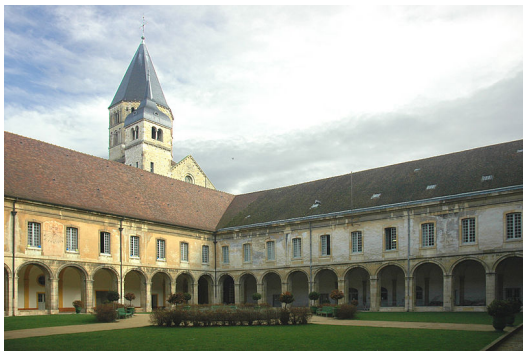
Algèbre linéaire pour le calcul de bases de Gröbner de suites multidimensionnelles récurrentes linéaires

par Jérémy Berthomieu[abc], Brice Boyer[abc], Jean-Charles Faugère[cab]

a. Sorbonne Universités, UPMC Univ Paris 06, Équipe PolSys, LIP6, Paris

b. CNRS, UMR 7606, LIP6, Paris

c. INRIA, Équipe PolSys, Centre Paris – Rocquencourt, Paris



JNCF 2015 – Cluny – Jeudi 5 novembre 2015

Problem.

Can we compress the following table:

$$\boldsymbol{u} = \begin{pmatrix} u_{0,0} & u_{0,1} & \cdots \\ u_{1,0} & u_{1,1} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 8 & 16 & \cdots \\ 3 & -1 & 12 & -4 & 48 & \cdots \\ -3 & 8 & -12 & 32 & -48 & \cdots \\ 9 & -24 & 36 & -96 & 144 & \cdots \\ -32 & 48 & -128 & 192 & -512 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Problem.

Can we compress the following table:

$$\boldsymbol{u} = \begin{pmatrix} u_{0,0} & u_{0,1} & \cdots \\ u_{1,0} & u_{1,1} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 8 & 16 & \cdots \\ 3 & -1 & 12 & -4 & 48 & \cdots \\ -3 & 8 & -12 & 32 & -48 & \cdots \\ 9 & -24 & 36 & -96 & 144 & \cdots \\ -32 & 48 & -128 & 192 & -512 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Solution.

For all $(i,j) \in \mathbb{N}^2$, we have

$$\begin{cases} u_{i+2,j} &= u_{i+1,j+1} - u_{i,j+1} \\ u_{i,j+2} &= 4\,u_{i,j}. \end{cases}$$

Problem.

Can we compress the following table:

$$\boldsymbol{u} = \begin{pmatrix} u_{0,0} & u_{0,1} & \cdots \\ u_{1,0} & u_{1,1} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 8 & 16 & \cdots \\ 3 & -1 & 12 & -4 & 48 & \cdots \\ -3 & 8 & -12 & 32 & -48 & \cdots \\ 9 & -24 & 36 & -96 & 144 & \cdots \\ -32 & 48 & -128 & 192 & -512 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Solution.

For all $(i,j) \in \mathbb{N}^2$, we have

$$\begin{cases} u_{i+2,j} &= u_{i+1,j+1} - u_{i,j+1} \\ u_{i,j+2} &= 4\,u_{i,j}. \end{cases}$$

Problem.

Can we compress the following table:

$$\boldsymbol{u} = \begin{pmatrix} u_{0,0} & u_{0,1} & \cdots \\ u_{1,0} & u_{1,1} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 8 & 16 & \cdots \\ 3 & -1 & 12 & -4 & 48 & \cdots \\ -3 & 8 & -12 & 32 & -48 & \cdots \\ 9 & -24 & 36 & -96 & 144 & \cdots \\ -32 & 48 & -128 & 192 & -512 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Solution.

→ Extension of Berlekamp – Massey problem [Berlekamp 1968, Massey 1969]
We can compress $\boldsymbol{u}$ with

$$\begin{cases} (u_{i,j})_{0 \le i,j \le 1} &= \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix} \\ u_{i+2,j} &= u_{i+1,j+1} - u_{i,j+1} \\ u_{i,j+2} &= 4\, u_{i,j}. \end{cases}$$

→ Berlekamp – Massey – Sakata (BMS) algorithm computes these relations [Sakata 1988, 1990].

Definition.

Let $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$ be a n-dimensional sequence. Let $\boldsymbol{x} = (x_1, ..., x_n)$, for any monomial $\boldsymbol{x^i} = x_1^{i_1} \cdots x_n^{i_n}$, we define

$$[\boldsymbol{x^i}] = [\boldsymbol{x^i}]_{\boldsymbol{u}} = u_{\boldsymbol{i}}.$$

We extend this definition to polynomials by linearity.

Example.

For $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^2}$ and $P = x_1\, x_2 - x_2 - 1$,

$$\begin{aligned} [P] &= u_{1,1} - u_{0,1} - u_{0,0} \\ [x_1^2\, x_2^3\, P] &= u_{3,4} - u_{2,4} - u_{2,3}. \end{aligned}$$

Definition – Dimension 1.

A nonzero sequence $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}}$ over $\mathbb{K}$ is linear recurrent with constant coefficients of order d if there exist $\alpha_0, \ldots, \alpha_{d-1} \in \mathbb{K}$ such that

$$\forall i \in \mathbb{N}, \quad u_{i+d} + \sum_{k=0}^{d-1} \alpha_k \, u_{i+k} = 0,$$

and d is minimal.

In other words, for all $i \in \mathbb{N}$, $[x^i \, (x^d + \sum_{k=0}^{d-1} \alpha_k \, x^k)] = 0$.

Example.

- $\boldsymbol{u} = (3^i)_{i\in\mathbb{N}}$ is linear recurrent with constant coefficients of order 1.
- $\boldsymbol{u} = ((3\,i+2)\,5^i)_{i\in\mathbb{N}}$ and $\boldsymbol{v} = (2^i + 3^i)_{i\in\mathbb{N}}$ are both linear recurrent with constant coefficients of order 2.
- $\boldsymbol{u} = (1/i!)_{i\in\mathbb{N}}$ is not linear recurrent with constant coefficients.

Definition – Dimension 1.

A nonzero sequence $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}}$ over $\mathbb{K}$ is linear recurrent with constant coefficients of order d if there exist $\alpha_0, \ldots, \alpha_{d-1} \in \mathbb{K}$ such that

$$\forall i \in \mathbb{N}, \quad u_{i+d} + \sum_{k=0}^{d-1} \alpha_k u_{i+k} = 0,$$

and d is minimal.

In other words, for all $i \in \mathbb{N}$, $[x^i (x^d + \sum_{k=0}^{d-1} \alpha_k x^k)] = 0$.

Proposition.

- Defining the ideal of relations of $\boldsymbol{u}$ as $I = \{P \in \mathbb{K}[x], [P] = 0\}$, then $\boldsymbol{u}$ is linear recurrent with constant coefficients of order d if and only if $\dim_{\mathbb{K}} \mathbb{K}[x]/I = d$.

  The knowledge of $u_0, \ldots, u_{d-1}$ and a generator of I allows us to compute u_i, for all $i \in \mathbb{N}$.

- The generating series $\sum_{i=0}^{\infty} u_i x^i$ of $\boldsymbol{u}$ is in $\mathbb{K}(x)$ if and only if $\boldsymbol{u}$ is linear recurrent with constant coefficients.

- Dimension 1: Berlekamp – Massey algorithm (BM).
- Definitions of multidimensional recurrent sequences.
- FGLM: inspiration and application.
- Algorithms for finding the relations.
- Complexity of the queries.
- Computation of the generating series.
- Applications to Sparse FGLM and correcting codes.

Definition.

Let $\boldsymbol{t} = (t_i)_{0 \le i \le 2n-1}$. Matrix $H = (h_{i,j})_{0 \le i,j \le n-1}$ is Hankel if for all $i, j \le n-1$,

$$h_{i,j} = t_{i+j}.$$

How to find the relations of a 1-dimensional sequence?

If one knows that sequence $\boldsymbol{u} = (u_i)_{i \in \mathbb{N}}$ is linear recurrent of order d.

- $\exists \alpha_0, \ldots, \alpha_{d-1}, \forall i \in \mathbb{N},\ \alpha_0 u_0 + \cdots + \alpha_{d-1} u_{d-1} + u_d = 0.$
- Solve the Hankel system $\begin{cases} \alpha_0 u_0 + \cdots + \alpha_{d-1} u_{d-1} &= -u_d \\ \vdots & \vdots \quad \vdots \\ \alpha_0 u_{d-1} + \cdots + \alpha_{d-1} u_{2d-2} &= -u_{2d-1}. \end{cases}$

Matrix version of BM.

Input: A sequence $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}}$ over $\mathbb{K}$, $d \in \mathbb{N}^*$.
Output: A polynomial of degree at most $d+1$.

$H := (u_{i+j})_{0\le i,j\le d-1}$. `/* a Hankel matrix */`
Compute $S' = \{s_0, ..., s_{r-1}\}$ the column rank profile.
`/*` $\{C_{s_0}, ..., C_{s_{r-1}}\}$ `set of indep. columns with minimal indices in` H `*/`

Find $\begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix}$ s.t. $\begin{pmatrix} u_0 & \cdots & u_{d-1} \\ \vdots & \ddots & \vdots \\ u_{d-1} & \cdots & u_{2d-2} \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} + \begin{pmatrix} u_d \\ \vdots \\ u_{2d-1} \end{pmatrix} = 0.$

Return $x^{s_{r-1}+1} + \sum_{j=0}^{r-1} \alpha_{s_j} x^{s_j}$.

Theorem. [Berlekamp 1968, Massey 1969, Kaltofen, Yuhasz 2013]

BM algorithm is correct. It computes the polynomial of the relation in $O(\mathsf{M}(d)\log d)$ operations in $\mathbb{K}$.

Matrix version of BM.

Input: A sequence $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}}$ over $\mathbb{K}$, $d \in \mathbb{N}^*$.
Output: A polynomial of degree at most $d+1$.

$H := (u_{i+j})_{0\le i,j\le d-1}$. `/* a Hankel matrix */`
Compute $S' = \{s_0, ..., s_{r-1}\}$ the column rank profile.
`/*` $\{C_{s_0}, ..., C_{s_{r-1}}\}$ `set of indep. columns with minimal indices in` H `*/`

Find $\begin{pmatrix} \alpha_{s_0} \\ \vdots \\ \alpha_{s_{r-1}} \end{pmatrix}$ s.t. $\begin{pmatrix} u_{2s_0} & \cdots & u_{s_0+s_{r-1}} \\ \vdots & \ddots & \vdots \\ u_{s_{r-1}+s_0} & \cdots & u_{2s_{r-1}} \end{pmatrix}\begin{pmatrix} \alpha_{s_0} \\ \vdots \\ \alpha_{s_{r-1}} \end{pmatrix} + \begin{pmatrix} u_{s_0+s_{r-1}+1} \\ \vdots \\ u_{2s_{r-1}+1} \end{pmatrix} = 0.$

Return $x^{s_{r-1}+1} + \sum_{j=0}^{r-1} \alpha_{s_j} x^{s_j}$.

Theorem. [Berlekamp 1968, Massey 1969, Kaltofen, Yuhasz 2013]

BM algorithm is correct. It computes the polynomial of the relation in $O(\mathsf{M}(d)\log d)$ operations in $\mathbb{K}$.

Problem.

Definitions for n-dimensional sequences linear recurrent sequences extends badly dimension 1 definition:

[Chabanne, Norton 1992, Saints, Heegard 1995]
$\boldsymbol{u}$ is linear recurrent if there exists $P \in \mathbb{K}[\boldsymbol{x}] \setminus \{0\}$ such that for all $\boldsymbol{i} \in \mathbb{N}^n$ $[\boldsymbol{x}^{\boldsymbol{i}} P] = 0$.

→ Sequence $\boldsymbol{u} = (2^{i_2}/i_1!)_{\boldsymbol{i} \in \mathbb{N}^2} = \begin{pmatrix} 1 & 2 & 4 & 8 & \cdots \\ 1 & 2 & 4 & 8 & \cdots \\ 1/2 & 1 & 2 & 4 & \cdots \\ 1/6 & 1/3 & 2/3 & 4/3 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$ satisfies $[\boldsymbol{x}^{\boldsymbol{i}} (x_2 - 2)] = 0$ but

- $\sum_{\boldsymbol{i} \in \mathbb{N}^2} \frac{2^{i_2}}{i_1!} \boldsymbol{x}^{\boldsymbol{i}} = \frac{\exp x_1}{1 - 2\, x_2} \notin \mathbb{K}(\boldsymbol{x})$;
- infinitely many coefficients $u_{i_1,0} = 1/i_1!, i_1 \in \mathbb{N}$ needed to compute them all.

→ Sequence $\boldsymbol{b} = \left(\binom{i_1}{i_2}\right)_{\boldsymbol{i} \in \mathbb{N}^2} = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots \\ 1 & 1 & 0 & 0 & \cdots \\ 1 & 2 & 1 & 0 & \cdots \\ 1 & 3 & 3 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$ satisifies $[\boldsymbol{x}^{\boldsymbol{i}} (x_1\, x_2 - x_2 - 1)] = 0$,

Pascal's rule, and

$\sum_{\boldsymbol{i} \in \mathbb{N}^2} \binom{i_1}{i_2} \boldsymbol{x}^{\boldsymbol{i}} = \frac{1}{1 - x_1 - x_1\, x_2} \in \mathbb{K}(\boldsymbol{x})$ but

- infinitely many coefficients $b_{i_1,0} = 1, i_1 \in \mathbb{N}, b_{0,i_2} = 0, i_2 \in \mathbb{N}^*$ to compute them all.

Definition. [Sakata 2009]

Let $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}}$ be a nonzero n-dimensional sequence with coefficients in $\mathbb{K}$. The sequence $\boldsymbol{u}$ is linear recurrent if from a nonzero finite number of initial terms $u_i, i \in S$, and a finite number of linear recurrence relations, without any contradiction, one can compute any term of the sequence. We say the order is d if $\#S = d$ and S is minimal.

Proposition.

Equivalently, $\boldsymbol{u}$ is linear recurrent if its ideal of relations has dimension 0.

Example.

- $\boldsymbol{u} = \begin{pmatrix} 1 & 2 & 4 & 8 & \cdots \\ 3 & -1 & 12 & -4 & \cdots \\ -3 & 8 & -12 & 32 & \cdots \\ 9 & -24 & 36 & -96 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$ is linear recurrent: $\begin{cases} (u_{i,j})_{0\le i,j\le 1} &= \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix} \\ u_{i+2,j} &= u_{i+1,j+1} - u_{i,j+1} \\ u_{i,j+2} &= 4\,u_{i,j}. \end{cases}$

  The ideal of relations is $\langle x^2 - x\,y + y, y^2 - 4\rangle$ of dimension 0 and $\boldsymbol{u}$ has order 4.

- $\boldsymbol{b} = \left(\binom{i}{j}\right)_{(i,j)\in\mathbb{N}^2} = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots \\ 1 & 1 & 0 & 0 & \cdots \\ 1 & 2 & 1 & 0 & \cdots \\ 1 & 3 & 3 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$ is not linear recurrent: $\begin{cases} (b_{i,0})_{0\le i} &= 1 \\ (b_{0,j})_{1\le j} &= 0 \\ b_{i+1,j+1} &= b_{i,j+1} + b_{i,j}. \end{cases}$

  BMS for $(b_{i,j})_{(i,j)}$ with $i + j \leqslant d$ returns $\langle (x-1)^{d+1}, x\,y - y - 1, y^{d+1}\rangle = \langle 1\rangle$ of dimension -1!

Definition. [Sakata 2009]

Let $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}}$ be a nonzero n-dimensional sequence with coefficients in $\mathbb{K}$. The sequence $\boldsymbol{u}$ is linear recurrent if from a nonzero finite number of initial terms $u_i, i \in S$, and a finite number of linear recurrence relations, without any contradiction, one can compute any term of the sequence. We say the order is d if $\#S = d$ and S is minimal.

Theorem.

Sequence $\boldsymbol{u}$ is linear recurrent if, equivalently,

- its ideal of relations has dimension 0;
- its generating series

$$S = \sum_{\boldsymbol{i}\in\mathbb{N}^n} u_{\boldsymbol{i}}\, \boldsymbol{x}^{\boldsymbol{i}} = \frac{N(\boldsymbol{x})}{Q_1(x_1)\cdots Q_n(x_n)} \in \mathbb{K}(\boldsymbol{x}).$$

Example.

The generating series of $\boldsymbol{u} = \begin{pmatrix} 1 & 2 & 4 & 8 & \cdots \\ 3 & -1 & 12 & -4 & \cdots \\ -3 & 8 & -12 & 32 & \cdots \\ 9 & -24 & 36 & -96 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$ is $\dfrac{N(x,y)}{(4\,x^4 - 8\,x^3 + 4\,x^2 - 1)\,(4\,y^2 - 1)}$.

Proposition.

Let $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i}\in\mathbb{N}^n}$ be a linear recurrent sequence over $\mathbb{K}$. Let S be the staircase of a Gröbner basis $\mathcal{G}$ of its ideal of relations I.

Let $T_1, \ldots, T_n$ be the multiplication matrices by $x_1, \ldots, x_n$ in $\mathbb{K}[\boldsymbol{x}]/I$ with basis $(s)_{s\in S}$. Let $\boldsymbol{r} = (u_{\mathbf{0}}, \ldots) = ([s]_{\boldsymbol{u}})_{s\in S}$, then

$$\forall \boldsymbol{i} \in \mathbb{N}^n, \quad u_{\boldsymbol{i}} = \langle \boldsymbol{r}, T_1^{i_1} \cdots T_n^{i_n} \cdot \mathbf{1} \rangle, \ \mathbf{1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Proof Sketch.

First, $T_1^{i_1} \cdots T_n^{i_n} \cdot \mathbf{1}$ is the vector representing $\boldsymbol{x}^{\boldsymbol{i}}$ in $\mathbb{K}[\boldsymbol{x}]/I$.
Then, the scalar product corresponds exactly to the evaluation $[\mathrm{NF}(\boldsymbol{x}^{\boldsymbol{i}}, \mathcal{G})]_{\boldsymbol{u}}$.

Idea.

Reciprocally, we can build a linear recurrent sequence with a Gröbner basis and initial terms!

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Proof Sketch.

For any $\boldsymbol{i} \in \mathbb{N}^n$, let $u_{\boldsymbol{i}} = [\mathrm{NF}(\boldsymbol{x}^{\boldsymbol{i}}, \mathcal{G})]_{\boldsymbol{u}}$.

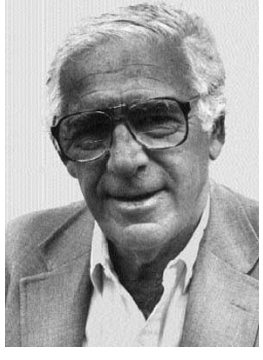


Figure 1. D. Gorenstein (1923 – 1992)

Figure 2. A. Grothendieck (1928 – 2014)

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Example.

$\mathcal{G} = \{y^2 - 1, x - 2\,y\}$, $\{[1]_{\boldsymbol{u}} = a, [y]_{\boldsymbol{u}} = b\}$

$$\rightsquigarrow \begin{pmatrix} a & b \end{pmatrix}$$

Remarks.

The Gröbner basis does not yield any contradiction!
We will want relations in the sequence.

$\rightarrow$ Find elements in the ideal. (The ideal is not known!)

$\rightarrow$ Find a Gröbner basis $\rightsquigarrow$ FGLM is an inspiration.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Example.

$\mathcal{G} = \{y^2 - 1, x - 2\,y\}$, $\{[1]_{\boldsymbol{u}} = a, [y]_{\boldsymbol{u}} = b\}$

$$\rightsquigarrow \begin{pmatrix} a & b & a \end{pmatrix}$$

Remarks.

The Gröbner basis does not yield any contradiction!
We will want relations in the sequence.

$\rightarrow$ Find elements in the ideal. (The ideal is not known!)

$\rightarrow$ Find a Gröbner basis $\rightsquigarrow$ FGLM is an inspiration.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Example.

$\mathcal{G} = \{y^2 - 1, x - 2\,y\}$, $\{[1]_{\boldsymbol{u}} = a, [y]_{\boldsymbol{u}} = b\}$

$$\rightsquigarrow (\ a \quad b \quad a \quad b \quad \cdots\ )$$

Remarks.

The Gröbner basis does not yield any contradiction!
We will want relations in the sequence.

→ Find elements in the ideal. (The ideal is not known!)

→ Find a Gröbner basis $\rightsquigarrow$ FGLM is an inspiration.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Example.

$\mathcal{G} = \{y^2 - 1, x - 2\,y\}$, $\{[1]_{\boldsymbol{u}} = a, [y]_{\boldsymbol{u}} = b\}$

$$\rightsquigarrow \begin{pmatrix} a & b & a & b & \cdots \\ 2\,b & 2\,a & 2\,b & 2\,a & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Remarks.

The Gröbner basis does not yield any contradiction!
We will want relations in the sequence.

→ Find elements in the ideal. (The ideal is not known!)

→ Find a Gröbner basis $\rightsquigarrow$ FGLM is an inspiration.

Idea.

Computation of a Gröbner basis $\rightsquigarrow$ change of variables.

Proposition.

Natural action of $\mathrm{GL}_n(\mathbb{K})$ on n-dimensional sequences.
Let $A \in \mathrm{GL}_n(\mathbb{K})$ and $\boldsymbol{\xi} = A \cdot \boldsymbol{x}$, then from sequence $\boldsymbol{u}$, we build $\boldsymbol{v} = A \cdot \boldsymbol{u} = ([\boldsymbol{\xi}^{\boldsymbol{i}}]_{\boldsymbol{u}})_{\boldsymbol{i} \in \mathbb{N}^n}$.
If $\boldsymbol{u}$ is linear recurrent with ideal I, then $\boldsymbol{v}$ is linear recurrent with ideal

$$A^{-1} \cdot I := \{P(A^{-1}\boldsymbol{x}) | P \in I\}.$$

One can compute $\{v_{\boldsymbol{i}} | \sum_{\ell=1}^{n} i_\ell = |\boldsymbol{i}| \leq d\}$ in

- $O(n^{2d})$ memory space and operations in $\mathbb{K}$;
- $O(n^d)$ queries to $\boldsymbol{u}$.

Proposition.

Natural action of $\mathrm{GL}_n(\mathbb{K})$ on n-dimensional sequences.
Let $A \in \mathrm{GL}_n(\mathbb{K})$ and $\boldsymbol{\xi} = A \cdot \boldsymbol{x}$, then from sequence $\boldsymbol{u}$, we build $\boldsymbol{v} = A \cdot \boldsymbol{u} = ([\boldsymbol{\xi}^{\boldsymbol{i}}]_{\boldsymbol{u}})_{\boldsymbol{i} \in \mathbb{N}^n}$.
If $\boldsymbol{u}$ is linear recurrent with ideal I, then $\boldsymbol{v}$ is linear recurrent with ideal

$$A^{-1} \cdot I := \{P(A^{-1}\,\boldsymbol{x}) | P \in I\}.$$

One can compute $\{v_{\boldsymbol{i}} | \sum_{\ell=1}^{n} i_\ell = |\boldsymbol{i}| \leq d\}$ in

- $O(n^{2d})$ memory space and operations in $\mathbb{K}$;
- $O(n^d)$ queries to $\boldsymbol{u}$.

Example.

$\boldsymbol{u} = (u_{i,j})_{(i,j) \in \mathbb{N}^2}$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the

$$\begin{aligned} v_{0,0} &= u_{0,0} \\ v_{1,0} &= a\,u_{1,0} + b\,u_{0,1} & v_{0,1} &= c\,u_{1,0} + d\,u_{0,1} \\ v_{2,0} &= a^2\,u_{2,0} + 2\,a\,b\,u_{1,1} + b^2\,u_{0,2} & v_{1,1} &= a\,c\,u_{2,0} + (a\,d + b\,c)\,u_{1,1} + b\,d\,u_{0,2} \quad \ldots \end{aligned}$$

Proposition.

Natural action of $\mathrm{GL}_n(\mathbb{K})$ on n-dimensional sequences.
Let $A \in \mathrm{GL}_n(\mathbb{K})$ and $\boldsymbol{\xi} = A \cdot \boldsymbol{x}$, then from sequence $\boldsymbol{u}$, we build $\boldsymbol{v} = A \cdot \boldsymbol{u} = ([\boldsymbol{\xi}^{\boldsymbol{i}}]_{\boldsymbol{u}})_{\boldsymbol{i} \in \mathbb{N}^n}$.
If $\boldsymbol{u}$ is linear recurrent with ideal I, then $\boldsymbol{v}$ is linear recurrent with ideal

$$A^{-1} \cdot I := \{P(A^{-1}\,\boldsymbol{x}) | P \in I\}.$$

One can compute $\{v_{\boldsymbol{i}} | \sum_{\ell=1}^{n} i_\ell = |\boldsymbol{i}| \leq d\}$ in

- $O(n^{2d})$ memory space and operations in $\mathbb{K}$;
- $O(n^d)$ queries to $\boldsymbol{u}$.

Proof Sketch.

$$[P(A^{-1}\,\boldsymbol{x})]_{\boldsymbol{v}} = [P(A^{-1}\,A\,\boldsymbol{x})]_{\boldsymbol{u}} = [P]_{\boldsymbol{u}} = 0.$$

With $\boldsymbol{\xi} = (\xi_1, ..., \xi_n)$, compute $[(z_0 + \xi_1\,z_1 + \cdots + \xi_n\,z_n)^d]_{\boldsymbol{u}}$.

The coefficient of $z_0^{d-|\boldsymbol{i}|}\,z_1^{i_1} \cdots z_n^{i_n}$ is exactly $v_{\boldsymbol{i}}$.

Theorem – Advantage.

For a generic n-dimensional sequence $\boldsymbol{u}$ of ideal of relations I and random $A \in \mathrm{GL}_n(\mathbb{K})$, $A^{-1} \cdot I$ is in shape position:

$$A^{-1} \cdot I = \langle x_1 - h_1(x_n), \ldots, x_{n-1} - h_{n-1}(x_n), h_n(x_n) \rangle, \quad \deg h_n = d.$$

This computation requires

- to run BM algorithm in $O(\mathsf{M}(d) \log d)$ operations in $\mathbb{K}$ for h_n;
- to solve $n-1$ Hankel systems in $O(n\,\mathsf{M}(d) \log d)$ operations in $\mathbb{K}$ for $h_1, \ldots, h_{n-1}$;
- $(n+1)\,d$ queries to the new table.

Example.

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 4 & 8 & \cdots \\ 3 & -1 & 12 & -4 & \cdots \\ -3 & 8 & -12 & 32 & \cdots \\ 9 & -24 & 36 & -96 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} 1 & 1 & 3 & 13 & 24 & 80 & 212 & 564 \\ 5 & -7 & -3 & -8 & \spadesuit & \spadesuit & \spadesuit & \spadesuit \\ \spadesuit & \spadesuit & \spadesuit & \spadesuit & \spadesuit & \spadesuit & \spadesuit & \spadesuit \end{pmatrix}$$ yields ideal

$$\langle x - 2\,y^3 + 2\,y^2 + 7\,y + 8, y^4 - 4\,y^2 - 8\,y - 4 \rangle.$$

Theorem – Advantage.

For a generic n-dimensional sequence $\boldsymbol{u}$ of ideal of relations I and random $A \in \mathrm{GL}_n(\mathbb{K})$, $A^{-1} \cdot I$ is in shape position:

$$A^{-1} \cdot I = \langle x_1 - h_1(x_n), \ldots, x_{n-1} - h_{n-1}(x_n), h_n(x_n) \rangle, \quad \deg h_n = d.$$

This computation requires

- to run BM algorithm in $O(\mathsf{M}(d) \log d)$ operations in $\mathbb{K}$ for h_n;
- to solve $n-1$ Hankel systems in $O(n\,\mathsf{M}(d) \log d)$ operations in $\mathbb{K}$ for $h_1, \ldots, h_{n-1}$;
- $(n+1)\,d$ queries to the new table.

Drawback.

This change of variables requires:

- $O(n^{d+2})$ memory space and operations in $\mathbb{K}$;
- $O(n^{2d})$ queries to the original table.

FGLM Algorithm.

Input: A Gröbner basis $\mathcal{G}_1$ of a 0-dim. ideal $I \subseteq \mathbb{K}[x]$ wrt. $\prec_1$ and another ordering $\prec_2$.
Output: A Gröbner basis $\mathcal{G}_2$ of I wrt. $\prec_2$.
$L := \{1\}, S := \{\}, \mathcal{G}_2 := \{\}$.

While $L \neq \varnothing$ **do**
  $t := \min_{\prec_2}(L)$ and remove t from L.
  $\bar{t} := \mathrm{NF}(t + \sum_{s \in S} \alpha_s s, \mathcal{G}_1)$.
  If $\exists (\alpha_s)_{s \in S},\ \bar{t} = 0$ **then** $\mathcal{G}_2 := \mathcal{G}_2 \cup \{t + \sum_{s \in S} \alpha_s s\}$ and remove multiples of t from L.
  Else $S := S \cup \{t\}, L := L \cup \{x_1 t, ..., x_n t\}$.
Return $\mathcal{G}_2$.

Theorem. [Faugère, Gianni, Lazard, Mora 1993]

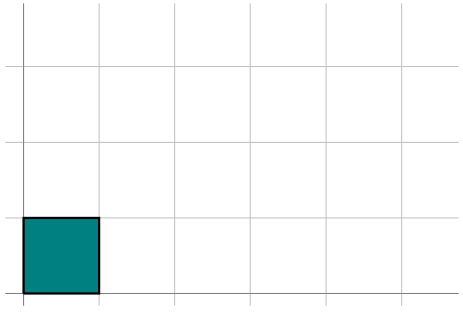
FGLM Algorithm is correct and computes $\mathcal{G}_2$ in $O(n\, d^3)$ operations in $\mathbb{K}$, where d is the dimension of I.

Example.

We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.

Example.

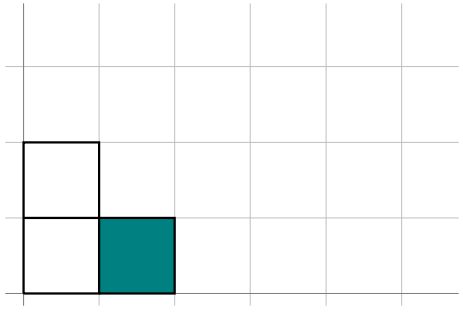
We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.



- $L = \{1\}$, $\mathrm{NF}(1, \mathcal{G}_1) = 1$.

Example.

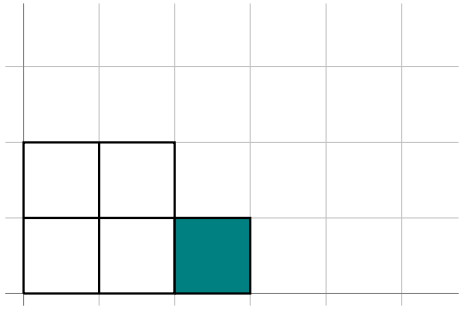
We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.



- $L = \{1\}$, $\mathrm{NF}(1, \mathcal{G}_1) = 1$.
- $L = \{x_1, x_2\}$, $\mathrm{NF}(x_1, \mathcal{G}_1) = x_1$.

Example.

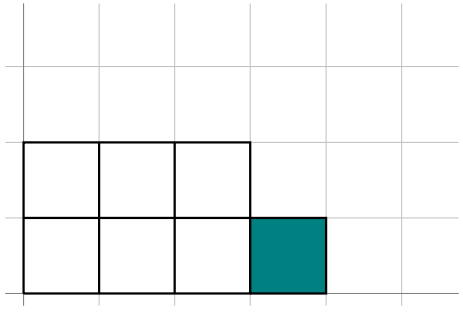
We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.



- $L = \{1\}$, $\mathrm{NF}(1, \mathcal{G}_1) = 1$.
- $L = \{x_1, x_2\}$, $\mathrm{NF}(x_1, \mathcal{G}_1) = x_1$.
- $L = \{x_1^2, x_2, x_1 x_2\}$, $\mathrm{NF}(x_1^2, \mathcal{G}_1) = -x_2 + x_1$.

Example.

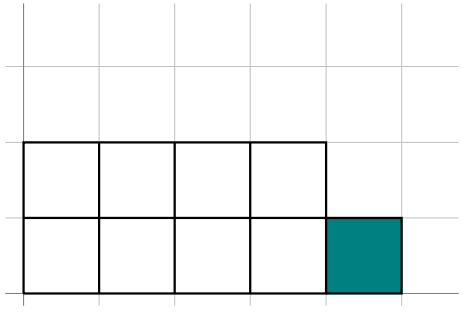
We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.



- $L = \{1\}$, $\mathrm{NF}(1, \mathcal{G}_1) = 1$.
- $L = \{x_1, x_2\}$, $\mathrm{NF}(x_1, \mathcal{G}_1) = x_1$.
- $L = \{x_1^2, x_2, x_1 x_2\}$, $\mathrm{NF}(x_1^2, \mathcal{G}_1) = -x_2 + x_1$.
- $L = \{x_1^3, x_2, x_1 x_2, x_1^2 x_2\}$, $\mathrm{NF}(x_1^3, \mathcal{G}_1) = -x_1 x_2 - x_2 + x_1$.

Example.

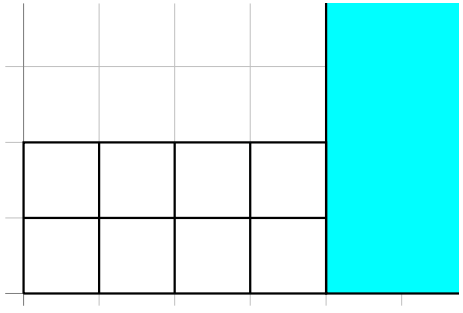
We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.



- $L = \{1\}$, $\mathrm{NF}(1, \mathcal{G}_1) = 1$.
- $L = \{x_1, x_2\}$, $\mathrm{NF}(x_1, \mathcal{G}_1) = x_1$.
- $L = \{x_1^2, x_2, x_1\,x_2\}$, $\mathrm{NF}(x_1^2, \mathcal{G}_1) = -x_2 + x_1$.
- $L = \{x_1^3, x_2, x_1\,x_2, x_1^2\,x_2\}$, $\mathrm{NF}(x_1^3, \mathcal{G}_1) = -x_1\,x_2 - x_2 + x_1$.
- $L = \{x_1^4, x_2, x_1\,x_2, x_1^2\,x_2, x_1^3\,x_2\}$, $\mathrm{NF}(x_1^4, \mathcal{G}_1) = -2\,x_1\,x_2 - x_2 + x_1 + 1$.

Example.

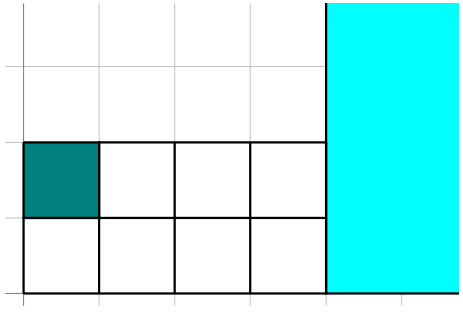
We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.



- $L = \{1\}$, $\mathrm{NF}(1, \mathcal{G}_1) = 1$.
- $L = \{x_1, x_2\}$, $\mathrm{NF}(x_1, \mathcal{G}_1) = x_1$.
- $L = \{x_1^2, x_2, x_1\,x_2\}$, $\mathrm{NF}(x_1^2, \mathcal{G}_1) = -x_2 + x_1$.
- $L = \{x_1^3, x_2, x_1\,x_2, x_1^2\,x_2\}$, $\mathrm{NF}(x_1^3, \mathcal{G}_1) = -x_1\,x_2 - x_2 + x_1$.
- $L = \{x_1^4, x_2, x_1\,x_2, x_1^2\,x_2, x_1^3\,x_2\}$, $\mathrm{NF}(x_1^4, \mathcal{G}_1) = -2\,x_1\,x_2 - x_2 + x_1 + 1$.

Example.

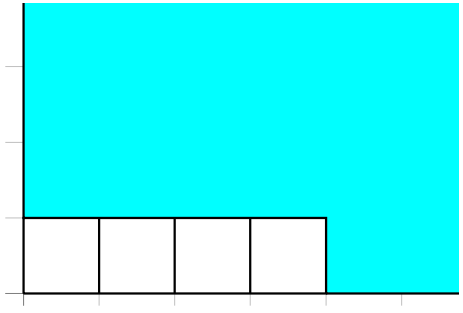
We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.



- $L = \{1\}$, $\mathrm{NF}(1, \mathcal{G}_1) = 1$.
- $L = \{x_1, x_2\}$, $\mathrm{NF}(x_1, \mathcal{G}_1) = x_1$.
- $L = \{x_1^2, x_2, x_1\,x_2\}$, $\mathrm{NF}(x_1^2, \mathcal{G}_1) = -x_2 + x_1$.
- $L = \{x_1^3, x_2, x_1\,x_2, x_1^2\,x_2\}$, $\mathrm{NF}(x_1^3, \mathcal{G}_1) = -x_1\,x_2 - x_2 + x_1$.
- $L = \{x_1^4,\ x_2,\ x_1\ x_2,\ x_1^2\ x_2,\ x_1^3\ x_2\}$, $\mathrm{NF}(x_1^4,\ \mathcal{G}_1) = -2\ x_1\ x_2 - x_2 + x_1 + 1 \Rightarrow (x_1^4 - 2\,x_1^3 + x_1^2 - 1) \in \mathcal{G}_2$.
- $L = \{x_2, x_1\,x_2, x_1^2\,x_2, x_1^3\,x_2\}$, $\mathrm{NF}(x_2, \mathcal{G}_1) = x_2$.

Example.

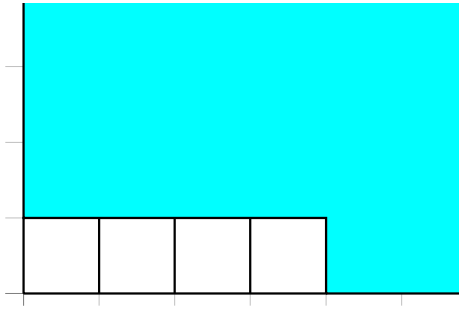
We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.



- $L = \{1\}$, $\mathrm{NF}(1, \mathcal{G}_1) = 1$.
- $L = \{x_1, x_2\}$, $\mathrm{NF}(x_1, \mathcal{G}_1) = x_1$.
- $L = \{x_1^2, x_2, x_1\,x_2\}$, $\mathrm{NF}(x_1^2, \mathcal{G}_1) = -x_2 + x_1$.
- $L = \{x_1^3, x_2, x_1\,x_2, x_1^2\,x_2\}$, $\mathrm{NF}(x_1^3, \mathcal{G}_1) = -x_1\,x_2 - x_2 + x_1$.
- $L = \{x_1^4,\ x_2,\ x_1\ x_2,\ x_1^2\ x_2,\ x_1^3\ x_2\}$, $\mathrm{NF}(x_1^4,\ \mathcal{G}_1) = -2\ x_1\ x_2 - x_2 + x_1 + 1 \Rightarrow (x_1^4 - 2\,x_1^3 + x_1^2 - 1) \in \mathcal{G}_2$.
- $L = \{x_2, x_1\,x_2, x_1^2\,x_2, x_1^3\,x_2\}$, $\mathrm{NF}(x_2, \mathcal{G}_1) = x_2 \Rightarrow (x_2 + x_1^2 - x_1) \in \mathcal{G}_2$.

Example.

We have $\mathcal{G}_1 = \{x_1^2 + x_2 - x_1,\ x_2^2 - 1\}$ wrt. DRL$(x_1 \prec_1 x_2)$ and we want $\mathcal{G}_2$ wrt. LEX$(x_1 \prec_2 x_2)$.



- $L = \{1\}$, $\mathrm{NF}(1, \mathcal{G}_1) = 1$.
- $L = \{x_1, x_2\}$, $\mathrm{NF}(x_1, \mathcal{G}_1) = x_1$.
- $L = \{x_1^2, x_2, x_1\,x_2\}$, $\mathrm{NF}(x_1^2, \mathcal{G}_1) = -x_2 + x_1$.
- $L = \{x_1^3, x_2, x_1\,x_2, x_1^2\,x_2\}$, $\mathrm{NF}(x_1^3, \mathcal{G}_1) = -x_1\,x_2 - x_2 + x_1$.
- $L = \{x_1^4,\ x_2,\ x_1\ x_2,\ x_1^2\ x_2,\ x_1^3\ x_2\}$, $\mathrm{NF}(x_1^4,\ \mathcal{G}_1) = -2\ x_1\ x_2 - x_2 + x_1 + 1 \Rightarrow (x_1^4 - 2\,x_1^3 + x_1^2 - 1) \in \mathcal{G}_2$.
- $L = \{x_2, x_1\,x_2, x_1^2\,x_2, x_1^3\,x_2\}$, $\mathrm{NF}(x_2, \mathcal{G}_1) = x_2 \Rightarrow (x_2 + x_1^2 - x_1) \in \mathcal{G}_2$.
- $L = \varnothing$, $\mathcal{G}_2 = \{x_1^4 - 2\,x_1^3 + x_1^2 - 1,\ x_2 + x_1^2 - x_1\}$.

What we want.

For a set of terms $\mathcal{T}$ and a polynomial $P \in \mathbb{K}[\boldsymbol{x}]$, we write

$$\mathrm{NF}(P, \mathcal{T}) = 0 \Leftrightarrow [t\,P]_{\boldsymbol{u}} = 0,\ \forall t \in \mathcal{T}.$$

What we should have.

Any BMS-like algorithm will generate minimal relations:

a) Find $P \in \mathbb{K}[\boldsymbol{x}]$, s.t. $\mathrm{NF}(P, \mathcal{T}) = 0$.

b) No nonzero relations $\sum_{t \prec \mathrm{LT}(P)} \alpha_t\,[m\,t]_{\boldsymbol{u}} = 0$ which are valid for all $m \in \mathcal{T}$.

Definition.

A finite set of terms S is a useful staircase if S is maximal for the inclusion, minimal for $\prec$ and $\sum_{t \in S} \beta_t\,[m\,t]_{\boldsymbol{u}} = 0,\ \forall m \in S$ implies that $\beta_t = 0$ for all $t \in S$.

Example.

For $\boldsymbol{u} = \begin{pmatrix} 1 & 2 & 4 & 8 & 16 & \cdots \\ 3 & -1 & 12 & -4 & 48 & \cdots \\ -3 & 8 & -12 & 32 & -48 & \cdots \\ 9 & -24 & 36 & -96 & 144 & \cdots \\ -32 & 48 & -128 & 192 & -512 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$ and $\mathcal{T} = \{1, y, x, y^2, x\,y, x^2\}$.

$\rightsquigarrow P = \alpha_1 + \alpha_y\, y + \alpha_x\, x + \alpha_{y^2}\, y^2 + \alpha_{xy}\, x\, y + \alpha_{x^2}\, x^2$ s.t. $\mathrm{NF}(P, \mathcal{T}) = 0$,

$\rightsquigarrow [t\,P]_{\boldsymbol{u}} = 0,\ \forall t \in \mathcal{T} \iff \begin{pmatrix} 1 & 2 & 3 & 4 & -1 & -3 \\ 2 & 4 & -1 & 8 & 12 & 8 \\ 3 & -1 & -3 & 12 & 8 & 9 \\ 4 & 8 & 12 & 16 & -4 & -12 \\ -1 & 12 & 8 & -4 & -12 & -24 \\ -3 & 8 & 9 & -12 & -24 & -3 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_y \\ \alpha_x \\ \alpha_{y^2} \\ \alpha_{xy} \\ \alpha_{x^2} \end{pmatrix} = 0.$

Finding a useful staircase is finding a maximal full rank submatrix $\rightsquigarrow$ rank profile.

Definition – Proposition.

For $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$ and two sorted sets of terms S, T, matrix $H_{S,T}$ is multi-Hankel

$$H_{S,T} = ([s\,t]_{\boldsymbol{u}})_{s \in S, t \in T} = \begin{array}{c} \\ \vdots \\ t \in T \\ \vdots \end{array} \begin{array}{c} \cdots \quad s \in S \quad \cdots \\ \begin{pmatrix} \ddots & \vdots & \iddots \\ \cdots & [s\,t]_{\boldsymbol{u}} & \cdots \\ \iddots & \vdots & \ddots \end{pmatrix} \end{array}.$$

If $S \subseteq T$ is a useful staircase, then $\operatorname{rank} H_S = \operatorname{rank} H_T$ with $H_S = H_{S,S}$.

Beware!

A useful staircase may fail to be a staircase.

Example.

For $\boldsymbol{u} = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$ and $\mathcal{T} = \{1, y, x, y^2, x\,y, x^2\}$

$\rightsquigarrow H_{\mathcal{T}} = ([s\,t]_{\boldsymbol{u}})_{s,t\in\mathcal{T}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ with useful staircase $S = \{y, x, y^2, x\,y\}$, $1 \notin S$.

Stabilization.

Stability criterion ensures we can turn a useful staircase into a staircase by adding divisors of the terms.

SCALAR-FGLM Algorithm.

Input: A sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i}\in\mathbb{N}^n}$ over $\mathbb{K}$, $d \in \mathbb{N}^*$ and $\prec$ a monomial ordering.
Output: A reduced $(d+1)$-truncated Gröbner basis wrt. $\prec$ of the ideal of relations of $\boldsymbol{u}$.

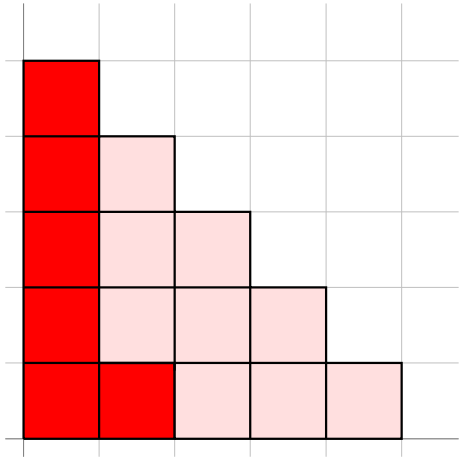
$\mathcal{T} := \{\boldsymbol{x}^{\boldsymbol{i}} \,|\, |\boldsymbol{i}| \leq d\}$ sorted by increasing order.
$H_{\mathcal{T}} := ([s\,t]_{\boldsymbol{u}})_{s,t\in\mathcal{T}}$. `/* a multi-Hankel matrix */`
Compute S' the useful staircase s.t. $\operatorname{rank} H_{S'} = \operatorname{rank} H_{\mathcal{T}}$.
$S := \operatorname{Stabilize}(S')$.
$L := \{\boldsymbol{x}^{\boldsymbol{i}} \,|\, |\boldsymbol{i}| \leq d+1\} \setminus S$.
$\mathcal{G} := \{\}$.
While $L \neq \varnothing$ **do**
  $t := \min_{\prec}(L)$ and remove t from L.
  Find $\boldsymbol{\alpha} = (\alpha_s)_{s\in S'}$ s.t. $H_{S'}\boldsymbol{\alpha} + H_{S',\{t\}} = 0$.
  $\mathcal{G} := \mathcal{G} \cup \{t + \sum_{s\in S'} \alpha_s\, s\}$ and remove multiples of t from L.
Return $\mathcal{G}$.

Proposition.

SCALAR-FGLM Algorithm is correct. If $\boldsymbol{u}$ is recursive of order D, then setting $d = D$ recovers the full Gröbner basis.

Problem.

We can visit too many elements! Assume $\mathrm{LT}(\mathcal{G}) = \{x_1, x_2^4\}$ with $x_1 \prec x_2$, then we visit $\{\boldsymbol{x^i} | i_1 + i_2 \leq 4\}$.



Solution.

Take the shape of the Gröbner basis into account!
Visit the monomial as in FGLM.

In FGLM, $\mathrm{NF}(f, \mathcal{G}) = 0 \Rightarrow \forall m, \mathrm{NF}(m\, f, \mathcal{G}) = 0$.
In BMS / Scalar-FGLM, $[f]_{\boldsymbol{u}} = 0 \not\Rightarrow \forall m, [m\, f]_{\boldsymbol{u}} = 0$.

From a staircase S, consider $t = x_i\, s$ for $s \in S$. If $\operatorname{rank} H_{S\cup\{t\}} > \operatorname{rank} H_S$, follow the lead!

Adaptive Scalar-FGLM Algorithm.

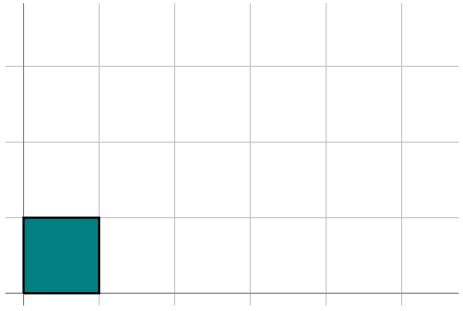
Input: A sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i}\in\mathbb{N}^n}$ over $\mathbb{K}$, $d \in \mathbb{N}^*$ and $\prec$ a monomial ordering.
Output: A reduced Gröbner basis wrt. $\prec$ of an ideal of degree at least d.
$L := \{1\}, S := \{\}, \mathcal{G}' := \{\}$.
While $L \neq \varnothing$ **do**
  $t := \min_{\prec}(L)$ and remove t from L.
  If $H_{S\cup\{t\}}$ is full rank **then**
    $S := S \cup \{t\}, L := L \cup \{x_1 t, ..., x_n t\}$ and remove multiples of $\mathcal{G}'$ in L.
    If $\#S \geq d$ **then** `/* early termination */`
      $\mathcal{G} := \{\}, \mathcal{G}' := \operatorname{MinGBasis}(\mathcal{G}' \cup L \cup \{\boldsymbol{x}^{\boldsymbol{i}} \,||\boldsymbol{i}| = \deg t + 1\} \setminus S)$.
      For all $t' \in \mathcal{G}'$ **do**
        $\mathcal{G} := \mathcal{G} \cup \{t' + \sum_{s\in S} \alpha_s\, s\}$ with $\boldsymbol{\alpha} = (\alpha_s)_{s\in S}$ s.t. $H_S\,\boldsymbol{\alpha} + H_{S,\{t'\}} = 0$.
      Return S and $\mathcal{G}$.
  Else $\mathcal{G}' := \mathcal{G}' \cup \{t\}$ and remove multiples of t in L.
Error "Run Scalar-FGLM".

Proposition.

S is a staircase of size at least d and for all $g \in \mathcal{G}$, $\operatorname{NF}(g, S) = 0$.
Can be extended to consider $t_1 = x_i\, s, t_2 = x_i^2\, s$ for $s \in S$ and so on.

Example.

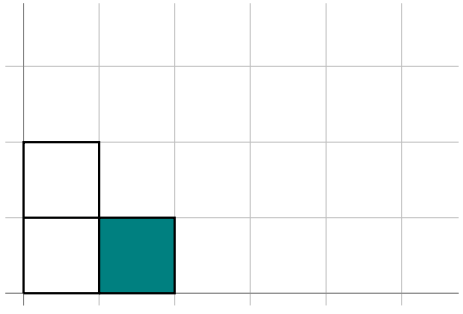
For $\boldsymbol{u} = \begin{pmatrix} 1 & -2 & -1 & 2 & 1 & \cdots \\ 1 & -6 & -1 & 6 & 1 & \cdots \\ 2 & 1 & -2 & -1 & 2 & \cdots \\ 6 & 1 & -6 & -1 & 6 & \cdots \\ -1 & 2 & 1 & -2 & -1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$, DRL$(x_1 \prec x_2)$ and $d = 4$.



- $L = \{1\}$, $H_{\{1\}} = (\ 1\ )$.

Example.

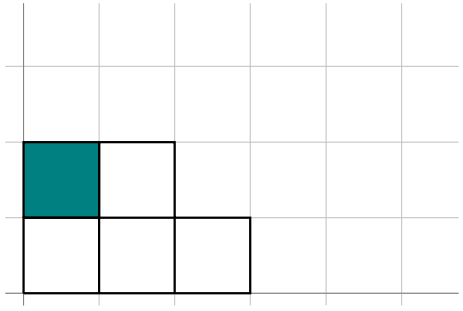
For $\boldsymbol{u} = \begin{pmatrix} 1 & -2 & -1 & 2 & 1 & \cdots \\ 1 & -6 & -1 & 6 & 1 & \cdots \\ 2 & 1 & -2 & -1 & 2 & \cdots \\ 6 & 1 & -6 & -1 & 6 & \cdots \\ -1 & 2 & 1 & -2 & -1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$, DRL$(x_1 \prec x_2)$ and $d = 4$.



- $L = \{1\}$, $\operatorname{rank} H_{\{1\}} = 1$, $S = \{1\}$.
- $L = \{x_1, x_2\}$, $H_{\{1,x_1\}} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

Example.

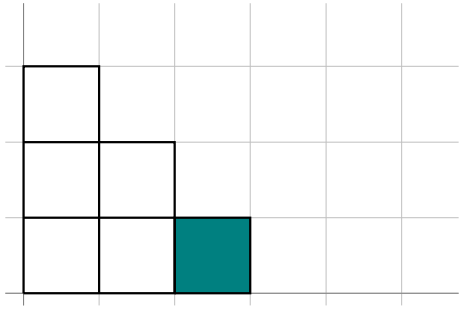
For $\boldsymbol{u} = \begin{pmatrix} 1 & -2 & -1 & 2 & 1 & \cdots \\ 1 & -6 & -1 & 6 & 1 & \cdots \\ 2 & 1 & -2 & -1 & 2 & \cdots \\ 6 & 1 & -6 & -1 & 6 & \cdots \\ -1 & 2 & 1 & -2 & -1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$, DRL$(x_1 \prec x_2)$ and $d = 4$.



- $L = \{1\}$, $\operatorname{rank} H_{\{1\}} = 1$, $S = \{1\}$.
- $L = \{x_1, x_2\}$, $\operatorname{rank} H_{\{1,x_1\}} = 2$, $S = \{1, x_1\}$.
- $L = \{x_2, x_1^2, x_1 x_2\}$, $H_{\{1,x_1,x_2\}} = \begin{pmatrix} 1 & 1 & -2 \\ 1 & 2 & -6 \\ -2 & -6 & -1 \end{pmatrix}$.

Example.

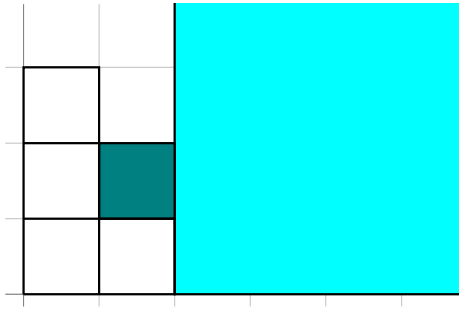
For $\boldsymbol{u} = \begin{pmatrix} 1 & -2 & -1 & 2 & 1 & \cdots \\ 1 & -6 & -1 & 6 & 1 & \cdots \\ 2 & 1 & -2 & -1 & 2 & \cdots \\ 6 & 1 & -6 & -1 & 6 & \cdots \\ -1 & 2 & 1 & -2 & -1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$, $\mathrm{DRL}(x_1 \prec x_2)$ and $d = 4$.



- $L = \{1\}$, $\operatorname{rank} H_{\{1\}} = 1$, $S = \{1\}$.
- $L = \{x_1, x_2\}$, $\operatorname{rank} H_{\{1,x_1\}} = 2$, $S = \{1, x_1\}$.
- $L = \{x_2, x_1^2, x_1 x_2\}$, $\operatorname{rank} H_{\{1,x_1,x_2\}} = 3$, $S = \{1, x_1, x_2\}$.
- $L = \{x_1^2, x_1 x_2, x_2^2\}$, $H_{\{1,x_1,x_2,x_1^2\}} = \begin{pmatrix} 1 & 1 & -2 & 2 \\ 1 & 2 & -6 & 6 \\ -2 & -6 & -1 & 1 \\ 2 & 6 & 1 & -1 \end{pmatrix}$.

Example.

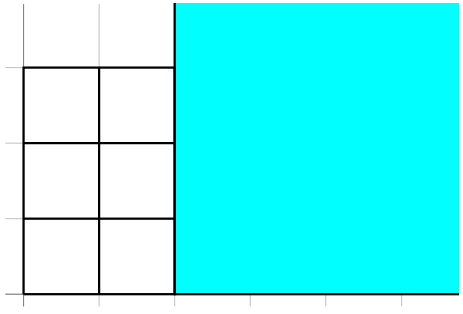
For $\boldsymbol{u} = \begin{pmatrix} 1 & -2 & -1 & 2 & 1 & \cdots \\ 1 & -6 & -1 & 6 & 1 & \cdots \\ 2 & 1 & -2 & -1 & 2 & \cdots \\ 6 & 1 & -6 & -1 & 6 & \cdots \\ -1 & 2 & 1 & -2 & -1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$, DRL$(x_1 \prec x_2)$ and $d = 4$.



- $L = \{1\}$, $\operatorname{rank} H_{\{1\}} = 1$, $S = \{1\}$.
- $L = \{x_1, x_2\}$, $\operatorname{rank} H_{\{1,x_1\}} = 2$, $S = \{1, x_1\}$.
- $L = \{x_2, x_1^2, x_1 x_2\}$, $\operatorname{rank} H_{\{1,x_1,x_2\}} = 3$, $S = \{1, x_1, x_2\}$.
- $L = \{x_1^2, x_1 x_2, x_2^2\}$, $\operatorname{rank} H_{\{1,x_1,x_2,x_1^2\}} = 3$, $\mathcal{G}' = \{x_1^2\}$.
- $L = \{x_1 x_2, x_2^2\}$, $H_{\{1,x_1,x_2,x_1x_2\}} = \begin{pmatrix} 1 & 1 & -2 & -6 \\ 1 & 2 & -6 & 1 \\ -2 & -6 & -1 & -1 \\ -6 & 1 & -1 & -2 \end{pmatrix}$

Example.

For $\boldsymbol{u} = \begin{pmatrix} 1 & -2 & -1 & 2 & 1 & \cdots \\ 1 & -6 & -1 & 6 & 1 & \cdots \\ 2 & 1 & -2 & -1 & 2 & \cdots \\ 6 & 1 & -6 & -1 & 6 & \cdots \\ -1 & 2 & 1 & -2 & -1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$, DRL$(x_1 \prec x_2)$ and $d = 4$.

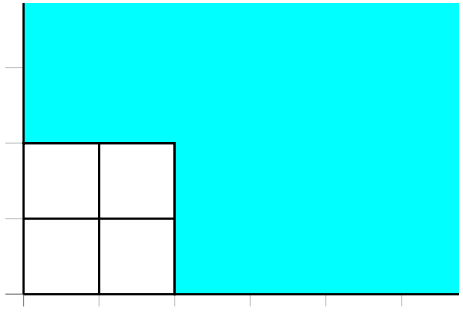


- $L = \{1\}$, $\operatorname{rank} H_{\{1\}} = 1$, $S = \{1\}$.
- $L = \{x_1, x_2\}$, $\operatorname{rank} H_{\{1,x_1\}} = 2$, $S = \{1, x_1\}$.
- $L = \{x_2, x_1^2, x_1 x_2\}$, $\operatorname{rank} H_{\{1,x_1,x_2\}} = 3$, $S = \{1, x_1, x_2\}$.
- $L = \{x_1^2, x_1 x_2, x_2^2\}$, $\operatorname{rank} H_{\{1,x_1,x_2,x_1^2\}} = 3$, $\mathcal{G}' = \{x_1^2\}$.
- $L = \{x_1 x_2, x_2^2\}$, $H_{\{1,x_1,x_2,x_1x_2\}} = \begin{pmatrix} 1 & 1 & -2 & -6 \\ 1 & 2 & -6 & 1 \\ -2 & -6 & -1 & -1 \\ -6 & 1 & -1 & -2 \end{pmatrix}$, $S = \{1, x_1, x_2, x_1 x_2\}$.

  $\#S = 4 \rightsquigarrow$ Early termination! $L := \{x_2^2, x_1 x_2^2\}$.
  $\mathcal{G}' = \text{MinGBasis}(\mathcal{G}' \cup L \cup \{\boldsymbol{x}^{\boldsymbol{i}} \,||\boldsymbol{i}| = 3\} \setminus S) = \{x_1^2, x_2^2\}$.

Example.

For $\boldsymbol{u} = \begin{pmatrix} 1 & -2 & -1 & 2 & 1 & \cdots \\ 1 & -6 & -1 & 6 & 1 & \cdots \\ 2 & 1 & -2 & -1 & 2 & \cdots \\ 6 & 1 & -6 & -1 & 6 & \cdots \\ -1 & 2 & 1 & -2 & -1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$, DRL$(x_1 \prec x_2)$ and $d = 4$.



- $L = \{1\}$, $\operatorname{rank} H_{\{1\}} = 1$, $S = \{1\}$.
- $L = \{x_1, x_2\}$, $\operatorname{rank} H_{\{1,x_1\}} = 2$, $S = \{1, x_1\}$.
- $L = \{x_2, x_1^2, x_1 x_2\}$, $\operatorname{rank} H_{\{1,x_1,x_2\}} = 3$, $S = \{1, x_1, x_2\}$.
- $L = \{x_1^2, x_1 x_2, x_2^2\}$, $\operatorname{rank} H_{\{1,x_1,x_2,x_1^2\}} = 3$, $\mathcal{G}' = \{x_1^2\}$.
- $L = \{x_1 x_2, x_2^2\}$, $H_{\{1,x_1,x_2,x_1x_2\}} = \begin{pmatrix} 1 & 1 & -2 & -6 \\ 1 & 2 & -6 & 1 \\ -2 & -6 & -1 & -1 \\ -6 & 1 & -1 & -2 \end{pmatrix}$, $S = \{1, x_1, x_2, x_1 x_2\}$.

  $\#S = 4 \rightsquigarrow$ Early termination! $L := \{x_2^2, x_1 x_2^2\}$.

  $\mathcal{G}' = \text{MinGBasis}(\mathcal{G}' \cup L \cup \{\boldsymbol{x}^{\boldsymbol{i}} \,||\boldsymbol{i}| = 3\} \setminus S) = \{x_1^2, x_2^2\} \rightsquigarrow \mathcal{G} = \{x_1^2 - x_2, x_2^2 + 1\}$.

Proposition.

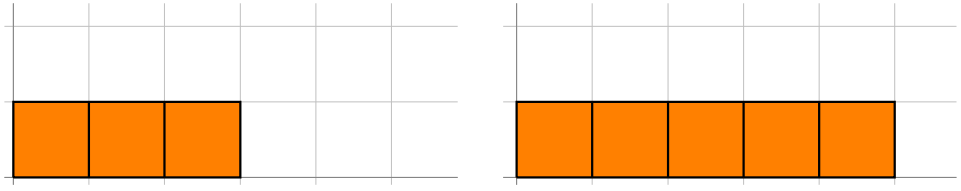
The number of table queries done by ADAPTIVE SCALAR-FGLM is the $\#(2\,S)$ where $2\,S = \{u\,v | u, v \in S\}$.

Problem.

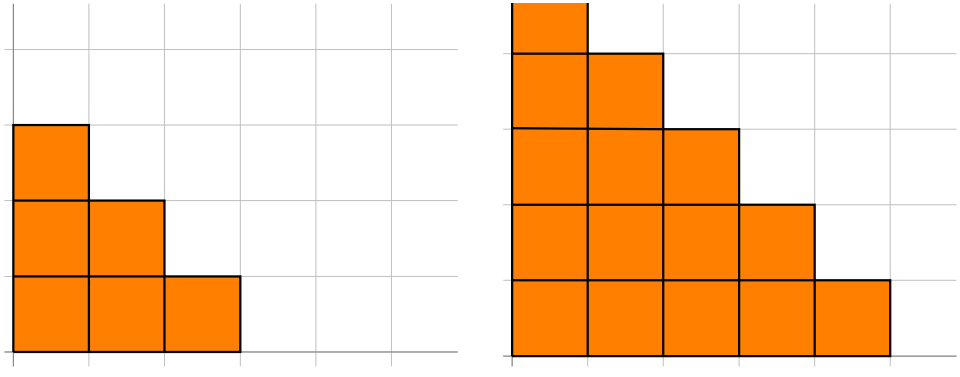
In the worst case $\#(2\,S) \leq \#S\,(\#S - 1)\,/\,2 \leq (\#S)^2\,/\,2$.

In practice.

- $S = \{1, ..., x^d\}, 2\,S = \{1, ..., x^{2d}\} \Rightarrow \#(2\,S) = 2\,\#S - 1.$

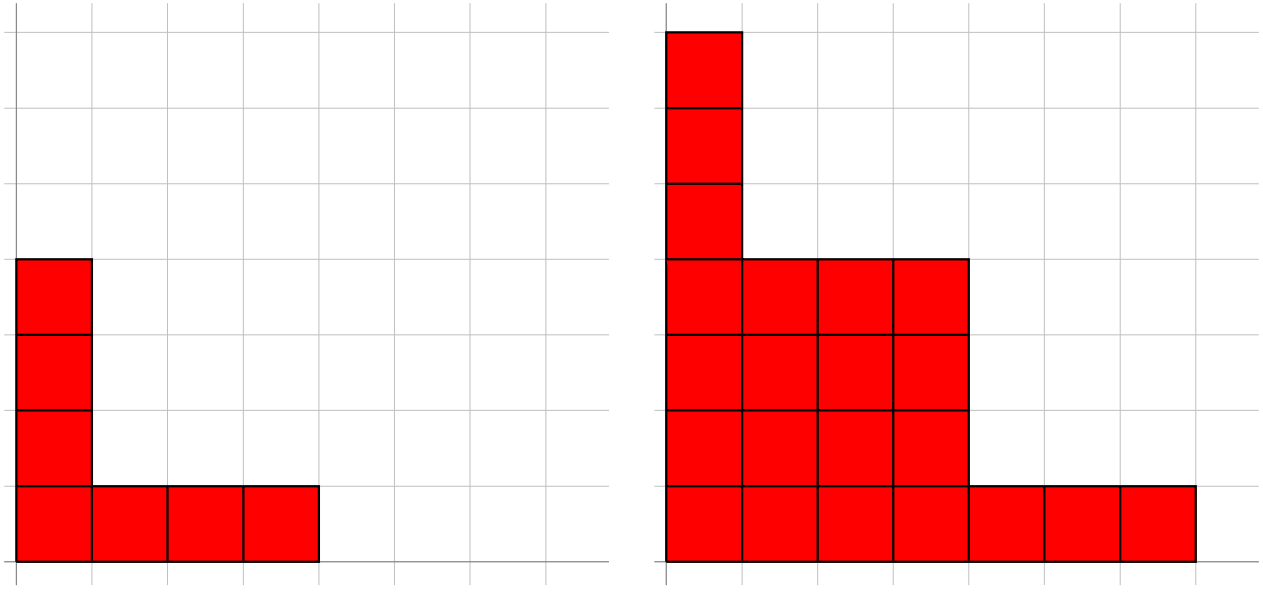


- $S = \{\boldsymbol{x^i} \,||\boldsymbol{i}| \leq d\}, 2\,S = \{\boldsymbol{x^i} \,||\boldsymbol{i}| \leq 2\,d\} \Rightarrow \#(2\,S) \leq 2^n\,\#S.$



Worst case.

$S = \bigcup_{i=1}^{n} \{1, ..., x_i^d\}$, $\#(2\,S) = \frac{n-1}{2\,n}\,(\#S)^2$.



Theorem. [Rusza, 1994]

Set S is included in a n-dimensional parallelotope with $C\,\#S$ points iff. $\#(2\,S) \leq c\,\#S$.

Definition. [Fasino, Tilli 2000, Serra-Capizzano 2002]

A scalar is a multilevel block Hankel matrix of depth 0. Recursively, a multilevel block Hankel matrix has depth $n+1$ if it is a block Hankel matrix where each block is multilevel block Hankel of depth n.

Example.

Scalar-FGLM on $(2^i + (1+j)\,(1+k))_{(i,j,k)\in\mathbb{N}^3}$ with LEX$(x \prec y \prec z)$ returns $I = ((x-1)\,(x-2), (x-1)\,(y-1), (y-1)^2, (x-1)\,(z-1), (z-1)^2)$, with

$$S = \{1, x, y, z, yz\}, \quad H_S = \begin{pmatrix} 2 & 3 & 3 & 3 & 5 \\ 3 & 5 & 4 & 4 & 6 \\ 3 & 4 & 4 & 5 & 7 \\ 3 & 4 & 5 & 4 & 7 \\ 5 & 6 & 7 & 7 & 10 \end{pmatrix}.$$

Definition. [Fasino, Tilli 2000, Serra-Capizzano 2002]

A scalar is a multilevel block Hankel matrix of depth 0. Recursively, a multilevel block Hankel matrix has depth $n+1$ if it is a block Hankel matrix where each block is multilevel block Hankel of depth n.

Example.

Scalar-FGLM on $(2^i + (1+j)\,(1+k))_{(i,j,k)\in\mathbb{N}^3}$ with LEX$(x \prec y \prec z)$ returns $I = ((x-1)\,(x-2), (x-1)\,(y-1), (y-1)^2, (x-1)\,(z-1), (z-1)^2)$, with

$$S = \{1, x, y, z, yz\}, \quad H_S = \left(\begin{array}{cc|c|cc} 2 & 3 & 3 & 3 & 5 \\ 3 & 5 & 4 & 4 & 6 \\ \hline 3 & 4 & 4 & 5 & 7 \\ \hline\hline 3 & 4 & 5 & 4 & 7 \\ \hline 5 & 6 & 7 & 7 & 10 \end{array}\right).$$

Definition. [Fasino, Tilli 2000, Serra-Capizzano 2002]

A scalar is a multilevel block Hankel matrix of depth 0. Recursively, a multilevel block Hankel matrix has depth $n+1$ if it is a block Hankel matrix where each block is multilevel block Hankel of depth n.

Example.

Scalar-FGLM on $(2^i + (1+j)\,(1+k))_{(i,j,k)\in\mathbb{N}^3}$ with LEX$(x \prec y \prec z)$ returns $I = ((x-1)\,(x-2), (x-1)\,(y-1), (y-1)^2, (x-1)\,(z-1), (z-1)^2)$, with

$$S = \{1, x, y, z, yz\}, \quad H_S = \left(\begin{array}{ccc|c|cc} 2 & 3 & 3 & 3 & 5 \\ 3 & 5 & 4 & 4 & 6 \\ \hline 3 & 4 & 4 & 5 & 7 \\ \hline 3 & 4 & 5 & 4 & 7 \\ \hline 5 & 6 & 7 & 7 & 10 \end{array}\right) \subseteq H_{S'} = \begin{array}{c} 1 \\ x \\ \hline y \\ xy \\ \hline z \\ xz \\ \hline yz \\ xyz \end{array} \left(\begin{array}{cccc|cccc} 2 & 3 & 3 & 4 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 4 & 6 & 6 & 7 \\ \hline 3 & 4 & 4 & 5 & 5 & 6 & 7 & 8 \\ 4 & 6 & 5 & 7 & 6 & 7 & 8 & 10 \\ \hline\hline 3 & 4 & 5 & 6 & 4 & 5 & 7 & 8 \\ 4 & 6 & 6 & 7 & 5 & 7 & 8 & 10 \\ \hline 5 & 6 & 7 & 8 & 7 & 8 & 10 & 11 \\ 6 & 7 & 8 & 10 & 8 & 10 & 11 & 13 \end{array}\right).$$

Example.

SCALAR-FGLM on $(2^i + (1+j)\,(1+k))_{(i,j,k)\in\mathbb{N}^3}$ with LEX$(x \prec y \prec z)$ returns $I = ((x-1)\,(x-2), (y-1)\,(x-1), (y-1)^2, (z-1)\,(x-1), (z-1)^2)$, with

$$S = \{1, x, y, z, yz\}, \quad H_S = \left(\begin{array}{ccc|c|cc} 2 & 3 & 3 & 3 & 5 \\ 3 & 5 & 4 & 4 & 6 \\ \hline 3 & 4 & 4 & 5 & 7 \\ \hline 3 & 4 & 5 & 4 & 7 \\ 5 & 6 & 7 & 7 & 10 \end{array}\right) \subseteq H_{S'} = \begin{array}{c} 1 \\ x \\ \hline y \\ xy \\ \hline z \\ xz \\ \hline yz \\ xyz \end{array} \left(\begin{array}{cc|cc|cc|cc} 2 & 3 & 3 & 4 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 4 & 6 & 6 & 7 \\ \hline 3 & 4 & 4 & 5 & 5 & 6 & 7 & 8 \\ 4 & 6 & 5 & 7 & 6 & 7 & 8 & 10 \\ \hline 3 & 4 & 5 & 6 & 4 & 5 & 7 & 8 \\ 4 & 6 & 6 & 7 & 5 & 7 & 8 & 10 \\ \hline 5 & 6 & 7 & 8 & 7 & 8 & 10 & 11 \\ 6 & 7 & 8 & 10 & 8 & 10 & 11 & 13 \end{array}\right).$$

Theorem. [BOSTAN, JEANNEROD, SCHOST 2007]

A quasi-Hankel system of size D and displ. rank α can be solved in $O(\alpha^{\omega-1}\,\mathsf{M}(D)\log D)$.

Proposition.

A multilevel block Hankel of depth n system can be solved in $O(d_n^{\omega-1}\,\mathsf{M}(d_1\cdots d_{n-1})\log(d_1\cdots d_{n-1}))$, with d_i the number of blocks of depth $i-1$.

Highly structured $\rightsquigarrow$ better complexity bound?

Proposition.

A n-dimensional sequence $\boldsymbol{u}$ is linear recurrent over $\mathbb{K}$ with ideal of relations I if and only if its generating series is

$$\frac{N(\boldsymbol{x})}{Q_1(x_1)\cdots Q_n(x_n)} = \frac{\left(Q_1\cdots Q_n \sum_{\boldsymbol{i}=(0,\ldots,0)}^{(d_1-1,\ldots,d_n-1)} u_{\boldsymbol{i}}\,\boldsymbol{x}^{\boldsymbol{i}}\right) \bmod (x_1^{d_1},\ldots,x_n^{d_n})}{Q_1(x_1)\cdots Q_n(x_n)} \in \mathbb{K}(\boldsymbol{x}),$$

where $I\cap\mathbb{K}[x_i]=(P_i)$, $d_i=\deg P_i$ and Q_i is the reverse polynomial of P_i.

Proof Sketch.

- Easily proven for $n=1$: $Q(x)\sum_{i=0}^{\infty} u_i\,x^i = (Q(x)\sum_{i=0}^{d-1} u_i\,x^i) \bmod x^d$, with d degree of P, $I=(P)$.
- Induction of n.

Proposition.

A n-dimensional sequence $\boldsymbol{u}$ is linear recurrent over $\mathbb{K}$ with ideal of relations I if and only if its generating series is

$$\frac{N(\boldsymbol{x})}{Q_1(x_1)\cdots Q_n(x_n)} = \frac{\left(Q_1\cdots Q_n \sum_{\boldsymbol{i}=(0,\ldots,0)}^{(d_1-1,\ldots,d_n-1)} u_{\boldsymbol{i}}\,\boldsymbol{x}^{\boldsymbol{i}}\right) \bmod (x_1^{d_1},\ldots,x_n^{d_n})}{Q_1(x_1)\cdots Q_n(x_n)} \in \mathbb{K}(\boldsymbol{x}),$$

where $I\cap\mathbb{K}[x_i]=(P_i)$, $d_i=\deg P_i$ and Q_i is the reverse polynomial of P_i.

Problem.

- How can we compute $P_1\in\mathbb{K}[x_1],\ldots,P_n\in\mathbb{K}[x_n]$?
- Let d be the degree of I, then $d_1,\ldots,d_n\le d$. Assuming $P_1,\ldots,P_n$, and thus $Q_1,\ldots,Q_n$, are know, computing $N(\boldsymbol{x})$ requires at most $O(n\,d^{n-1}\,\mathsf{M}(d))$ operations in $\mathbb{K}$.

Generating Series Algorithm.

Input: A sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.
Output: The n univariate polynomials $P_1, ..., P_n$.

Compute $\mathcal{G}_1 := \{P_1, P_{1,2}, ..., P_{1,m_1}\}$ with Scalar-FGLM for LEX$(x_1 \prec [x_2, ..., x_n])$.
For k **from** 2 **to** n **do**
  Compute $\mathcal{G}_k := \{P_k, P_{k,2}, ..., P_{k,m_k}\}$ for LEX$(x_k \prec [x_1, ...x_{k-1}, x_{k+1}, x_n])$.
Return $P_1, ..., P_n$.

Better idea!

A subsequence $(u_{i,N_2,...,N_n})_{i \in \mathbb{N}}$ is linear recurrent with P_1 in its ideal of relations.

Idea.

A subsequence $(u_{i,N_2,\dots,N_n})_{i\in\mathbb{N}}$ is linear recurrent with P_1 in its ideal of relations.
P_1 is the lcm of relations of such sequences.
$\rightarrow$ Make a linear combination of such sequences to have P_1 has minimal relation.

Example.

$$\boldsymbol{u} = ((-1)^{ij})_{(i,j)\in\mathbb{N}^2} = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots \\ 1 & -1 & 1 & -1 & \cdots \\ 1 & 1 & 1 & 1 & \cdots \\ 1 & -1 & 1 & -1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \text{ has ideal } \langle x^2-1, y^2-1\rangle.$$

- For N even, subsequence $(u_{i,N})_{i\in\mathbb{N}} = (1)_{i\in\mathbb{N}}$ has ideal $\langle x-1\rangle$.
- For N odd, subsequence $(u_{i,N})_{i\in\mathbb{N}} = ((-1)^i)_{i\in\mathbb{N}}$ has ideal $\langle x+1\rangle$.
- For $\alpha_1, \alpha_2 \in \mathbb{K}^*$, with probability $1/2$, wlog. N_1 is even, N_2 is odd and sequence

$$(\alpha_1\, u_{i,N_1} + \alpha_2\, u_{i,N_2})_{i\in\mathbb{N}} = (\alpha_1 + \alpha_2\,(-1)^i)_{i\in\mathbb{N}}$$

has ideal $\langle x^2-1\rangle$.

Theorem.

Let $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i}\in\mathbb{N}^n}$ be a n-dimensional linear recurrent sequence of order d over $\mathbb{K}$. Fast Generating Series Algorithm computes the n univariate polynomials in $O(n\,\mathsf{M}(d)\log d)$ operations in $\mathbb{K}$ and at most $2\,n\,d^2$ queries to the table.

Fast Generating Series Algorithm.

Input: A sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i}\in\mathbb{N}^n}$.
Output: The n univariate polynomials $P_1, \ldots, P_n$.

For k **from** 1 **to** n **do**
  For ℓ **from** 1 **to** d **do**
    Pick at random $\alpha_\ell \in \mathbb{K}$.
    Pick at random $N_{\ell,1}, \ldots, N_{\ell,k-1}, N_{\ell,k+1}, \ldots, N_{\ell,n} \in \{0, d-1\}$.
  Compute $P_k = \mathsf{BM}((\sum_{\ell=1}^{d} \alpha_\ell\, u_{N_{\ell,1},\ldots,i,\ldots,N_{\ell,n}})_{i\in\mathbb{N}}, d)$.
Return $P_1, \ldots, P_n$.

Proof Sketch.

Each subsequence requires d *rows* of $2\,d$ elements, hence at most $2\,n\,d^2$ queries.
Each call to BM is in $O(\mathsf{M}(d)\log d)$ operations in $\mathbb{K}$.

Sparse-FGLM on Cyclic-n.

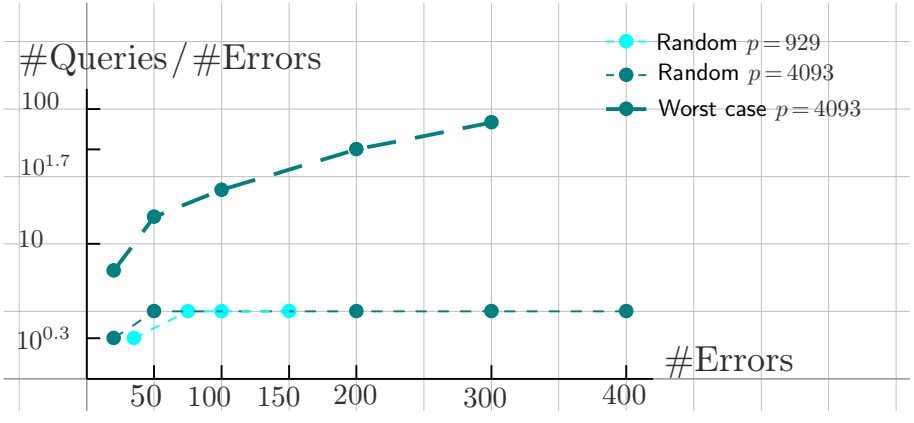
Input: A Gröbner basis $\mathcal{G}_1$ of $I \subseteq \mathbb{K}[\boldsymbol{x}]$ 0-dim. wrt. $\prec_1$ and order $\prec_2$.
Output: A Gröbner basis $\mathcal{G}_2$ of I wrt. $\prec_2$.
Compute multiplication matrices $T_1, \ldots, T_n$ wrt. $x_1, \ldots, x_n$ in $\mathbb{K}[\boldsymbol{x}]/I$.
Pick at random a vector $\boldsymbol{r} = (r_{\mathbf{0}}, \ldots) = ([s]_{\boldsymbol{u}})_{s \in S}$, with S the staircase of $\mathcal{G}_1$.
Compute $\mathcal{G}_2$ with Scalar-FGLM on $\boldsymbol{u} = (\langle \boldsymbol{r}, T_1^{i_1} \cdots T_n^{i_n} \cdot \mathbf{1} \rangle)_{\boldsymbol{i} \in \mathbb{N}^n}$ for $\prec_2$.
If $\deg(\langle \mathcal{G}_2 \rangle) = \#S$ **then return** $\mathcal{G}_2$.
Else error "Not Gorenstein"

$\rightarrow$ n equations in n variables of degree $1, \ldots, n$.

Cyclic-n	D	#Ranks	#Queries$/(2^{n-1} D)$
Cyclic-5	70	76	0.5
Cyclic-6	156	167	0.3
Cyclic-7	924	953	0.3

Coding Theory: n-dimensional cyclic codes.

$\rightarrow$ Sparse interpolation in $\mathbb{F}_p[\boldsymbol{x}]/(x_1^{p-1} - 1, \ldots, x_n^{p-1} - 1)$ at points $(a^{i_1}, \ldots, a^{i_n})$, $\langle a \rangle = \mathbb{F}_p^*$.
$\rightarrow$ Goal: recover the support of the error polynomial.



Conclusion.

- Definition of linear recurrent n-dimensional sequences with constant coefficients.
- Algorithms to compute the ideal of relations.
- Estimation of the number of table queries for these algorithms.
- Computation of the generating series.

Prospectives.

- Extension of these algorithms for the holonomic (P-recursive) n-dimensional sequences.
- Is Scalar-FGLM a matrix version of BMS?

Thank you for your attention!

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$.

Proof Sketch.

For any $\boldsymbol{i} \in \mathbb{N}^n$, let $u_{\boldsymbol{i}} = [\mathrm{NF}(\boldsymbol{x}^{\boldsymbol{i}}, \mathcal{G})]_{\boldsymbol{u}}$.

Example.

From $u_0 = a \neq 0, u_1 = b$ and $J = (x^2)$, we build the table

$$(\ a \ \ b \ \ 0 \ \ 0 \ \ \cdots \ ).$$

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$.

Proof Sketch.

For any $\boldsymbol{i} \in \mathbb{N}^n$, let $u_{\boldsymbol{i}} = [\mathrm{NF}(\boldsymbol{x}^{\boldsymbol{i}}, \mathcal{G})]_{\boldsymbol{u}}$.

Example.

From $u_0 = a \neq 0, u_1 = b$ and $J = (x^2)$, we build the table

$$(\ a \ \ b \ \ 0 \ \ 0 \ \ \cdots \ ).$$

Its ideal of relation contains a polynomial of degree 1, if $\exists (\alpha, \beta) \neq (0,0) \in \mathbb{K}^2$ such that $\alpha\, a + \beta\, b = 0$ and $\alpha\, b + \beta\, 0 = 0$.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$.

Proof Sketch.

For any $\boldsymbol{i} \in \mathbb{N}^n$, let $u_{\boldsymbol{i}} = [\mathrm{NF}(\boldsymbol{x}^{\boldsymbol{i}}, \mathcal{G})]_{\boldsymbol{u}}$.

Example.

From $u_0 = a \neq 0, u_1 = b$ and $J = (x^2)$, we build the table

$$(\; a \;\; b \;\; 0 \;\; 0 \;\; \cdots \;).$$

Its ideal of relation contains a polynomial of degree 1, if $\exists (\alpha, \beta) \neq (0,0) \in \mathbb{K}^2$ such that $\alpha\, a + \beta\, b = 0$ and $\alpha\, b + \beta\, 0 = 0$.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$.

Proof Sketch.

For any $\boldsymbol{i} \in \mathbb{N}^n$, let $u_{\boldsymbol{i}} = [\mathrm{NF}(\boldsymbol{x}^{\boldsymbol{i}}, \mathcal{G})]_{\boldsymbol{u}}$.

Example.

From $u_0 = a \neq 0, u_1 = b$ and $J = (x^2)$, we build the table

$$(\; a \;\; b \;\; 0 \;\; 0 \;\; \cdots \;).$$

Its ideal of relation contains a polynomial of degree 1, if $\exists (\alpha, \beta) \neq (0,0) \in \mathbb{K}^2$ such that $\alpha\, a + \beta\, b = 0$ and $\alpha\, b + \beta\, 0 = 0$.
$\rightarrow$ Thus, if $b \neq 0$, then $I = (x^2) = J$.
$\rightarrow$ If $b = 0$, then $I = (x)$.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Example.

From $u_{0,0} = a \neq 0, u_{1,0} = b, u_{0,1} = c$ and $J = (x^2, x\,y, y^2)$, we build the table

$$\begin{pmatrix} a & c & 0 & 0 & \cdots \\ b & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Its ideal of relation contains a polynomial of degree 1, if $\exists (\alpha, \beta, \gamma) \neq (0,0,0) \in \mathbb{K}^3$ such that $\alpha\,a + \beta\,b + \gamma\,c = 0$, $\alpha\,b + \beta\,0 + \gamma\,0 = 0$ and $\alpha\,c + \beta\,0 + \gamma\,0 = 0$.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Example.

From $u_{0,0} = a \neq 0, u_{1,0} = b, u_{0,1} = c$ and $J = (x^2, x\,y, y^2)$, we build the table

$$\begin{pmatrix} a & c & 0 & 0 & \cdots \\ b & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Its ideal of relation contains a polynomial of degree 1, if $\exists (\alpha, \beta, \gamma) \neq (0,0,0) \in \mathbb{K}^3$ such that $\alpha\,a + \beta\,b + \gamma\,c = 0$, $\alpha\,b + \beta\,0 + \gamma\,0 = 0$ and $\alpha\,c + \beta\,0 + \gamma\,0 = 0$.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Example.

From $u_{0,0} = a \neq 0, u_{1,0} = b, u_{0,1} = c$ and $J = (x^2, x\,y, y^2)$, we build the table

$$\begin{pmatrix} a & c & 0 & 0 & \cdots \\ b & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Its ideal of relation contains a polynomial of degree 1, if $\exists (\alpha, \beta, \gamma) \neq (0,0,0) \in \mathbb{K}^3$ such that $\alpha\,a + \beta\,b + \gamma\,c = 0$, $\alpha\,b + \beta\,0 + \gamma\,0 = 0$ and $\alpha\,c + \beta\,0 + \gamma\,0 = 0$.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Example.

From $u_{0,0} = a \neq 0, u_{1,0} = b, u_{0,1} = c$ and $J = (x^2, x\,y, y^2)$, we build the table

$$\begin{pmatrix} a & c & 0 & 0 & \cdots \\ b & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Its ideal of relation contains a polynomial of degree 1, if $\exists (\alpha, \beta, \gamma) \neq (0,0,0) \in \mathbb{K}^3$ such that $\alpha\,a + \beta\,b + \gamma\,c = 0$, $\alpha\,b + \beta\,0 + \gamma\,0 = 0$ and $\alpha\,c + \beta\,0 + \gamma\,0 = 0$.

Theorem.

Let $\mathcal{G} \subseteq \mathbb{K}[\boldsymbol{x}]$ be a Gröbner basis of an ideal J and let S be its staircase. Given $\{[s]_{\boldsymbol{u}} | s \in S\}$, one can make a unique linear recurrent sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$.

Furthermore, I the ideal of relations of $\boldsymbol{u}$ satisfies $J \subseteq I$ and is Gorenstein (*i.e.* $R = \mathbb{K}[\boldsymbol{x}]/I$ is R-isomorphic to its dual) [Brachat, *et al.* 2010]).

Example.

From $u_{0,0} = a \neq 0, u_{1,0} = b, u_{0,1} = c$ and $J = (x^2, x\,y, y^2)$, we build the table

$$\begin{pmatrix} a & c & 0 & 0 & \cdots \\ b & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Its ideal of relation contains a polynomial of degree 1, if $\exists (\alpha, \beta, \gamma) \neq (0,0,0) \in \mathbb{K}^3$ such that $\alpha\,a + \beta\,b + \gamma\,c = 0$, $\alpha\,b + \beta\,0 + \gamma\,0 = 0$ and $\alpha\,c + \beta\,0 + \gamma\,0 = 0$.
$\rightarrow$ Thus, if $b \neq 0$ and $c \neq 0$, then $I = \left(x - \frac{c}{b}\,y, y^2\right) \supsetneq J$.
$\rightarrow$ If $b = 0$ (resp. $c = 0$, $b = c = 0$), then $I = (x, y^2)$, (resp. $I = (x^2, y)$, $I = (x, y)$).