiger-Schost-Villard, 2015] $\tilde{\mathcal{O}}(\sigma^\omega)$ with arbitrary shift, Popov basis

List-decoding: Sudan algorithm

given σ points $\{(x_1, y_1), \ldots, (x_\sigma, y_\sigma)\}$

f solution: $\deg f \leqslant k$ and $f(x_i) = y_i$ for $\geqslant \sigma - e$ points

[Sudan, 1997]

- Compute degree constraints m and b
- Interpolation step
  compute $Q(X, Y) = Q_0 + Q_1 Y + \cdots + Q_m Y^m$ such that
  - $Q_0, \ldots, Q_m$ have small shifted degree: $\deg Q_j < b - jk$
  - $Q(x_i, y_i) = 0$ for all points
- Root-finding step
  the solutions f are among the Y-roots of $Q(X, Y)$

Interpolation steps in related contexts

[Guruswami - Sudan, 1999]
List-decoding of Reed-Solomon codes,
further extends the error-correction bound

Compute $Q(X, Y) = Q_0 + Q_1 Y + \cdots + Q_m Y^m$ such that

- $Q_0, \ldots, Q_m$ have small shifted degree
- $Q(x_i, y_i) = 0$ with multiplicity μ for all points

Interpolation steps in related contexts

[Kötter - Vardy, 2003]
Soft-decision decoding of Reed-Solomon codes

$x_1, \ldots, x_n$ are not pairwise distinct
Compute $Q(X, Y) = Q_0 + Q_1 Y + \cdots + Q_m Y^m$ such that

- $Q_0, \ldots, Q_m$ have small shifted degree
- $Q(x_i, y_i) = 0$ with multiplicity μ_i for all points

Interpolation steps in related contexts

[Guruswami - Rudra, 2006]
List-decoding of folded Reed-Solomon codes:
extends the error-correction bound up to the information-theoretic limit

[Devet - Goldberg - Heninger, 2012]
Optimally robust Private Information Retrieval

Compute $Q(X, Y_1, \ldots, Y_s) = \sum_{(j_1,\ldots,j_s)\in\Gamma} Q_{j_1,\ldots,j_s} Y_1^{j_1} \cdots Y_s^{j_s}$ such that

- the $Q_{(j_1,\ldots,j_s)}$ have small shifted degree
- $Q(x_i, y_{i1}, \ldots, y_{is}) = 0$ with multiplicity μ for all points

Ingredient 3: linearizing at small orders (1/3)

Base case $\sigma = m$, goal $\tilde{\mathcal{O}}(m^\omega)$

Input: points $x_1, \ldots, x_m$, evaluation matrix $\mathbf{E} \in \mathbb{K}^{m \times m}$

Output: $\mathbf{0}$-minimal interpolation basis $\mathbf{P}$

sum of row degrees $\leqslant m \Rightarrow$ average degree in the matrix $\leqslant 1$

Complete linearization over $\mathbb{K}$

$$\mathcal{K} = \begin{bmatrix} \mathbf{E} \\ \mathbf{ED} \\ \mathbf{ED^2} \\ \vdots \\ \mathbf{ED^M} \end{bmatrix} \qquad \text{where} \quad \mathbf{D} = \mathrm{Diag}(x_1, \ldots, x_m)$$

minimal interpolation basis $\longleftrightarrow$ minimal linear relations between rows of $\mathcal{K}$

Fast computation of those relations, in $\mathcal{O}(m^\omega \log m)$

Iterative algorithm [Van Barel-Bultheel / Beckermann-Labahn / Kötter]

1. $\mathbf{P} = \begin{bmatrix} -\mathbf{p}_1- \\ \vdots \\ -\mathbf{p}_m- \end{bmatrix} = \text{Identity in } \mathbb{K}[X]^{m\times m}$

2. *For i from 1 to σ:*

a. Compute evaluations $\begin{bmatrix} (\mathbf{p}_1 \cdot \mathbf{f})(x_i) \\ \vdots \\ (\mathbf{p}_m \cdot \mathbf{f})(x_i) \end{bmatrix} = (\mathbf{P} \cdot \mathbf{f})(x_i)$

b. Choose pivot π with smallest s_π such that $(\mathbf{p}_\pi \cdot \mathbf{f})(x_i) \neq 0$
Update pivot shift $s_\pi = s_\pi + 1$

c. Eliminate:

For $j \neq \pi$ do $\mathbf{p}_j = \mathbf{p}_j - \dfrac{(\mathbf{p}_j \cdot \mathbf{f})(x_i)}{(\mathbf{p}_\pi \cdot \mathbf{f})(x_i)}\mathbf{p}_\pi$ /* $\forall j \neq \pi,\ (\mathbf{p}_j \cdot \mathbf{f})(x_i) = 0$ */

$\mathbf{p}_\pi = (X - x_i)\mathbf{p}_\pi$ /* $(\mathbf{p}_\pi \cdot \mathbf{f})(x_i) = 0$ */

After i iterations: $\mathbf{P}$ MIB of for $(x_1, \ldots, x_i)$