Block Sparse-FGLM

Kevin Hyun Vincent Neiger Hamid Rahkooy Éric Schost

September 25, 2018

Introduction

Given:

$$I \subset \mathbb{K}[x_1, \ldots, x_n]\text{: zero dimensional ideal}$$
$$\mathcal{B}\text{: monomial basis of } \mathbb{K}[x_1, \ldots, x_n]/I$$
$$M_1, \ldots, M_n\text{: multiplication matrices for } x_1, \ldots, x_n \text{ resp.}$$
$$D : \text{vector space dimension of } \mathbb{K}[x_1, \ldots, x_n]/I$$

Find the Gröbner basis wrt lexicographical ordering (change of ordering)

Introduction

Given:

$$I \subset \mathbb{K}[x_1, \ldots, x_n]\text{: zero dimensional ideal}$$
$$\mathcal{B}\text{: monomial basis of } \mathbb{K}[x_1, \ldots, x_n]/I$$
$$M_1, \ldots, M_n\text{: multiplication matrices for } x_1, \ldots, x_n \text{ resp.}$$
$$D \text{ : vector space dimension of } \mathbb{K}[x_1, \ldots, x_n]/I$$

Find the Gröbner basis wrt lexicographical ordering (change of ordering)
More precisely, find univariate polynomials $P_1, \ldots, P_n$ st:

$$\{x_1 - P_1(x_n), x_2 - P_2(x_n), \ldots, P_n(x_n)\}$$

where

$$V(I) = \{(P_1(\tau), P_2(\tau), \ldots, \tau) \mid P_n(\tau) = 0\}$$

Example

Given, in $GF(97)$

$$I = \langle -27x_2^2 - 28x_2x_1 - 45x_1^2 - 44x_2 - 12x_1 + 16, \\ -20x_2^2 + 39x_2x_1 + 13x_1^2 - 35x_2 - 17x_1 + 6\rangle$$

$$\mathcal{B} = \{x_1^2, x_1, x_2, 1\}, D = 4,$$

$$M_1 = \begin{bmatrix} 27 & 59 & 9 & 0 \\ 57 & 2 & 37 & 0 \\ 91 & 44 & 21 & 1 \\ 23 & 1 & 75 & 0 \end{bmatrix}, M_2 = \begin{bmatrix} 60 & 1 & 59 & 0 \\ 57 & 0 & 2 & 1 \\ 46 & 0 & 44 & 0 \\ 95 & 0 & 1 & 0 \end{bmatrix}$$

Want

$$\{x_1 - (86x_2^3 + 49x_2^2 + 39x_2 + 38), x_2^4 + 47x_2^3 + 16x_2^2 + 64x_2 + 16\}$$

$V(I)$ has one point in $GF(97)$: $(35, 88)$

Sparse-FGLM

- Faugère and Mou [2017]
- Key idea: min. poly of M_n equals P_n
- M_i's expected to be sparse: use the Wiedemann algorithm

Wiedemann Algorithm

- Solves linear system $Mx = b$, $M \in \mathbb{K}^{D \times D}$
- able to exploit the sparsity of A
- Key idea: for $u, v \in \mathbb{K}^{D \times 1}$ random, minimal polynomial generator $P = \sum_{i=0}^{D} p_i T^i$ of $(uA^i v^t)_{i \geq 0}$ is also the minimal polynomial of A

Wiedemann Algorithm

- Solves linear system $Mx = b$, $M \in \mathbb{K}^{D \times D}$
- able to exploit the sparsity of A
- Key idea: for $u, v \in \mathbb{K}^{D \times 1}$ random, minimal polynomial generator $P = \sum_{i=0}^{D} p_i T^i$ of $(uA^i v^t)_{i \geq 0}$ is also the minimal polynomial of A

Definition (Minimal Polynomial Generator)

Minimal polynomial generator $P = p_0 + p_1 T + \cdots + p_d T^D$ of a (linearly recurrent) sequence $(L_s)_{s \geq 0}$ is the monic polynomial of lowest degree st

$$p_0 L_s + p_1 L_{s+1} + \cdots + p_D L_{s+D} = 0, \ \forall s \geq 0$$

Equivalently, $P \sum_{s \geq 0} L_s / T^{s+1}$ is a polynomial.

In other words:

$$\sum_{i=0}^{d} p_i u M^{s+i} v^t = 0 \iff \sum_{i=0}^{d} p_i M^{s+i} = 0$$

Sparse-FGLM

Let $e = \begin{bmatrix} 1 & 0 & \dots & 0 \end{bmatrix}^t$
Given $M_1, \dots, M_n$ and D as before:

1. Choose $u \in \mathbb{K}^{1 \times D}$ of random entries
2. Compute $L_s = uM_n^s e$ for $s = 0, \dots, 2D$
3. Let P be the minimal polynomial generator of $(L_s)_{0 \leq s \leq 2D}$
4. Let $N = P \sum_{s \geq 0} L_s / T^{s+1}$
5. for $i = 1 \dots n - 1$:
   - 5a. Compute $N_i = P \sum_{s \geq 0} (uM_n^s M_i e) / T^{s+1}$
   - 5b. Let $C_i = N_i / N \mod P$
6. Return $\{x_1 - C_1, x_2 - C_2, \dots, P\}$

- Randomized; may lose some points

Example cont.

Given previous input:

- Choose $u = \begin{bmatrix} 3 & 11 & 1 & 2 \end{bmatrix}$
- $(uM_2^s e)_{0 \leq i < 2D} = (3, 69, 96, 94, 58, 65, 8, 61)$,
  with minimum polynomial generator:
  $P = T^4 + 47T^3 + 16T^2 + 64T + 16$

Example cont.

Given previous input:

- Choose $u = \begin{bmatrix} 3 & 11 & 1 & 2 \end{bmatrix}$
- $(uM_2^s e)_{0 \le i < 2D} = (3, 69, 96, 94, 58, 65, 8, 61)$,
  with minimum polynomial generator:
  $P = T^4 + 47T^3 + 16T^2 + 64T + 16$
- $N = P(3/T + 69/T^2 + 96/T^3 + \dots) = 3T^3 + 16T^2 + 89T + 82$
- $N_1 = P(7/T + 1/T^2 + 5/T^3 + \dots) = 73T^3 + 88T^2 + 55T + 31$

Example cont.

Given previous input:

- Choose $u = \begin{bmatrix} 3 & 11 & 1 & 2 \end{bmatrix}$
- $(uM_2^s e)_{0 \le i < 2D} = (3, 69, 96, 94, 58, 65, 8, 61)$, with minimum polynomial generator: $P = T^4 + 47T^3 + 16T^2 + 64T + 16$
- $N = P(3/T + 69/T^2 + 96/T^3 + \dots) = 3T^3 + 16T^2 + 89T + 82$
- $N_1 = P(7/T + 1/T^2 + 5/T^3 + \dots) = 73T^3 + 88T^2 + 55T + 31$
- Finally $N_1/N \mod P = 86T^3 + 49T^2 + 39T + 38$

Recall, lex basis of I:

$$\{x_1 - (86x_2^3 + 49x_2^2 + 39x_2 + 38), x_2^4 + 47x_2^3 + 16x_2^2 + 64x_2 + 16\}$$

Closer Look

- Berlekamp-Massey algorithm finds the minimal polynomial
- Bottleneck: computing $(uM_n^s)_{0\leq s<2D}$
- difficult to parallelize: need uM_n^s to compute uM_n^{s+1}
- Use block Wiedemann algorithm instead!

For "bad" inputs:

- Uses Berlekamp-Massey-Sakata algorithm for non radical/shape position ideals

Block Sparse-FGLM

Three goals:

1. Easily parallelizable
2. Deal with non radical/shape position ideals without using Berlekamp-Massey-Sakata
3. Avoid using generic linear forms $x = t_1 x_1 + \cdots + t_n x_n$ as much as possible

Block Sparse-FGLM

Three goals:

1. Easily parallelizable
2. Deal with non radical/shape position ideals without using Berlekamp-Massey-Sakata
3. Avoid using generic linear forms $x = t_1 x_1 + \cdots + t_n x_n$ as much as possible

Additionally,

- Steel [2015] already showed how to compute $P_n(x_n)$ through the block Wiedemann algorithm
- Computed the rest through "evaluation" method
- Want to compute the rest algebraically

Block Wiedemann Algorithm

- Coppersmith [1994], Kaltofen [1995], Villard [1997], Kaltofen and Villard [2001]
- Compute matrix sequences rather than scalar
- Choose $m \in \mathbb{N}$ and $U, V \in \mathbb{K}^{m \times D}$ of random entries
- Compute (in parallel), for $1 \leq s < 2D/m$,

$$\begin{aligned} L_{s,1} &= u_1 M^s \\ L_{s,2} &= u_2 M^s \\ &\vdots \\ L_{s,m} &= u_m M^s \end{aligned}$$

  and

$$A_s = L_s V^t, 0 \leq s < 2D/m$$

- Exists a notion of **minimal polynomial matrix generator**

Minimal Polynomial Matrix Generator

Let $F = \sum_{i=0}^{\lceil D/m \rceil} F_i T^i$, where $F_i \in \mathbb{K}^{m \times m}$, be the minimal polynomial matrix generator of $(A_s)_{s \geq 0}$

- $\sum_{i=0}^{\lceil D/m \rceil} F_i A_{s+i} = 0$ for any $s \geq 0$
- $F \sum_{s \geq 0} A_s / T^{s+1}$ has polynomial entries
- Expected to have degree at most $\lceil D/m \rceil$
- Berlekamp-Massey, Extended Euclidean, Padé approximant, σ-basis, Toeplitz/Hankel solver

Computing Scalar Quantities

- Given block quantities, want corresponding scalar quantities
- Largest invariant factor of $F =$ minimal polynomial generator P
- Compute by:
  - Smith Normal Form
  - LCM of denominators of y that satisfy $Fy = b$, for random b
- Find a that satisfy $aF = \begin{bmatrix} 0 & \dots & 0 & P \end{bmatrix}$ by linear system solving
- $N = aF \sum_{s \geq 0} UM^s e / T^{s+1}$ corresponds to scalar numerator $N = P \sum_{s \geq 0} u_n M^s e / T^{s+1}$

"Bad" Inputs

- Need x_n to **separate** all points in $V(I)$
- Choose $x = t_1x_1 + \cdots + t_nx_n$ with multiplication matrix M
- Compute output weaker than lex basis of I [Bostan et al, 2003]

Definition (Zero-dimensional Parametrization)

The tuple $((Q, V_1, \ldots, V_n), x)$, where Q is a monic square-free polynomial and V_i's are polynomials of degree less than Q, such that

$$V(I) = \{(V_1(\tau), \ldots, V_n(\tau)) \mid Q(\tau) = 0\}$$

- Similar to computing the lex basis for the radical of I

Block Sparse-FGLM

Given $M, M_1, \ldots, M_n$, D as before:

1. choose $U, V \in \mathbb{K}^{m \times D}$
2. $A_s = UM^sV^t$ for $0 \leq s < 2d$, with $d = \frac{D}{m}$
3. $F = \text{MatrixBerlekampMassey}((A_s)_{0 \leq s < 2d})$
4. $P =$ largest invariant factor of F and $R = \text{SquareFreePart}(P)$
5. $N = F \sum_{s \geq 0} \frac{UM^se}{T^{i+1}}$
6. $a = [0 \ \cdots 0P]F^{-1}$
7. $N^* =$ first entry of aN
8. for $j = 1 \ldots n$:
   - **8.1.** $N_j = F \sum_{i \geq 0} \frac{(UM^iM_je)}{T^{i+1}}$
   - **8.2.** $N_j^* =$ first entry of aN_j
   - **8.3.** $R_j = N_j^*/N^* \bmod R$
9. return $((R, R_1, \ldots, R_n), x)$

Example cont.

- Choose $m = 2$, $U = \begin{bmatrix} 95 & 78 & 40 & 77 \\ 21 & 0 & 84 & 2 \end{bmatrix}$, $V^t = \begin{bmatrix} 84 & 55 & 12 & 33 \\ 43 & 27 & 81 & 50 \end{bmatrix}$
- $(UM_2^s V^t)_{0 \le s < 4} = \left(\begin{bmatrix} 62 & 89 \\ 25 & 47 \end{bmatrix}, \begin{bmatrix} 10 & 95 \\ 45 & 92 \end{bmatrix}, \begin{bmatrix} 61 & 93 \\ 32 & 50 \end{bmatrix}, \begin{bmatrix} 22 & 49 \\ 5 & 13 \end{bmatrix} \right)$

Example cont.

- Choose $m = 2$, $U = \begin{bmatrix} 95 & 78 & 40 & 77 \\ 21 & 0 & 84 & 2 \end{bmatrix}$, $V^t = \begin{bmatrix} 84 & 55 & 12 & 33 \\ 43 & 27 & 81 & 50 \end{bmatrix}$
- $(UM_2^s V^t)_{0 \leq s < 4} = \left(\begin{bmatrix} 62 & 89 \\ 25 & 47 \end{bmatrix}, \begin{bmatrix} 10 & 95 \\ 45 & 92 \end{bmatrix}, \begin{bmatrix} 61 & 93 \\ 32 & 50 \end{bmatrix}, \begin{bmatrix} 22 & 49 \\ 5 & 13 \end{bmatrix} \right)$
- $F = \begin{bmatrix} T^2 + 19T + 17 & 41T + 68 \\ 18T + 61 & T^2 + 28T + 11 \end{bmatrix}$
  and $P = T^4 + 47T^3 + 16T^2 + 64T + 16$
  and $a = \begin{bmatrix} 36 + 79T & 17 + 19T + T^2 \end{bmatrix}$

Example cont.

- Choose $m = 2$, $U = \begin{bmatrix} 95 & 78 & 40 & 77 \\ 21 & 0 & 84 & 2 \end{bmatrix}$, $V^t = \begin{bmatrix} 84 & 55 & 12 & 33 \\ 43 & 27 & 81 & 50 \end{bmatrix}$
- $(UM_2^s V^t)_{0 \leq s < 4} = \left(\begin{bmatrix} 62 & 89 \\ 25 & 47 \end{bmatrix}, \begin{bmatrix} 10 & 95 \\ 45 & 92 \end{bmatrix}, \begin{bmatrix} 61 & 93 \\ 32 & 50 \end{bmatrix}, \begin{bmatrix} 22 & 49 \\ 5 & 13 \end{bmatrix} \right)$
- $F = \begin{bmatrix} T^2 + 19T + 17 & 41T + 68 \\ 18T + 61 & T^2 + 28T + 11 \end{bmatrix}$
  and $P = T^4 + 47T^3 + 16T^2 + 64T + 16$
  and $a = \begin{bmatrix} 36 + 79T & 17 + 19T + T^2 \end{bmatrix}$
- $N = F\left(\begin{bmatrix} 95 \\ 21 \end{bmatrix} / T + \begin{bmatrix} 6 \\ 12 \end{bmatrix} / T^2 + \dots \right) = \begin{bmatrix} 53 + 95T \\ 79 + 21T \end{bmatrix}$
  and $N^* = aN = 50 + 56T + 29T^2 + 21T^3$

Example cont.

- Choose $m = 2$, $U = \begin{bmatrix} 95 & 78 & 40 & 77 \\ 21 & 0 & 84 & 2 \end{bmatrix}$, $V^t = \begin{bmatrix} 84 & 55 & 12 & 33 \\ 43 & 27 & 81 & 50 \end{bmatrix}$
- $(UM_2^s V^t)_{0 \leq s < 4} = \left(\begin{bmatrix} 62 & 89 \\ 25 & 47 \end{bmatrix}, \begin{bmatrix} 10 & 95 \\ 45 & 92 \end{bmatrix}, \begin{bmatrix} 61 & 93 \\ 32 & 50 \end{bmatrix}, \begin{bmatrix} 22 & 49 \\ 5 & 13 \end{bmatrix} \right)$
- $F = \begin{bmatrix} T^2 + 19T + 17 & 41T + 68 \\ 18T + 61 & T^2 + 28T + 11 \end{bmatrix}$
  and $P = T^4 + 47T^3 + 16T^2 + 64T + 16$
  and $a = \begin{bmatrix} 36 + 79T & 17 + 19T + T^2 \end{bmatrix}$
- $N = F\left(\begin{bmatrix} 95 \\ 21 \end{bmatrix} / T + \begin{bmatrix} 6 \\ 12 \end{bmatrix} / T^2 + \dots \right) = \begin{bmatrix} 53 + 95T \\ 79 + 21T \end{bmatrix}$
  and $N^* = aN = 50 + 56T + 29T^2 + 21T^3$
- $N_1 = F\left(\begin{bmatrix} 95 \\ 76 \end{bmatrix} / T + \begin{bmatrix} 76 \\ 11 \end{bmatrix} / T^2 + \dots \right) = \begin{bmatrix} 50 + 95T \\ 66 + 76T \end{bmatrix}$
  and $N_1^* = aN_1 = 12 + 22T + 91T^2 + 76T^3$

Example cont.

- Choose $m = 2$, $U = \begin{bmatrix} 95 & 78 & 40 & 77 \\ 21 & 0 & 84 & 2 \end{bmatrix}$, $V^t = \begin{bmatrix} 84 & 55 & 12 & 33 \\ 43 & 27 & 81 & 50 \end{bmatrix}$
- $(UM_2^s V^t)_{0 \le s < 4} = \left(\begin{bmatrix} 62 & 89 \\ 25 & 47 \end{bmatrix}, \begin{bmatrix} 10 & 95 \\ 45 & 92 \end{bmatrix}, \begin{bmatrix} 61 & 93 \\ 32 & 50 \end{bmatrix}, \begin{bmatrix} 22 & 49 \\ 5 & 13 \end{bmatrix} \right)$
- $F = \begin{bmatrix} T^2 + 19T + 17 & 41T + 68 \\ 18T + 61 & T^2 + 28T + 11 \end{bmatrix}$
  and $P = T^4 + 47T^3 + 16T^2 + 64T + 16$
  and $a = \begin{bmatrix} 36 + 79T & 17 + 19T + T^2 \end{bmatrix}$
- $N = F\left(\begin{bmatrix} 95 \\ 21 \end{bmatrix} / T + \begin{bmatrix} 6 \\ 12 \end{bmatrix} / T^2 + \dots \right) = \begin{bmatrix} 53 + 95T \\ 79 + 21T \end{bmatrix}$
  and $N^* = aN = 50 + 56T + 29T^2 + 21T^3$
- $N_1 = F\left(\begin{bmatrix} 95 \\ 76 \end{bmatrix} / T + \begin{bmatrix} 76 \\ 11 \end{bmatrix} / T^2 + \dots \right) = \begin{bmatrix} 50 + 95T \\ 66 + 76T \end{bmatrix}$
  and $N_1^* = aN_1 = 12 + 22T + 91T^2 + 76T^3$
- Finally $N_1^* / N^* \mod P = 86T^3 + 49T^2 + 39T + 38$

Experimental Results

- Implemented in LinBox, Eigen, NTL
- M_i's computed by Magma, over $GF(65537)$

name	n	D	**density**	$m = 1$	$m = 3$	$m = 6$
rand1-26	3	17576	0.06	692	307	168
rand1-28	3	21952	0.05	1261	471	331
rand1-30	3	27000	0.05	2191	786	512
rand2-10	4	10000	0.14	301	109	79
rand2-11	4	14641	0.13	851	303	239
rand2-12	4	20736	0.12	2180	784	648
mixed1-22	3	10864	0.07	207	75	58
mixed1-23	3	12383	0.07	294	107	92
mixed1-24	3	14040	0.07	413	150	125
mixed2-10	4	10256	0.16	362	130	113
mixed2-11	4	14897	0.14	989	384	278
mixed2-12	4	20992	0.13	2480	892	807
mixed3-12	12	4109	0.5	75	27	21
mixed3-13	13	8206	0.48	554	198	171

Using Original Coordinates

- Multiplication matrix M for $x = t_1x_1 + \cdots + t_nx_n$ denser than M_i's
- Compute as many points in $V(I)$ as possible using x_n
- Compute the residual points by using $x = t_1x_1 + \cdots + t_nx_n$
- Some additional polynomial operations required

Experimental Results

- Ratio of improved/original

name	n	D	$m = 1$	$m = 3$	$m = 6$	x_n/x
rand1-26	3	17576	0.426	0.339	0.511	17576/17576
rand1-28	3	21952	0.414	0.393	0.461	21952/21952
rand1-30	3	27000	0.41	0.54	0.521	27000/27000
rand2-10	4	10000	0.412	0.407	0.367	10000/10000
rand2-11	4	14641	0.406	0.53	0.365	14641/14641
rand2-12	4	20736	0.417	0.412	0.35	20736/20736
mixed1-22	3	10864	0.425	0.417	0.446	10648/10675
mixed1-23	3	12383	0.42	0.414	0.398	12167/12194
mixed1-24	3	14040	0.413	0.404	0.4	13824/13851
mixed2-10	4	10256	0.379	0.379	0.434	10000/10016
mixed2-11	4	14897	0.378	0.349	0.402	14641/14657
mixed2-12	4	20992	0.39	0.391	0.338	20736/20752
mixed3-12	12	4109	0.401	0.392	0.422	4096/4097
mixed3-13	13	8206	0.41	0.405	0.384	8192/8193