Algèbre linéaire dédiée pour les algorithmes Scalar-FGLM et Berlekamp-Massey-Sakata

Vincent Guisse

Algèbre linéaire dédiée pour les algorithmes Scalar-FGLM et Berlekamp-Massey-Sakata

Vincent GUISSE
Encadré par Jean-Charles FAUGÈRE
et Jérémy Berthomieu, UPMC-LIP6-POLSYS

17 août 2016

Le contexte général

L'algorithme de Berlekamp-Massey ([1], [11]) a été inventé par Berlekamp pour décoder les codes BCH ([5]), puis Massey a montré qu'il permettait de résoudre le problème de devinette de récurrence linéaire pour les suites à un indice. Il a ensuite été étendu par Sakata ([13]) pour résoudre le même problème pour les suites à plusieurs indices (algorithme de Berlekamp-Massey-Sakata, ou BMS). La solution prend alors la forme d'une base de Gröbner de l'idéal des relations d'une table de valeurs de la suite. Il a enfin été légèrement adapté pour permettre le décodage des codes d'évaluations sur un domaine ordonné ([6]).

Récemment, dans [3], Faugère, Berthomieu et Boyer on présenté un algorithme, Scalar-FGLM, généralisant la version matricielle de l'algorithme de Berlekamp-Massey pour les suites à plusieurs indices. Cette dernière consiste à résoudre un système linéaire de Hankel de taille d, l'ordre de la récurrence. Ceci est possible en complexité en temps $O(\mathbf{M}(d)\log d)$, où $\mathbf{M}(d)$ est le coût du produit de polynômes de degré d (voir [7]). Dans le cas de Scalar-FGLM, on extrait une sous matrice de rang maximal d'une matrice multi-Hankel puis on résout des systèmes faisant intervenir directement cette matrice. Cela est possible en complexité $O(\mathbf{M}(d)\log d)$ pour l'ordre lexicographique et dans le cas générique (shape position). Cependant, sans cette hypothèse de généricité on ne sait pas résoudre le système linéaire aussi efficacement.

Dans [4], les auteurs de Scalar-FGLM l'étendent aux suites linéaires récurrentes à coefficients polynomiaux, les suites P-récurrentes. Le problème ouvert de savoir si certaines marches de l'espaces sont P-récurrentes ou non pourrait se voir apporter des réponses en cas de progrès pratiques ou théoriques dans la gestion des matrices générées par Scalar-FGLM.

Le problème étudié

Un premier objectif du stage était d'obtenir une algèbre linéaire plus rapide en pratique ou en théorie pour Scalar-FGLM et ses dérivés. Un second était de rapprocher les descriptions de Scalar-FGLM et de BMS, puisque ces deux algorithmes ont des sorties équivalentes.

La contribution proposée

Dans le but d'obtenir une algèbre linéaire plus rapide pour Scalar-FGLM et ses dérivés, nous avons tenté d'étendre l'algorithme du demi-PGCD en dimension supérieure. Ceci nous a amené à une formulation polynomiale de l'algèbre linéaire de Scalar-FGLM, mais qui n'a pas débouché sur un algorithme efficace.

Par ailleurs nous avons spécialisé la version de BMS qui est donnée dans [6] pour la localisation d'erreur des codes d'évaluation sur un domaine ordonné. Nous l'avons appliquée à la devinette de récurrence linéaire multidimensionnelle, ce qui revenait à se placer dans le cadre d'un anneau de polynômes multivariés muni d'un ordre du degré. Ce travail a été accompagné d'une implémentation en Maple, et il a permis d'identifier des différences fondamentales entre Scalar-FGLM et BMS.

Les arguments en faveur de sa validité

Notre formulation polynomiale de l'algèbre linéaire de Scalar-FGLM est bien une généralisation directe de la formulation polynomiale en dimension 1, qui mène à une solution efficace avec l'algorithme du demi-PGCD.

Notre spécialisation de BMS a été implémentée et testée. Elle repose sur une présentation de BMS (dans [6]) de lecture probablement plus accessible que la version originale de Sakata, mais qui nécessitait une traduction dans le langage des polynômes pour être directement exploitée par les non spécialistes de la théorie des codes correcteurs.

Le bilan et les perspectives

Nous n'avons pas trouvé d'algèbre linéaire dédiée efficace pour Scalar-FGLM et ses dérivés. Cependant nous proposons une formulation polynomiale de cette algèbre linéaire qui peut être un point de départ pour un tel algorithme, analogue au demi-PGCD.

Notre réécriture de BMS dans le langage des polynômes et son implémentation en Maple ont permis de rapprocher les descriptions de Scalar-FGLM et de BMS, la question reste cependant ouverte de savoir si ces algorithmes effectuent les mêmes calculs. Pour y répondre il est nécessaire d'expliciter une version itérative de Scalar-FGLM.

1 Problème, contexte

1.1 Suites récurrentes linéaires, tables

Nous présentons dans cette partie les suites récurrentes linéaires à coefficients constants à un ou à plusieurs indices, et les problèmes de devinette de récurrence sur des tables (finies) de valeurs de ces suites.

1.1.1 Suites unidimensionnelles

Dans un corps $\mathbb{K}$, une suite $u = (u_i)_{i\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ est récurrente linéaire à coefficients constants si et seulement s'il existe un entier d et des coefficients $(\alpha_k)_{k\in\{0,\dots,d-1\}}$ dans $\mathbb{K}$ tels que :

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

Ainsi, $(u_i)_{i\in\mathbb{N}}$ est déterminée par la donnée de ses d premiers termes et la relation (1). Le plus petit d satisfaisant la relation (1) est appelé l'ordre de la suite linéaire récurrente u.

Si on connaît seulement la table $(u_0, u_1, \dots, u_{N-1})$ des N premiers termes de la suite u, on peut rechercher un entier L_N et des coefficients $(\alpha_k)_{k\in\{0,\dots,L_N-1\}}$ tels que

$$\forall i \in \mathbb{N},\ L_{N+i} \leq N-1 \Rightarrow u_{L_N+i} + \sum_{k=0}^{L_N-1} \alpha_k u_{k+i} = 0. \tag{2}$$

Formellement, il s'agit de résoudre le problème suivant :

Problème 1. *Devinette de récurrence linéaire simple*

Entrées : *La table $(u_0, u_1, \dots, u_{N-1})$ des N premiers termes d'une suite.*

Sorties : *Le plus petit entier L_N et des coefficients $(\alpha_k)_{k\in\{0,\dots,L_N-1\}}$ vérifiant la relation (2).*

Observons sur un exemple élémentaire différents cas de figure :

Exemple 1. *Soit $(u_i)_{i\in\mathbb{N}}$ la suite de Fibonacci, définie par $u_0 = 0$, $u_1 = 1$ et pour tout $i \in \mathbb{N}$, $u_{i+2} = u_{i+1} + u_i$. Alors on a :*

- *Pour $N = 1$ et la table (0), $L_1 = 0$ et il n'y a pas de coefficients.*
- *Pour $N = 2$ et la table $(0, 1)$, $L_2 = 2$ et tous les couples (α_0, α_1) de coefficients conviennent.*
- *Pour $N = 3$ et la table $(0, 1, 1)$, $L_3 = 2$ et on peut prendre α_0 arbitraire pourvu que $\alpha_1 = -1$.*
- *Pour $N = 4$ et la table $(0, 1, 1, 2)$, $L_4 = 2$ et les seuls coefficients possibles sont $\alpha_0 = -1$ et $\alpha_1 = -1$. De même pour tout $N > 4$.*

On remarque dans cet exemple que contrairement à L_N, les coefficients (α_k) ne sont pas nécessairement uniques (par exemple pour $N = 3$). En particulier dans le cas $L_N = N$, tous les coefficients conviennent et d'une certaine façon « il n'y a pas de relation de récurrence » pour lier les termes connus de la suite.

1.1.2 Suites multidimensionnelles

On va généraliser ce qui précède aux suites à plusieurs indices. Soit $n \geq 1$, on note $\mathbf{i} = (i_1, \ldots, i_n) \in \mathbb{N}^n$. Soit $u = (u_{\mathbf{i}})_{\mathbf{i} \in \mathbb{N}^n}$ une suite à n indices d'éléments de $\mathbb{K}$. S'il existe une partie finie $\mathcal{K} \subset \mathbb{N}^n$ et des coefficients non tous nuls $(\alpha_{\mathbf{k}})_{\mathbf{k} \in \mathcal{K}}$ tels que

$$\forall \mathbf{i} \in \mathbb{N}^n, \sum_{\mathbf{k} \in \mathcal{K}} \alpha_{\mathbf{k}} u_{\mathbf{k}+\mathbf{i}} = 0, \tag{3}$$

alors la relation (3) est appelée une relation de récurrence linéaire multidimensionnelle de support $\mathcal{K}$.

Exemple 2. *La suite* $b = \left(\binom{i}{j}\right)_{(i,j) \in \mathbb{N}^2}$ *des coefficients binomiaux vérifie la relation de Pascal :*

$$\forall (i,j) \in \mathbb{N}^2, \, b_{i+1,j+1} - b_{i,j+1} - b_{i,j} = 0.$$

Ces relations permettent de définir les suites linéaires récurrentes multidimensionnelles à coefficients constants par analogie avec ce qui se passe en dimension 1 (voir [3]) :

Définition 1. *La suite* $(u_{\boldsymbol{i}})_{\boldsymbol{i} \in \mathbb{N}^n}$ *est récurrente linéaire n-dimensionnelle à coefficients constants lorsqu'on peut calculer sans contradiction tous les termes de la suite à partir d'un nombre fini de termes initiaux et d'un nombre fini de relations de récurrence linéaire multidimensionnelles à coefficients constants.*

La suite des coefficients binomiaux de l'exemple 2 n'est pas récurrente linéaire à coefficients constants car malgré la relation de Pascal, on ne peut pas déduire toutes les relations $b_{i,0} = \binom{0}{i} = 0$ pour $i \geq 1$ et $b_{0,j} = \binom{j}{0} = 1$ avec un nombre fini de conditions initiales. Elle est cependant P-récurrente, c'est à dire récurrente linéaire à coefficients polynomiaux.

Exemple 3. *La suite* u *définie sur* $\mathbb{N}^2$ *par* $u_{i,j} = 2^i \cdot 3^j$ *vérifie les relations* $u_{i+1,j} - 2u_{i,j} = 0$ *et* $u_{i,j+1} - 3u_{i,j} = 0$. *La donnée de* $u_{0,0} = 1$ *permet avec ces deux relations de calculer sans contradiction tous les termes de la suite* u, *comme on le voit en raisonnant par récurrence sur* $i + j$.

Quand on connaît seulement la table constituée des termes $u_{\mathbf{i}}$ tels que $|\mathbf{i}| = i_1 + i_2 + \cdots + i_n \leq 2d+1$, on peut rechercher une partie $S \in \mathbb{N}^n$ et des relations de récurrence permettant de générer cette table.

Problème 2. *Devinette de récurrence linéaire multidimensionnelle*

Entrées : *Une borne* $d \in \mathbb{N}$ *et la table* $(u_{\boldsymbol{i}})_{|\boldsymbol{i}| \leq 2d+1}$ *des* $(2d+1)^n$ *« premiers » termes d'une suite multidimensionnelle.*

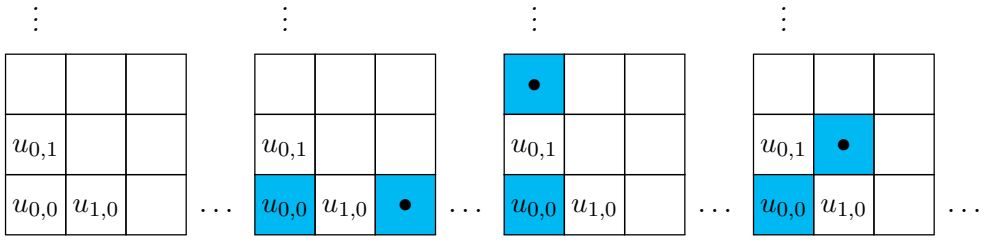
Sorties : *Une partie* $S \subset \mathbb{N}^n$ *d'indices de termes initiaux à connaître et des relations permettant de générer toute la table sans contradiction.*

La définition 1 suggère deux difficultés par rapport au cas unidimensionnel.

La première, rencontrée pour l'exemple 2 de la suite des coefficients binomiaux, est la possibilité de calculer tous les termes à partir d'un nombre finis de conditions initiales et de relations toutes données au départ.

La seconde est la non contradiction des calculs et peut être discutée sur l'exemple suivant, traité dans [14] page 147 et repris dans [3].

Exemple 4. *Soit* $u = (u_{i,j})_{(i,j)\in\mathbb{N}^2}$ *définie par la donnée des termes initiaux* $S = \{u_{0,0}, u_{0,1}, u_{1,0}\}$ *et les relations, pour tous* $(i,j) \in \mathbb{N}^2$, $\{u_{i+2,j} + u_{i,j} = 0, u_{i+1,j+1} + u_{i,j} = 0, u_{i,j+2} + u_{i,j} = 0\}$.



Si on se donne un ordre $\prec$ *de parcours des indices* $(i,j) \in \mathbb{N}^2$, *par exemple*

$$(i,j) \prec (i',j') \Leftrightarrow i + j < i' + j' \text{ ou } (i + j = i' + j' \text{ et } i < j),$$

il est clair qu'on peut parcourir les termes dans cet ordre et les calculer successivement : avec la première relation si l'on se trouve sur le bord inférieur de la table, avec la dernière si l'on se trouve sur le bord latéral gauche, et avec n'importe laquelle des trois sinon. Par contre rien ne garantit a priori que dans ce dernier cas les trois calculs donneront la même valeur. En particulier, on peut combiner la première et la troisième relation pour obtenir successivement, pour tous $(i,j) \in \mathbb{N}^2$ *:* $u_{i+2,j+1} + u_{i,j+1} = 0$ *par translation de la première relation, et* $u_{i+2,j+1} + u_{i+1,j} = 0$ *par translation de la troisième, donc* $u_{i,j+1} - u_{i+1,j} = 0$ *par soustraction de ces deux dernières relations. On en déduit que si* $u_{0,1} - u_{1,0} \neq 0$, *les calculs donnent des contradictions.*

Pour « réparer » l'exemple précédent, il suffit de restreindre S en prenant $S = \{u_{0,0}, u_{0,1}\}$, et l'ensemble de relations $\{u_{i+2,j+1} + u_{i,j+1} = 0, u_{i,j+1} - u_{i+1,j} = 0\}$. Le problème venait du fait que l'ensemble des relations permettait, par combinaison, de générer une relation de support « trop petit » par rapport au support S des conditions initiales, choisi de manière trop hâtive par rapport au support des relations.

Plus généralement, une interprétation polynomiale des relations va permettre de ramener les difficultés de la définition 1 aux notions de base de Gröbner et d'escalier d'une base de Gröbner d'un idéal zéro dimensionnel.

1.2 Interprétation polynomiale, idéal des relations

On va associer à une suite multidimensionnelle un ensemble de polynômes multivariés correspondant aux relations de récurrence linéaire vérifiées par la suite.

Définition 2. *Soit* $f(\boldsymbol{x}) = \sum_{\boldsymbol{k}\in\mathcal{K}} \alpha_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \in \mathbb{K}[\boldsymbol{x}]$. *On note* $[f]_u = \sum_{\boldsymbol{k}\in\mathcal{K}} \alpha_{\boldsymbol{k}} u_{\boldsymbol{k}}$ *de sorte que*

$$\forall \boldsymbol{i} \in \mathbb{N}^n,\ \left[x^{\boldsymbol{i}} f\right]_u = 0 \Leftrightarrow \forall \boldsymbol{i} \in \mathbb{N}^n,\ \sum_{\boldsymbol{k}\in\mathcal{K}} \alpha_{\boldsymbol{k}} u_{\boldsymbol{k}+\boldsymbol{i}} = 0.$$

Lorsque cela a lieu, on dit que f *est le polynôme de la relation* $(\alpha_{\boldsymbol{k}})_{\boldsymbol{k}\in\mathcal{K}}$ *pour la suite* u.

Ainsi pour l'exemple 2, le polynôme de la relation $b_{i+1,j+1} - b_{i,j+1} - b_{i,j} = 0$ est $P(x, y) = xy - y - 1$.

Dans la suite et en suivant [14] on identifiera un polynôme et la relation correspondante.

Proposition 1. *L'ensemble* $\mathcal{I}_u$ *des polynômes de relations de la suite* u *est un idéal de* $\mathbb{K}[\boldsymbol{x}]$.

Démonstration. Soit $\mathcal{A}$ l'ensemble des suites n-dimensionnelles, alors

$$\begin{array}{rccl} \Phi_u & : & \mathbb{K}[\mathbf{x}] & \to \mathcal{A} \\ & & P & \mapsto \left(\left[\mathbf{x}^{\mathbf{i}} P\right]_u\right)_{\mathbf{i}\in\mathbb{N}^n} \end{array}$$

est un morphisme de $\mathbb{K}$-espaces vectoriels, de noyau $\mathcal{I}_u$ qui est donc un sous espace de $\mathbb{K}[\mathbf{x}]$. De plus, pour $P \in \mathbb{K}[\mathbf{x}]$ il est clair que pour tout $\mathbf{i} \in \mathbb{N}^n$, si $\Phi_u(P) = 0_{\mathcal{A}}$ alors $\Phi_u(x^{\mathbf{i}} P) = 0_{\mathcal{A}}$, ce qui donne par linéarité que $\mathcal{I}_u$ est bien un idéal de $\mathbb{K}[\mathbf{x}]$. □

On a de plus une caractérisation simple des suites récurrentes linéaires multidimensionnelles à coefficients constants telles que nous les avons définies en suivant [3].

Proposition 2. *La suite* u *est récurrente linéaire multidimensionnelle à coefficients constants si et seulement si son idéal des relations est zéro dimensionnel. Dans ce cas, les relations permettant de calculer tous les termes de la suite peuvent correspondre à une base de Gröbner de l'idéal des relations* $\mathcal{I}_u$ *pour un ordre monomial donné, et les termes initiaux à connaître peuvent correspondre à l'escalier fini de cette base.*

Démonstration. Si u est récurrente linéaire multidimensionnelle, soit F la partie finie de $\mathbb{K}[\mathbf{x}]$ telle que $\mathcal{I}_u = (F)$ et $S \subset \mathbb{N}^n$ le support fini de ses conditions initiales. Soit $\mathbf{i} \in \mathbb{N}^n$, comme on peut calculer $u_{\mathbf{i}}$ en utilisant seulement les relations de F et les conditions initiales de support S, alors on a des coefficients $(\alpha_{\mathbf{k}})_{\mathbf{k}\in S}$ tels que $x^{\mathbf{i}} = \sum_{\mathbf{k}\in S} \alpha_{\mathbf{k}} x^{\mathbf{k}} \mod \mathcal{I}_u$, ainsi $\mathbb{K}[\mathbf{x}]/\mathcal{I}_u$ est de dimension finie inférieure à $|S|$ et $\mathcal{I}_u$ est bien zéro dimensionnel.

Réciproquement si $\mathcal{I}_u$ est zéro dimensionnel, soit G une base de Gröbner de I_u pour un ordre monomial $\prec$ et soit $S \in \mathbb{N}^n$ le support fini de son escalier. Prenons les valeurs de u sur S comme conditions initiales, et les éléments de G comme relations. Alors pour $\mathbf{i} \in \mathbb{N}^n$, on peut calculer la forme normale de $\mathbf{x}^{\mathbf{i}}$ par rapport à G et $\prec$, ce qui nous donne des coefficients $(\alpha_{\mathbf{k}})_{\mathbf{k}\in S}$ tels que

$\mathbf{x}^{\mathbf{i}} = \sum_{\mathbf{k}\in S} \alpha_{\mathbf{k}}\mathbf{x}^{\mathbf{k}} \mod \mathcal{I}_u$, on en déduit que $u_{\mathbf{i}} = \sum_{\mathbf{k}\in S} \alpha_{\mathbf{k}} u_{\mathbf{k}}$ peut être calculé. Il reste à montrer que ces calculs ne mènent pas à des contradictions. Par l'absurde, supposons que l'on puisse combiner les relations de G de deux manières différentes pour le calcul de $u_{\mathbf{i}}$, c'est à dire que l'on ait

$$\mathbf{x}^{\mathbf{i}} = \sum_{\mathbf{k}\in S} \alpha_{\mathbf{k}}\mathbf{x}^{\mathbf{k}} = \sum_{\mathbf{k}\in S} \beta_{\mathbf{k}}\mathbf{x}^{\mathbf{k}} \mod \mathcal{I}_u,$$

avec $(\alpha_{\mathbf{k}})_{\mathbf{k}\in S} \neq (\beta_{\mathbf{k}})_{\mathbf{k}\in S}$. Alors $\sum_{\mathbf{k}\in S}(\alpha_{\mathbf{k}} - \beta_{\mathbf{k}})\mathbf{x}^{\mathbf{k}} \in \mathcal{I}_u$ est non nul et de support inclus dans S, son monôme de tête est donc dans $\mathbf{x}^S$ ce qui contredit le fait que S est le support de l'escalier de G. □

On peut revenir sur l'exemple 4 pour illustrer la partie finale de cette preuve. Les relations étaient $F = \{x^2+1 = 0, y^2+1 = 0, xy+1 = 0\}$, et le support des conditions initiales $S = \{(0,0),(1,0),(0,1)\}$. En prenant par exemple l'ordre $\prec$ du degré lexicographique avec $x < y$, S est bien le support de l'escalier correspondant aux monômes de tête des éléments de F. Mais en calculant le S-polynôme de deux éléments de F :

$$y(x^2+1) - x(xy+1) = y - x,$$

on voit que F n'est pas une base de Gröbner pour $\prec$, donc S est trop grand et peut donner lieu à des contradictions dans le calcul des termes.

La notion d'idéal des relations permet de reformuler le problème 2 en utilisant la notion de base de Gröbner.

Problème 3. *Devinette de récurrence linéaire multidimensionnelle, version polynomiale*

Entrées : *Une borne $d \in \mathbb{N}$, la table $(u_{\boldsymbol{i}})_{|\boldsymbol{i}|\leq 2d+1}$ des $(2d+1)^n$ « premiers » termes d'une suite multidimensionnelle, et un ordre monômial $\prec$.*

Sorties : *Une partie $S \in \mathbb{N}^n$ d'indices de termes initiaux à connaître et une base de Gröbner de $\mathcal{I}_u$ pour $\prec$, d'escalier S.*

1.3 Interprétation matricielle

En dimension 1, dire que la suite $u = (u_i)_{i\in\mathbb{N}}$ est récurente d'ordre d peut s'écrire matriciellement :

$$\begin{pmatrix} u_0 & u_1 & u_2 & \dots & u_{d-1} \\ u_1 & u_2 & u_3 & \dots & u_d \\ u_2 & u_3 & u_4 & \dots & u_{d+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} -\alpha_0 \\ -\alpha_1 \\ -\alpha_2 \\ \vdots \\ -\alpha_{d-1} \end{pmatrix} = \begin{pmatrix} u_d \\ u_{d+1} \\ u_{d+2} \\ \vdots \end{pmatrix}, \tag{4}$$

le fait que u soit d'ordre d donnant aussi qu'aucune des colonnes infinies de la matrice à gauche ne soit liée à celles qui la précèdent. On en déduit qu'on peut

extraire une matrice de rang maximal d. Comme la relation (4) lie aussi par symétrie toutes les lignes à partir de la $d+1$-ième aux précédentes et donc aux d premières, la matrice de Hankel

$$H_{d-1} = \begin{pmatrix} u_0 & u_1 & u_2 & \dots & u_{d-1} \\ u_1 & u_2 & u_3 & \dots & u_d \\ u_2 & u_3 & u_4 & \dots & u_{d+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ u_{d-1} & u_d & u_{d+1} & \dots & u_{2d-2} \end{pmatrix}$$

est de rang plein égal à d.

Si on se restreint à la table des N premiers termes de la suite, une solution du problème 1 va s'écrire

$$\begin{pmatrix} u_0 & u_1 & u_2 & \dots & u_{L_N-1} \\ u_1 & u_2 & u_3 & \dots & u_{L_N} \\ u_2 & u_3 & u_4 & \dots & u_{L_N+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ u_{N-L_N-1} & u_{N-L_N} & u_{N-L_N} & \dots & u_{N-2} \end{pmatrix} \begin{pmatrix} -\alpha_0^N \\ -\alpha_1^N \\ -\alpha_2^N \\ \vdots \\ -\alpha_{L_N-1}^N \end{pmatrix} = \begin{pmatrix} u_{L_N} \\ u_{L_N+1} \\ u_{L_N+2} \\ \vdots \\ u_{N-1} \end{pmatrix}, \quad (5)$$

le caractère minimal de L_N assurant que toute extension de la matrice

$$H_{N,\infty} = \begin{pmatrix} u_0 & u_1 & u_2 & \cdots & u_{N-1} & ? \\ u_1 & u_2 & \cdots & u_{N-1} & ? & \\ \vdots & & & & & \\ u_{N-2} & u_{N-1} & ? & & & \\ u_{N-1} & ? & & & & \\ ? & & & & & \end{pmatrix} \quad (6)$$

soit au moins de rang L_N (voir [10]). On peut à présent reformuler le problème 1 :

Problème 4. *Devinette de récurrence linéaire simple, version matricielle*

Entrées : *La table $(u_0, u_1, \dots, u_{N-1})$ des N premiers termes d'une suite.*

Sorties : *Le rang minimal L_N de toutes les extensions de la matrice $H_{N,\infty}$ déterminée par la table en entrée et des coefficients $(\alpha_k)_{k\in\{0,\dots,L_N-1\}}$ solution du système linéaire (5).*

Ainsi les matrices de Hankel

$$H_n = \begin{array}{c} \\ 1 \\ \vdots \\ x^n \end{array} \begin{array}{c} \begin{array}{ccc} 1 & \cdots & x^n \end{array} \\ \begin{pmatrix} u_0 & \cdots & u_n \\ \vdots & & \vdots \\ u_n & \cdots & u_{2n} \end{pmatrix} \end{array} = \begin{array}{c} \\ 1 \\ \vdots \\ x^i \\ \vdots \\ x^n \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & \cdots & x^j & \cdots & x^n \end{array} \\ \begin{pmatrix} & & & & \\ & \ddots & \vdots & \iddots & \\ & \cdots & [x^i x^j]_u & \cdots & \\ & \iddots & \vdots & \ddots & \\ & & & & \end{pmatrix} \end{array}$$

jouent un rôle déterminant, elles sont exploitées dans [10] pour proposer une interprétation de l'algorithme de Berlekamp-Massey, comme on le verra dans la section 2.3.

Dans le cas multidimensionnel, on peut de manière analogue utiliser comme dans [3] des matrices $H_{T,S}$ formées à partir de deux ensembles de monômes T et S de $\mathbb{K}[\mathbf{x}]$ selon

$$H_{T,S} = \begin{array}{c} \\ \vdots \\ \mathbf{x^i} \in T \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccc} \cdots & \mathbf{x^j} \in S & \cdots \end{array} \\ \begin{pmatrix} \ddots & \vdots & \iddots \\ \cdots & [\mathbf{x^i x^j}]_u & \cdots \\ \iddots & \vdots & \ddots \end{pmatrix} \end{array}$$

dont le rang sera utile dans l'algorithme Scalar -FGLM.

2 Solutions en Dimension 1

2.1 Demi-PGCD

Si on note $H(x) = \sum_{i \in \mathbb{N}} u_i x^i$ la série génératrice de la suite linéaire récurrente u d'ordre d et de relation

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

en notant $C(x) = 1 + \sum_{k=0}^{d-1} \alpha_k x^{d-k}$ le polynôme réciproque du polynôme de la relation, on observe que

$$\begin{aligned} H(x)C(x) &= (\sum_{i \in \mathbb{N}} u_i x^i)(1 + \sum_{k=0}^{d-1} \alpha_k x^{d-k}) \\ &= u_0 + \cdots + (u_{d-1} + \sum_{k=1}^{d-1} \alpha_k u_{d-1-k}) x^{d-1} + \sum_{i \geq d} \left(u_i + \sum_{k=0}^{d-1} \alpha_k u_{i-d+k} \right) x^i \\ &= u_0 + \cdots + (u_{d-1} + \sum_{k=1}^{d-1} \alpha_k u_{d-1-k}) x^{d-1} \\ &= R(x),\ \text{avec } deg(R(x)) \leq d-1. \end{aligned}$$

Autrement dit, on a $H(x) = \dfrac{R(x)}{C(x)}$, avec C de degré inférieur à d et R de degré inférieur à $d-1$.

En notant $H_N(x) = \sum_{i=0}^{N-1} u_i x^i$ pour tenir compte des données du problème 1, on est amené à chercher à résoudre

$$H_N(x)C_N(x) = R_N(x) \mod x^N \tag{7}$$

avec $L_N = \max\{deg(C_N(x)),\, deg(R_N(x)) + 1\}$ minimal.

Dans [12] il est montré que toutes les solutions de (7) avec $deg(C_N) + deg(R_N) < N$ sont obtenues avec les cofacteurs successifs de l'algorithme d'Euclide étendu. Ainsi, pour résoudre le problème (1), il suffit de calculer les cofacteurs du demi-PGCD de $H_N(x)$ et de x^N.

Lors de ce stage, nous avons tenté, sans succès, d'étendre cette solution en dimension supérieure, comme nous le verrons à la section 3.3.

2.2 Berlekamp Massey

L'algorithme de Berlekamp-Massey ([2], [11]) a été initialement inventé par Berlekamp pour décoder les codes BCH. Massey a ensuite montré qu'il permettait de résoudre le problème 1 de devinette de récurrence linéaire, et il s'avère qu'il est équivalent à l'algorithme du demi-PGCD présenté dans la section précédente (voir [8]). Il s'agit de déterminer la longueur L_N et des coefficients $(\alpha_k)_{k\in\{0,\dots,N-1\}}$ d'une relation de récurrence permettant de générer les N premiers termes de manière itérative (on itère sur le nombre de termes connus de la suite $(u_i)_{i\in\mathbb{N}}$).

Dans [11], Lemma 1, il est d'abord établi la proposition suivante.

Proposition 3. *Si une relation de longueur L_N génère la table $(u_i)_{i\in\{0,\dots,N-1\}}$ mais pas la table $(u_i)_{i\in\{0,\dots,N\}}$, alors on a*

$$L_{N+1} \geq \max\{L_N, N + 1 - L_N\}. \tag{8}$$

L'égalité dans (8) est ensuite obtenue effectivement par le pas d'itération de l'algorithme de Berlekamp-Massey, qui combine la solution connue au rang N et qui échoue à générer aussi u_N avec une solution « auxiliaire » du plus grand problème de rang inférieur et dont la longueur de la solution est inférieure à L_N, pour obtenir une relation de longueur optimale $\max\{L_N, N + 1 - L_N\}$ générant la table $(u_i)_{i\in\{0,\dots,N\}}$. Nous ne le présentons pas en détail car il a déjà été généralisé par Sakata dans [13] pour résoudre le cas multidimensionnel (problème 3). Nous renvoyons plutôt à la description de la section 3.1, où la quantité $N + 1 - L_N$ est généralisée sous le nom de *span*.

2.3 Interprétation matricielle de Berlekamp Massey

Dans [10], l'algorithme de Berlekamp-Massey est interprété dans le point de vue matriciel présenté à la section 1.3. Autrement dit, il s'agit de résoudre le problème 4. L'égalité $L_N = \max\{L_N, N + 1 - L_N\}$ dans (8) est obtenue cette fois ci indépendemment du pas d'itération de l'algorithme de Berlekamp-Massey, par des considérations sur le rang de matrices de Hankel.

3 Solutions en dimensions supérieures

3.1 Berlekamp Massey Sakata

Dans le but de rapprocher les descriptions de Scalar-FGLM et de BMS, nous spécialisons à $\mathbb{K}[\mathbf{x}]$ la version de BMS donnée dans [6] dans le cadre plus général des domaines ordonnés.

Il s'agit de résoudre le problème 3. On se donne donc un entier d, la table $(u_{\mathbf{i}})_{|\mathbf{i}|\leq 2d+1}$ et un ordre monômial du degré total $\prec$. On note $\mathcal{T}_0 = \{\mathbf{x}^{\mathbf{i}}, \mathbf{i} \in \mathbb{N}^n\} \cup \{0\}$ et on prolonge l'ordre total $\prec$ (qu'on continue de noter $\prec$) sur $\mathcal{T}_0$ en convenant que $0 \prec 1$.

On va itérer sur les monômes $m \in \{\mathbf{x}^{\mathbf{i}}, |\mathbf{i}| < 2d+1\}$, en ne considérant à chaque étape que la table $([\mathbf{x}^{\mathbf{i}}]_u)_{\mathbf{x}^{\mathbf{i}} \preceq m}$. On est donc amené à définir des notions tenant compte du caractère partiel de notre connaissance de u à l'étape m.

Définition 3. *Soit $m \in \mathcal{T}_0$. Soit $f \in \mathbb{K}[\boldsymbol{x}]$, lorsque*

$$\forall t \in \mathcal{T}_0,\ LT(tf) \preceq m \Rightarrow [tf]_u = 0, \tag{9}$$

on dit que la relation f est vraie jusqu'à m. Sinon, lorsque

$$\forall t \in \mathcal{T}_0,\ tf \prec m \Rightarrow [tf]_u = 0 \text{ et } [\frac{m}{LT(f)} f]_u \neq 0,$$

on dit que la relation f échoue en m et on définit

$$fail(f) = m \tag{10}$$

$$span(f) = \frac{m}{LT(f)} \tag{11}$$

$$disc(f) = [span(f)f]_u. \tag{12}$$

Enfin, si f est une relation de I_u on convient que $fail(f) = +\infty$.

Par linéarité, on obtient facilement les caractérisations suivantes :

Proposition 4. *Avec les notations de la définition 3, on a :*

$$fail(f) \succ m \Leftrightarrow \forall g \in \mathbb{K}[\boldsymbol{x}],\ LT(gf) \preceq m \Rightarrow [gf]_u = 0 \tag{13}$$

$$span(f) = s \Leftrightarrow \forall g \in \mathbb{K}[\boldsymbol{x}],\ \begin{cases} LT(g) \prec s & \Rightarrow [gf]_u = 0 \\ LT(g) = s & \Rightarrow [gf]_u \neq 0 \end{cases} \tag{14}$$

Démonstration. Pour montrer (13), supposons que $\text{fail}(f) \succ m$. Si $\text{fail}(f) = +\infty$, alors $f \in \mathcal{I}_u$ et on a pour tout $g \in \mathbb{K}[\mathbf{x}]$ que $[gf]_u = 0$. Sinon, soit $m' = \text{fail}(m) \succ m$ et $g = \sum_{\mathbf{x}^{\mathbf{i}} \preceq \text{LT}(g)} g_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \in \mathbb{K}[\mathbf{x}]$ avec $\text{LT}(gf) \prec m'$, alors $[gf]_u = \sum_{\mathbf{x}^{\mathbf{i}} \preceq \text{LT}(g)} g_{\mathbf{i}} \left[\mathbf{x}^{\mathbf{i}} f\right]_u = 0$, car pour $\mathbf{x}^{\mathbf{i}} \preceq \text{LT}(g)$, $\text{LT}(\mathbf{x}^{\mathbf{i}} f) \prec m'$. La réciproque est directe en prenant $g = \mathbf{x}^{\mathbf{i}}$. Pour (14), supposons que $\text{span}(f) = s$. Alors pour tout $\mathbf{x}^{\mathbf{i}} \prec s$, $[\mathbf{x}^{\mathbf{i}} f]_u = 0$ et par linéarité on a que pour tout $g \in \mathbb{K}[\mathbf{x}]$ avec $\text{LT}(g) \prec s$, $[gf]_u = 0$. Soit à présent $g \in \mathbb{K}[\mathbf{x}]$ tel que $\text{LT}(g) = s$, toujours par linéarité on obtient $[gf]_u = \text{LC}(g)[sg]_u \neq 0$. La réciproque est claire. □

Le résultat suivant montre qu'on peut combiner des relations de même span pour obtenir une relation de span plus grand.

Proposition 5. *Si f et f' sont deux relations telles que $span(f) = span(f')$, alors $span(f - \frac{disc(f)}{disc(f')} f') \succ span(f)$.*

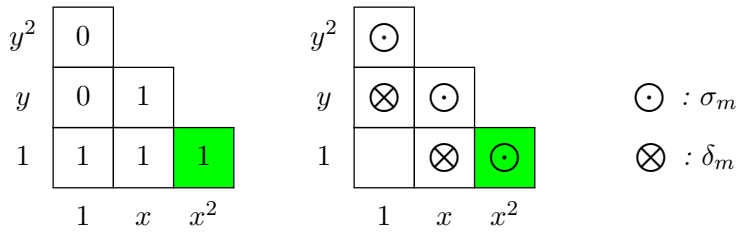
Démonstration. Pour tout $\alpha \in \mathbb{K}$ et pour toute relation g avec $\mathrm{LT}(g) \prec \mathrm{span}(f) = \mathrm{span}(f')$ on a par linéarité $[g(f + \alpha f')]_u = 0$, de sorte que $\mathrm{span}(f + \alpha f') \succeq \mathrm{span}(f)$. Le choix de la valeur $\alpha = -\dfrac{\mathrm{disc}(f)}{\mathrm{disc}(f')}$ donne $[\mathrm{span}(f)(f + \alpha f')]_u = 0$, donc $\mathrm{span}(f - \dfrac{\mathrm{disc}(f)}{\mathrm{disc}(f')} f') \neq \mathrm{span}(f)$ et la conclusion. □

On définit également les ensembles :

Définition 4. *Avec les notations de la définition 3,*

$$\begin{aligned} I_m &= \{f \in \mathbb{K}[\boldsymbol{x}],\ m \prec fail(f)\} \\ \Sigma_m &= LT(I_m) \\ \sigma_m &= \min_{\prec}(\Sigma_m) \\ \Delta_m &= \mathcal{T}_0 \setminus \Sigma_m \\ \delta_m &= \max_{\prec}(\Delta_m) \end{aligned}$$

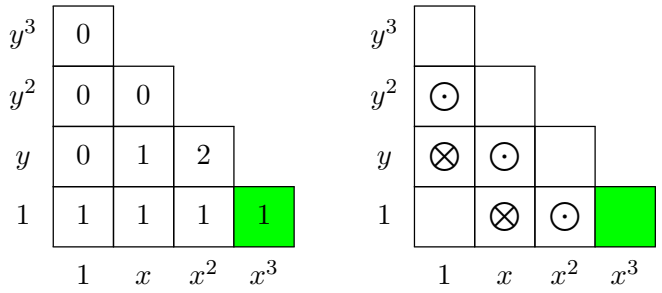
Exemple 5. *Revenons sur l'exemple 2 de la suite $u = \left(\binom{i}{j}\right)_{(i,j)\in\mathbb{N}^2}$. Prenons dans $\mathbb{K}[x, y]$ l'ordre DRL avec $x \prec y$, et $m = x^2$. On a alors :*



En effet, il n'y a pas de relation de terme de tête 1 valide jusqu'à x^2 car la table n'est pas identiquement nulle. Donc $1 \notin \Sigma_{x^2}$, donc $1 \in \Delta_{x^2}$. On a aussi $y \in \Delta_{x^2}$, car les seules relations possibles de terme de tête y et valides jusqu'à y sont de la forme ky avec $k \neq 0$, et ces relations échouent en $xy \preceq x^2$ (autrement dit $fail(ky) = xy$). Enfin $x \in \Delta_{x^2}$, car les seules relations possibles de terme de tête x et valides jusqu'à x sont de la forme $kx + ly - k$ avec $k \neq 0$ et on a $fail(kx + ly - k) = xy \preceq x^2$. Ainsi $\{1, y, x\} \subseteq \Delta_{x^2}$.

Comme par ailleurs on a les relations y^2, $xy - y - 1$ et $x^2 - x$ qui sont vraies jusqu'à x^2, on a que $\Delta_{x^2} = \{1, y, x\}$, puis que $\delta_{x^2} = \{y, x\}$ et que $\sigma_{x^2} = \{y^2, xy, x^2\}$.

Pour $m = x^3$ on obtient :



car les relations y^2 et $xy - y - 1$ sont valides jusqu'à x^3, et bien qu'on ait fail$(x^2 - x) = x^2y \prec x^3$, on trouve avec $x^2 - 2x + 1$ une autre relation de monôme de tête x^2 valide jusqu'à x^3.

On remarque avec cet exemple que si $x^2 - x$ et $x^2 - 2x + 1$ sont dans I_{x^2}, la combinaison linéaire $x^2 - x - (x^2 - 2x + 1) = x - 1$ qui vérifie fail$(x - 1) = xy$ ne l'est pas. Ainsi I_{x^2} n'est pas un idéal de $\mathbb{K}[x, y]$.

Il est cependant clair que $(I_m)_{m\in\mathcal{T}_0}$ décroît et que $\mathcal{I}_u = \bigcap_{m\in\mathcal{T}_0} I_m$. Il en résulte que $(\Delta_m)_{m\in\mathcal{T}_0}$ croît et a pour limite $\mathbf{x}^S$ l'escalier cherché, qui est fini. Ainsi pour m assez grand, Δ_m donnera l'escalier cherché ce qui justifie son calcul.

On a de plus les résultats immédiats suivants :

Proposition 6. *Avec les notations des définitions 3 et 4, on a que*

1. *I_m est stable par multiplication par des éléments de $\mathbb{K}[\boldsymbol{x}]$,*
2. *pour tous $\boldsymbol{i}, \boldsymbol{j} \in \mathbb{N}^n$ tels que $\boldsymbol{x^i} \mid \boldsymbol{x^j}$,*
   (a) *si $\boldsymbol{x^i} \in \Sigma_m$, alors $\boldsymbol{x^j} \in \Sigma_m$,*
   (b) *si $\boldsymbol{x^j} \in \Delta_m$, alors $\boldsymbol{x^i} \in \Delta_m$.*

Démonstration. Pour 1, soit $f \in I_m$, et $g \in \mathbb{K}[\mathbf{x}]$, alors avec (13) il est clair que $gf \in I_m$. On en déduit 2a qui est une conséquence directe, et sa contraposée 2b. □

Le résultat suivant donne une caractérisation intrinsèque de Δ_m et est crucial dans l'itération de BMS.

Proposition 7. *Pour tout monôme $m \in \mathcal{T}_0$, on a $\Delta_m = \{span(f),\ f \notin I_m\}$. De plus, si $m \neq 0$ et si $m' \in \mathcal{T}_0$ est le prédécesseur immédiat de m pour $\prec$, $\delta \in \Delta_m \setminus \Delta_{m'}$ si et seulement si $\delta \mid m$ et $\dfrac{m}{\delta} \in \Delta_m \setminus \Delta_{m'}$.*

Démonstration. L'inclusion $\{\text{span}(f),\ f \notin I_m\} \subseteq \Delta_m$ est claire du fait que si $s = \text{span}(f)$, alors pour tout $g \in \mathbb{K}[\mathbf{x}]$ tel que $\text{LT}(g) = s$, on a d'après (14) que fail$(g) \preceq m$, et donc que $s \notin I_m$, soit $s \in \Delta_m$.

Pour l'inclusion inverse $\Delta_m \subseteq \{\text{span}(f),\ f \notin I_m\}$, raisonnons par induction sur $m \in (\mathcal{T}_0, \prec)$.

Pour $m = 0$, on a $I_0 = \mathbb{K}[\mathbf{x}]$ donc $\Delta_0 = \emptyset$.

Soit $m \succeq 1$, supposons l'inclusion vraie pour tout $n \prec m$ et notons m' le prédécesseur immédiat de m pour $\prec$. Soit $\delta \in \Delta_m$. Si $\delta \in \Delta_{m'}$, alors par hypothèse d'induction on a que $\delta \in \{\text{span}(f),\ f \notin I_{m'}\}$, et comme $I_m \subseteq I_{m'}$, on a bien $\delta \in \{\text{span}(f),\ f \notin I_m\}$. Supposons à présent que $\delta \in \Delta_m \setminus \Delta_{m'}$. Alors il existe une relation $f \in \mathbb{K}[\mathbf{x}]$ avec $\text{LT}(f) = \delta$, et $m' \prec \text{fail}(f) \preceq m$, donc $\text{fail}(f) = m$. Donc pour toute relation g de terme de tête $\dfrac{m}{\delta}$, on a $[gf]_u = 0$ et donc $\text{fail}(g) \preceq m$. S'il existe une telle relation g telle que de plus $\text{fail}(g) = m$, alors on aura bien $\text{span}(g) = \text{LT}(f) = \delta$ et donc $\delta \in \{\text{span}(f),\ f \notin I_m\}$, avec l'implication $\delta \in \Delta_m \setminus \Delta_{m'} \Rightarrow \delta \mid m$ et $\dfrac{m}{\delta} \in \Delta_m \setminus \Delta_{m'}$, qui implique sa réciproque.

Par l'absurde, supposons que pour toute relation $g \in \mathbb{K}[\mathbf{x}]$ de terme de tête $\dfrac{m}{\delta}$ on ait $\text{fail}(g) \prec m$. Alors $\dfrac{m}{\delta} \in \Delta_{m'}$ et par hypothèse d'induction il existe $h \notin I_{m'}$ tel que $\text{span}(h) = \dfrac{m}{\delta}$. Avec $\text{span}(f) = \dfrac{m}{\delta}$ et la proposition 5, on a que $\text{span}(f - \dfrac{\text{disc}(f)}{\text{disc}(h)}) \succ \dfrac{m}{\delta}$. Comme $\text{LT}(h) = \dfrac{\text{fail}(h)}{\text{span}(h)} = \dfrac{\text{fail}(h)}{\frac{m}{\delta}}$ avec $\text{fail}(h) \preceq m' \prec m$, on a $\text{LT}(h) \leq \delta$ donc $\text{LT}(f - \dfrac{\text{disc}(f)}{\text{disc}(h)}) = \delta$, donc $\text{fail}(f - \dfrac{\text{disc}(f)}{\text{disc}(h)}) \succ \dfrac{m}{\delta} m = m$, ce qui contredit que $\delta \in \Delta_m$. □

On en déduit que si $m \in \mathcal{T}_0$ et si $m' \prec m$ le précède immédiatement on a :

$$\delta_m = \underset{\prec}{max}\left(\delta_{m'} \cup \{\frac{m}{s},\ s \in \sigma_{m'} \cap \Delta_m\}\right) \tag{15}$$

Avec cette relation, on peut construire de manière itérative un ensemble S_m de relations indexées par leurs monômes de tête décrivant σ_m et un ensemble D_m de relations indexées par leurs spans décrivant δ_m.

On a vu que pour m assez grand, Δ_m est l'escalier cherché. La proposition suivante quantifie cela.

Proposition 8. *Soit $d_{\max}$ le plus grand monôme de $\boldsymbol{x}^S$. Alors pour $m \succeq (d_{\max})^2$, $\Delta_m = \boldsymbol{x}^S$.*

Démonstration. Soit m le plus petit monôme tel que $d_{\max} \in \Delta_m$, et $m' \prec m$ son prédécesseur immédiat. Alors $d_{\max} \in \Delta_m \setminus \Delta_{m'}$ et d'après la proposition 7, on a $\dfrac{m}{d_{\max}} \in \Delta_m$, donc $\dfrac{m}{d_{\max}} \preceq d_{\max}$ et $m \preceq (d_{\max})^2$. □

Il s'ensuit que $\mathbf{x}^S = \{\text{span}(f),\ f \notin \mathcal{I}_u\}$. En effet d'après (14) on a $\{\text{span}(f),\ f \notin \mathcal{I}_u\} \subseteq \mathbf{x}^S$, et d'après ce qui précède pour $m = (d_{\max})^2$, $\mathbf{x}^S = \Delta_m = \{\text{span}(f),\ f \notin I_m\} \supseteq \{\text{span}(f),\ f \notin \mathcal{I}_u\}$.

On peut enfin obtenir une borne pour la correction de BMS :

Proposition 9. *Soit $s_{\max}$ le plus grand monôme de tête des éléments de G et soit $M = d_{\max} \cdot \max\{d_{\max}, s_{\max}\}$. Pour tout $m \succeq M$, S_m est une base de Gröbner de $\mathcal{I}_u$.*

Algorithm 1 BMS

Entrée : La table $(u)_{i_1,\dots i_n}$, le monôme d'arrêt m_a, l'ordre $\prec$.

$m \leftarrow 1$, $D_m \leftarrow \emptyset$, $S_m \leftarrow \{1\}$

Tant que $m \preceq m_a$ **Faire**

$D'_m \leftarrow D_m$

Pour $s \in S_m$ **Faire**

Si $lt(s)|m$ et $d^s_m := [\frac{m}{ht(s)}s]_{\mathbf{u}} \neq 0$ **alors**

$D'_m(\frac{m}{ht(s)}) \leftarrow \frac{s}{d^s_m}$

$D'_m \leftarrow$ éléments de span max pour la divisibilité de D'_m

$T \leftarrow min\{\mathbf{x^i} \text{ tq } \mathbf{x^i} \nmid span(D'_m)\}$

$S'_m \leftarrow \emptyset$

Pour $t \in T$ **Faire**

Soient $s \in S_m$ et a tels que $t = sa$

Si $t \nmid m$ **alors**

$S'_m(t) \leftarrow \frac{t}{s}S_m(s)$

Sinon, si $\frac{m}{t} \mid span(D_m)$ **alors**

Soit $c \in D_m$ tel que $\frac{m}{t}b = span(c)$

$S'_m(t) \leftarrow S_m(s)a - [S_m(s)a\frac{m}{t}]_u bc$

Sinon

$S'_m(t) \leftarrow S_m(s)$

$S_m \leftarrow S'_m$

$D_m \leftarrow D'_m$

$m \leftarrow$ suivant de m pour l'ordre

Sortie : S_m

Démonstration. D'après la proposition précédente, $\Delta_m = \mathbf{x}^S$ et donc σ_m est bien l'ensemble des monômes de tête d'une base de Gröbner de $\mathcal{I}_u$. Il ne reste plus qu'à montrer que les éléments de S_m sont bien dans $\mathcal{I}_u$. Par l'absurde, supposons que pour un certain $s \in \sigma_m$, on ait $f_s = S_m(s) \notin \mathcal{I}_u$. Alors $\text{span}(f_s) \in \mathbf{x}^S$ et $\text{fail}(f_s) = s \cdot \text{span}(f_s) \preceq s_{\max} \cdot d_{\max}$, donc $f_s \notin I_m$, contradiction. □

3.2 Scalar-FGLM

Nous décrivons ici l'algorithme Scalar-FGLM introduit dans [3], dans le but de rapprocher sa description de celle de BMS.

Comme pour BMS il s'agit de calculer une solution pour une instance du problème 3, mais cette fois ci en utilisant le point de vue matriciel déjà évoqué en 1.3 et une construction de la base de Gröbner analogue à celle de l'algorithme FGLM (voir [9]).

On ne connaît q'un nombre fini de termes de la suite u, on va donc devoir définir une notion de relation vraie jusqu'à un certain point.

Définition 5. *Soit $f \in \mathbb{K}[\boldsymbol{x}]$ et T un ensemble de monômes de $\mathbb{K}[\boldsymbol{x}]$, lorsque*

$$\forall \boldsymbol{x^i} \in T,\ [\boldsymbol{x^i} f]_u = 0, \tag{16}$$

on dit que la relation f est valide sur T.

Cette définition est à rapprocher de la définition 3 pour BMS, elle correspond à une inégalité sur le $fail$. Dans le cas ou T est un ensemble de monômes de la forme $T_m = \{t \in \mathcal{T},\ t \preceq m\}$, on a en effet que f est valide sur T_m si et seulement si $\text{fail}(f) \succ \text{LT}(f)m$.

Pour T et S deux ensembles de monômes de $\mathbb{K}[\mathbf{x}]$ tels que $|T| \geq |S|$, la matrice

$$H_{T,S} = \begin{array}{c} \\ \vdots \\ \mathbf{x^i} \in T \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccc} \cdots & \mathbf{x^j} \in S & \cdots \end{array} \\ \begin{pmatrix} \ddots & \vdots & \iddots \\ \cdots & [\mathbf{x^i x^j}]_u & \cdots \\ \iddots & \vdots & \ddots \end{pmatrix} \end{array}$$

est de rang plein égal à $|S|$ si et seulement si ses colonnes sont indépendantes, et donc si et seulement s'il n'existe pas de relation de support S qui soit valide sur T.

Si S est maximale pour cette propriété, alors c'est un plus petit ensemble pour lequel on peut trouver des relations de supports de la forme $S \cup \{m\}$, avec m « juste au dessus » de S.

C'est donc un bon candidat pour jouer le rôle de l'ensemble Δ dans BMS.

Définition 6. *Soit T une partie finie de $\mathcal{T}$, le usefull staircase $S \subseteq T$ relativement à T et $\prec$ est défini par :*

$$S = \min_{\prec} \left\{ \max_{\subseteq} \{S,\ H_{T,S} \text{ est de rang } |S|\} \right\}$$

où le minimum est pris en voyant les parties S comme des $|S|$-uples à coordonnées croissantes pour $\prec$, ordonnés par l'ordre lexicographique induit par $\prec$.

Il est à noter que le usefull staircase n'est pas nécessairement stable par division, contrairement à l'escalier d'un base de Gröbner pour un ordre donné.

Exemple 6. *Pour la suite* $(0,0,1,0,\dots)$*, pour* $T=\{1,x\}$ *et l'ordre du degré, on a*

$$H_T = H_{T,T} = \begin{array}{c} \\ 1 \\ x \end{array} \begin{array}{c} \begin{array}{cc} 1 & x \end{array} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{array},$$

et le useful staircase est $S=\{x\}$*, et ne contient pas 1. Cependant pour* $T=\{1,x,x^2\}$ *on a*

$$H_T = H_{T,T} = \begin{array}{c} \\ 1 \\ x \\ x^2 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & x & x^2 \end{array} \\ \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array},$$

et on retrouve $S=\{1,x,x^2\}$ *qui est l'escalier de la base de Gröbner* $G=\{x^3\}$ *de l'idéal des relations.*

Proposition 10. *Si* S *est le usefull staircase relativement à la partie finie* T *de* $\mathcal{T}$ *et à* $\prec$*, alors pour tout* m *appartenant à la frontière de* S*, il existe une relation de support* $S\cup\{m\}$ *valide sur* T*.*

Démonstration. Comme le rang de $H_{T,S\cup\{m\}}$ n'est pas $|S|+1$ et que celui de $H_{T,S}$ est $|S|$, la dernière colonne de cette première matrice est une combinaison linéaire des précédentes et il existe donc bien une relation de support $S\cup\{m\}$ valide sur T. □

Pour trouver cette relation, il suffit de résoudre le système linéaire non dégénéré $H_S\boldsymbol{\alpha} = -H_{T,\{m\}}$.

On obtient ainsi l'algorithme 2.

Algorithm 2 Scalar FGLM

Entrée : La table $(u)_{i_1,\dots i_n}$, une borne $d\in\mathbb{N}$, un ordre du degré $\prec$.
  Construire H_{T_d}
  Déterminer S en extrayant une sous matrice de rang maximal
  $L \leftarrow T_{d+1}\setminus\{s\in T_d,\ s \text{ divise un élément de } S\}$
  $G\leftarrow\emptyset$
  Tant que $L\neq\emptyset$ **Faire**
    $m\leftarrow \min_{\prec} L$
    Résoudre $H_S\boldsymbol{\alpha} = -H_{T,\{m\}}$
    $G\leftarrow G\cup\{m+\sum_{s\in S}\alpha_s s\}$
    Supprimer de L les multiples de $\mathrm{LT}(G)$
Sortie : G

C'est pour l'étape de résolution du système linéaire multi-Hankel $H_S\boldsymbol{\alpha} = -H_{T,\{m\}}$ que nous avons tenté d'obtenir une algèbre linéaire dédiée rapide, par le biais d'une interprétation polynomiale que nous présentons dans la partie suivante.

3.3 Écriture polynomiale en dimension ≥ 2

Une partie significative du stage a constitué à rechercher en dimension ≥ 2 une solution analogue au demi-PGCD présenté à la section 2.1.

Pour une suite à un seul indice, trouver une relation de récurrence linéaire d'ordre d pour la suite $(u_i)_{i\in\mathbb{N}}$ revient à résoudre un système de la forme

$$\begin{array}{c} \\ 1 \\ \vdots \\ x^{d-1} \end{array} \begin{array}{c} \begin{array}{cccc} 1 & \cdots & x^{d-1} & x^d \end{array} \\ \begin{pmatrix} u_0 & \cdots & u_{d-1} & u_d \\ \vdots & & \vdots & \vdots \\ u_{d-1} & \cdots & u_{2d-2} & u_{2d-1} \end{pmatrix} \end{array} \begin{array}{c} x^d \\ \vdots \\ x \\ 1 \end{array} \begin{pmatrix} c_d \\ \vdots \\ c_1 \\ 1 \end{pmatrix} = \begin{array}{c} x^d \\ \vdots \\ x^{2d-1} \end{array} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{17}$$

ce qui peut se faire en trouvant deux polynômes $C(x)$ et $R(x)$ tels que

$$C(x)H_{2d-1}(x) = R(x) \mod I, \text{ où } I =< x^{2d} > \tag{18}$$

$$deg(C(x)) \leq d, \text{ autrement dit } support(C(x)) \subseteq \{1, x, \ldots, x^d\} \tag{19}$$

$$deg(R(x)) < d, \text{ autrement dit } support(R(x)) \subseteq \{1, x, \ldots, x^{d-1}\} \tag{20}$$

en utilisant l'algorithme d'Euclide étendu avec $H_{2d-1}(x)$ et x^{2d}. On obtient $C(x)$ comme cofacteur pour le demi-PGCD de $H_{2d-1}(x)$ et x^{2d}. Le polynôme $g(x) = x^d C(\frac{1}{x})$ engendre l'idéal des relations (à condition que H_{2d-2} soit de rang plein maximale).

En dimension supérieure, pour trouver une base de Gröbner de l'idéal des relations de la suite $(u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ d'escalier $S = \{s_0 = 1, s_1, \ldots, s_{d-1}\}$ pour un ordre monomial donné $\prec$, on est amené dans Scalar-FGLM à résoudre des systèmes de la forme $H_S\boldsymbol{\alpha} = -H_{T,\{m\}}$, qu'on peut aussi écrire sous de la forme :

$$\begin{array}{c} \\ 1 \\ \vdots \\ s_{d-1} \end{array} \begin{array}{c} \begin{array}{cccc} 1 & \cdots & s_{d-1} & m \end{array} \\ \begin{pmatrix} u_0 & \cdots & [s_{d-1}]_u & [m]_u \\ \vdots & & \vdots & \vdots \\ [s_{d-1}]_u & \cdots & [(s_{d-1})^2]_u & [s_{d-1}m]_u \end{pmatrix} \end{array} \begin{array}{c} a_m \\ \vdots \\ \frac{a_m}{s_{d-1}} \\ \frac{a_m}{m} \end{array} \begin{pmatrix} c_{a_m} \\ \vdots \\ c_{\frac{a_m}{s_{d-1}}} \\ c_{\frac{a_m}{m}} = 1 \end{pmatrix} = \begin{array}{c} a_m \\ \vdots \\ s_{d-1}a_m \end{array} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{21}$$

pour tout monôme m minimal pour la divisibilité dans la frontière de S, où $a_m = ppcm(S \cup \{m\})$. Il s'agit donc de trouver un polynôme $C_m(\mathbf{x})$ tel que :

$$C_m(\mathbf{x})H_m(\mathbf{x}) = R_m(\mathbf{x}) \mod I_m \tag{22}$$

$$support(C_m(\mathbf{x})) \subseteq \{\frac{a_m}{t},\, t \in S \cup \{m\}\} \tag{23}$$

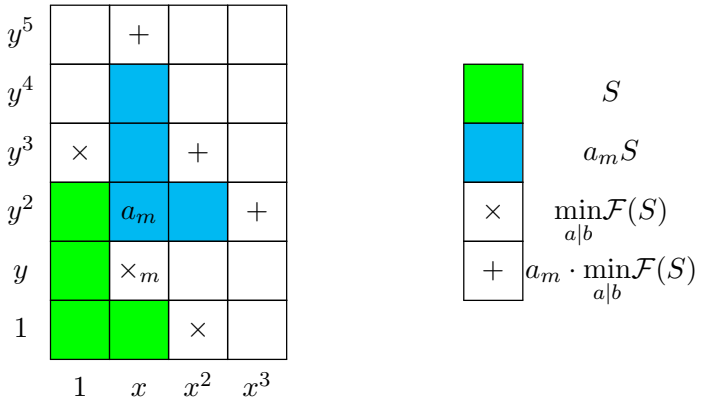
$$support(R_m(x)) \subseteq \{r \in \mathcal{T},\, \exists s \in S,\, r \mid a_m s\} \setminus a_m S \tag{24}$$

où I_m est l'idéal monomial engendré par les monômes de la frontière de S translatés d'un facteur a_m :

$$I_m =< \{a_m f,\, f \in \text{Frontière}(S)\} > .$$

Les polynômes $g_m(\mathbf{x}) = a_m C_m(\frac{1}{\mathbf{x}})$ forment alors une base de Gröbner de l'idéal des relations cherché.

FIGURE 1 – interprétation polynomiale



Exemple 7. *En deux indices, trouver une relation de récurrence peut par exemple revenir à résoudre :*

$$\begin{array}{c} \\ 1 \\ y \\ x \\ y^2 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & y & x & y^2 & xy \end{array} \\ \begin{pmatrix} [1]_u & [y]_u & [x]_u & [y^2]_u & [xy]_u \\ [y]_u & [y^2]_u & [xy]_u & [y^3]_u & [xy^2]_u \\ [x]_u & [xy]_u & [x^2]_u & [xy^2]_u & [x^2y]_u \\ [y^2]_u & [y^3]_u & [xy^2]_u & [y^4]_u & [xy^3]_u \end{pmatrix} \end{array} \begin{array}{c} xy^2 \\ xy \\ y^2 \\ x \\ y \end{array} \begin{pmatrix} c_{xy^2} \\ c_{xy} \\ c_{y^2} \\ c_x \\ 1 \end{pmatrix} = \begin{array}{c} xy^2 \\ xy^3 \\ x^2y^2 \\ xy^4 \end{array} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad (25)$$

pour l'escalier $S = \{1, y, x, y^2\}$, et $m = xy$ le monôme avec lequel on cherche une relation.

Sur la figure 1 on peut visualiser l'escalier, le monôme m à lier par la relation à déterminer, le ppcm a_m de $S \cup \{m\}$, le translaté de S par le facteur a_m, $a_m S$, qui correspond aux termes annulés dans le second membre. Le support de C_m est inclus dans $\{\frac{a_m}{t},\ t \in S \cup \{m\}\}$. On peut visualiser cet ensemble comme $S \cup \{m\}$ vu depuis le repère d'origine a_m et d'axes inversés. Le support de R_m est inclus dans les monômes diviseurs stricts de l'escalier translaté.

Cette interprétation polynomiale ne nous a pas permis d'obtenir un calcul efficace de C_m, les différentes tentatives échouant toutes sur des exemples élémentaires.

Références

[1] E. Berlekamp. Nonbinary bch decoding (abstr.). *IEEE Transactions on Information Theory*, 14(2) :242–242, March 1968.

[2] E.R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill series in systems science. Aegean Park Press, 1984.

[3] Jérémy Berthomieu, Brice Boyer, and Jean-Charles Faugère. Linear algebra for computing gröbner bases of linear recursive multidimensional sequences. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '15, pages 61–68, New York, NY, USA, 2015. ACM.

[4] Jérémy Berthomieu and Jean-Charles Faugère. Guessing Linear Recurrence Relations of Sequence Tuples and P-recursive Sequences with Linear Algebra. In *41st International Symposium on Symbolic and Algebraic Computation*, page 8, Waterloo, ON, Canada, July 2016.

[5] R.C. Bose and D.K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3(1) :68 – 79, 1960.

[6] Maria Bras-Amorós and Michael E. O'Sullivan. The correction capability of the berlekamp–massey–sakata algorithm with majority voting. *Applicable Algebra in Engineering, Communication and Computing*, 17(5) :315–335, 2006.

[7] Richard P Brent, Fred G Gustavson, and David YY Yun. Fast solution of toeplitz systems of equations and computation of padé approximants. *Journal of Algorithms*, 1(3) :259–295, 1980.

[8] Jean Louis Dornstetter. On the equivalence between berlekamp's and euclid's algorithms. *IEEE Trans. Inf. Theor.*, 33(3) :428–431, May 1987.

[9] Jean-Charles. Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation*, 16(4) :329–344, 1993.

[10] Edmund Jonckheere and Chingwo Ma. A simple hankel interpretation of the berlekamp-massey algorithm. *Linear Algebra and its Applications*, 125 :65 – 76, 1989.

[11] J. Massey. Shift-register synthesis and bch decoding. *IEEE Transactions on Information Theory*, 15(1) :122–127, Jan 1969.

[12] Robert J. McEliece and James B. Shearer. A property of euclid's algorithm and an application to padé approximation. *SIAM Journal on Applied Mathematics*, 34(4) :611–615, 1978.

[13] Shojiro Sakata. Extension of the berlekamp-massey algorithm to n dimensions. *Inf. Comput.*, 84(2) :207–239, February 1990.

[14] M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso. *Gröbner Bases, Coding, and Cryptography*. Springer Berlin Heidelberg, 2009.