# Algorithmes à signature pour le calcul des bases de Gröbner non-commutatives

Arthur Léonard

2021

## Introduction

Dans les années 1960, Bruno Buchberger introduit les bases de Gröbner, et trouve un algorithme qui permet de les calculer [1]. Cependant, cet algorithme, basé sur des divisions polynomiales multivariées répétées, effectue de nombreuses divisions dont le reste est nul, qui ne permettent pas de découvrir des nouveaux polynômes dans la base. Pour améliorer significativement la performance des algorithmes de calcul des bases de Gröbner, de nombreux critères ont été trouvés pour éviter d'effectuer ces divisions.

En 1999 et 2002, Jean-Charles Faugère introduit deux algorithmes, F4 [2] et F5 [3]. Le premier utilise de l'algèbre linéaire pour effectuer plusieurs réductions en parallèle. En revanche, le second utilise l'information donnée par les divisions à zéro, en étudiant le module des syzygies. C'est le premier algorithme à signature. L'algorithme F5 a ensuite été simplifié par Gao, Guan et Volny dans l'algorithme G2V [7], qui a lui-même été amélioré et généralisé par Gao, Volny et Wang en 2010 dans l'algorithme GVW.

Dans le mémoire, nous avons présenté l'algorithme GVW [8], dans le cas particulier d'un anneau de polynômes sur un corps, avec un seul ordre monomial et l'ordre POT (Position Over Term).

L'objectif du stage, qui s'est déroulé en présentiel dans le laboratoire XLIM de l'université de Limoges, était d'étudier comment les algorithmes à signature peuvent s'adapter au contexte non-commutatif. Avec l'aide de mes maîtres de stage, Tristan Vaccon et Cyrille Chenavier, que je tiens à remercier pour leur supervision, nous avons adapté de nombreuses définitions en non-commutatif, et nous avons remarqué *a posteriori* que nos définitions coïncidaient avec celles d'un autre article [4], apparu en preprint après la fin du stage. Une fois ces définitions posées, nous nous sommes heurtés à des difficultés que nous avons essayé d'identifier au mieux. Nous avons ainsi démontré un résultat qui montre une obstruction à la création d'un algorithme à signature non-commutatif : l'ensemble des monômes dominants des syzygies, ensemble essentiel à la création d'un algorithme à signature, n'est pas nécessairement un langage décidable. En ajoutant pour contrainte que l'ordre soit isomorphe à $\mathbb{N}$ pour les ordres ("fair"

dans [4]), nous avons réussi à démontré que l'ensemble des monômes dominants des syzygies n'est pas algébrique.

## Algorithme de Buchberger non-commutatif

Commençons par adapter les différentes définitions du mémoire au cadre non-commutatif. Soit $\mathbb{K}$ un corps, on se place dans $\mathbb{A} = \mathbb{K}\langle X_1, \dots, X_n\rangle$, l'ensemble des polynômes non-commutatifs à $n$ variables à coefficients dans $\mathbb{K}$. On note :

$$\mathcal{M} := \{X_{i_1}X_{i_2}\dots X_{i_k} \mid k \in \mathbb{N}, (i_1, i_2, \dots, i_k) \in \{1, \dots, n\}^k\}$$

l'ensemble des monômes non-commutatifs. On fixe un ordre monomial $\leq$, c'est à dire un bon ordre sur $\mathcal{M}$ qui vérifie :

— $\forall A \in \mathcal{M}, 1 \leq A$
— $\forall A, B \in \mathcal{M}, (A \leq B \implies \forall M \in \mathcal{M}, AM \leq BM)$
— $\forall A, B \in \mathcal{M}, (A \leq B \implies \forall M \in \mathcal{M}, MA \leq MB)$

Pour $f = \sum_{M\in\mathcal{M}} \alpha_M M \in A$, on notera :

— $\mathrm{LM}(f) := \sup\{M \in \mathcal{M} \mid \alpha_M \neq 0\}$ le monôme dominant de $f$.
— $\mathrm{LC}(f) := \alpha_{\mathrm{LM}(f)}$ le coefficient dominant de $f$.
— $\mathrm{LT}(f) := \mathrm{LC}(f)\,\mathrm{LM}(f)$ le terme dominant de $f$.

Soit $\mid$ la relation de divisibilité sur $\mathcal{M}$, définie par :

$$\forall A, B \in \mathcal{M}, (A \mid B \iff \exists L, R \in \mathcal{M}, LAR = B)$$

**Définition** (Base de Gröbner)**.** *Soit $I$ un idéal de $\mathbb{A}$, et soit $G$ un ensemble de polynômes de $I$. On dit que $G$ est une base de Gröbner de $I$ si pour tout $f \in I$, il existe $g \in G$ tel que* $\mathrm{LM}(g) \mid \mathrm{LM}(f)$*,*

**Fait.** *Contrairement au cas commutatif, tous les idéaux ne sont pas finiment engendrés, et certains idéaux finiment engendrés n'ont pas de base de Gröbner finie.*

*Démonstration.* Si l'on savait trouver une base de Gröbner finie de tout idéal finiment engendré, on pourrait décider le problème du mot en calculant une base de Gröbner de $(A_i - B_i)_{i\in\{1,\dots,k\}}$ qui correspondent aux règles de réécriture $A_i \to B_i$. Or le problème du mot est indécidable. □

Soit $I$ un idéal de type fini, engendré par $g_1, \dots, g_m$, nous disposons de l'algorithme de Buchberger non-commutatif qui nous permet de calculer une base de Gröbner finie de $I$ si elle existe.

L'algorithme de Buchberger non-commutatif est en fait très similaire à l'algorithme commutatif, à l'exception que les S-polynômes de deux polynômes $P$ et $Q$ sont de la forme $lPr - l'Qr'$, où $l, r, l', r \in \mathcal{M}$ sont tels que $l\,\mathrm{LM}(P)r = l'\,\mathrm{LM}(Q)r'$, $\deg(l\,\mathrm{LM}(P)) > \deg(l')$ et $\deg(\mathrm{LM}(Q)r') > \deg(r)$.

Cependant, comme dans le cas commutatif, cet algorithme effectue des réductions à zéro que nous voudrions éviter.

### Exemple d'exécution

Considérons $g_1 = ts - a, g_2 = sa - at$ avec l'ordre deglex (c'est une présentation finie du module des tresses à trois brins [6]). On obtient dans l'ordre les S-polynômes suivants :

- $g_1 a - t g_2 = tat - aa$, qui est irréductible, on ajoute donc $g_3 := tat - aa$ à la base de Gröbner.
- $g_3 s - t a g_1 = taa - aas$, qui est irréductible, on ajoute donc $g_4 := taa - aas$ à la base de Gröbner.
- $tag_3 - g_3 at = -taaas + aaaa$, qui se réduit de la manière suivante :

$$-taaas + aaaa \to -aasas + aaaa \to -aaats + aaaa \to 0$$

  On fait donc une première réduction à 0.
- $tag_3 - g_3 at = -taaa + aaat$, qui se réduit de la manière suivante :

$$-taaa + aaat \to -aasa + aaat \to 0$$

  On fait donc une deuxième réduction à 0.

La base de Gröbner obtenue est $(ts - a, sa - at, tat - aa, taa - aas)$.

Comme il était fastidieux d'exécuter l'algorithme de Buchberger à la main sur des exemples, ce dernier a été implémenté.

## Signatures

Nous aimerions donc adapter le concept de signature au cadre non-commutatif, afin d'obtenir un algorithme qui permette de calculer une base de Gröbner finie de $I$ si elle existe, avec peu de réductions à zéro, grâce à un théorème F5 non-commutatif.

Comme nous allons le voir, les concepts s'adaptent naturellement, mais il est difficile de garantir la terminaison d'un algorithme à signature.

**Définition** (Chemins de réduction)**.** *On appelle $\mathbb{K}[\mathcal{M} \times \{1, \dots, m\} \times \mathcal{M}]$ l'ensemble des chemins de réduction. Cet ensemble est muni d'une structure naturelle de $\mathbb{A}$-bimodule et d'un morphisme*

$$\begin{aligned} E : \mathbb{K}[\mathcal{M} \times \{1, \dots, m\} \times \mathcal{M}] &\to \mathbb{A} \\ \sum_{(l,i,r) \in \mathcal{M} \times \{1,\dots,m\} \times \mathcal{M}} \alpha_{(l,i,r)} (l, i, r) &\mapsto \sum_{(l,i,r) \in \mathcal{M} \times \{1,\dots,m\} \times \mathcal{M}} \alpha_{(l,i,r)} l g_i r \end{aligned}$$

Soit $\leq$ un ordre sur $\mathcal{M} \times \{1, \dots, m\} \times \mathcal{M}$ compatible avec la multiplication à gauche et à droite par un élément de $\mathcal{M}$. Pour

$$\sigma = \sum_{(l,i,r) \in \mathcal{M} \times \{1,\dots,m\} \times \mathcal{M}} \alpha_{(l,i,r)} (l, i, r) \in \mathbb{K}[\mathcal{M} \times \{1, \dots, m\} \times \mathcal{M}],$$

on notera :

— $\mathrm{LM}(\sigma) := \sup\{(l,i,r) \in \mathcal{M} \times \{1,\dots,m\} \times \mathcal{M} \mid \alpha_{(l,i,r)} \neq 0\}$ le monôme dominant de $\sigma$.
— $\mathrm{LC}(\sigma) := \alpha_{\mathrm{LM}(\sigma)}$ le coefficient dominant de $\sigma$.
— $\mathrm{LT}(\sigma) := \mathrm{LC}(\sigma)\,\mathrm{LM}(\sigma)$ le terme dominant de $\sigma$.

**Définition** (Sigpolynômes, Syzygies)**.** *On note :*

$$M := \{(\sigma, f) \in \mathbb{K}[\mathcal{M} \times \{1,\dots,m\} \times \mathcal{M}] \times \mathbb{A} \mid E(\sigma) = f\}$$

*Les élements de $M$ sont appelés sigpolynômes. Les premières composantes des élements de $M$ de second membre nul sont appelés syzygies.*

*Pour $p = (\sigma, f) \in \mathbb{K}[\mathcal{M} \times \{1,\dots,m\} \times \mathcal{M}] \times \mathbb{A}$, on notera :*
— $\mathrm{LM}(p) := \mathrm{LM}(f)$ *le monôme dominant de $p$.*
— $\mathrm{Sig}(p) := \mathrm{LM}(\sigma)$ *la signature de $p$.*

**Définition** (Réduction en tête)**.** *On dit que le sigpolynôme $(\sigma, f)$ est réductible en tête par le sigpolynôme $(\sigma', f')$ si on est dans l'un des cas suivants :*
— *$f' = 0$ et il existe $l, r \in \mathcal{M}$ tels que $\mathrm{LM}(\sigma) = l\,\mathrm{LM}(\sigma')r$.*
— *Il existe $l, r \in \mathcal{M}$ tels que $\mathrm{LM}(f) = l\,\mathrm{LM}(f')r$ et $l\,\mathrm{LM}(\sigma')r \leq \mathrm{LM}(\sigma)$.*

Les algorithmes à signatures calculent tous une base de Gröbner forte :

**Définition** (Base de Gröbner forte)**.** *Une base de Gröbner forte de $M$ est un sous-ensemble $G_f$ de $M$ tel que tout élément non-nul de $M$ est réductible en tête par un élément de $G_f$.*

L'intérêt de regarder une base de Gröbner forte est le théorème suivant :

**Théorème** (Théorème de projection)**.** *Soit $G_f$ une base de Gröbner forte de $M$, alors :*

$$\pi_2(G_f) := \{v \mid (u, v) \in M\}$$

*est une base de Gröbner de $I$.*

*Démonstration.* Soit $f \in I$ non-nul. Par définition, il existe donc $\sigma \in \mathbb{K}[\mathcal{M} \times \{1,\dots,m\} \times \mathcal{M}]$ tel que $E(\sigma) = f$, d'où $(\sigma, f) \in M$. Choisissons un $\sigma$ tel que $\mathrm{LM}(\sigma)$ soit minimal. Comme $G_f$ est une base de Gröbner forte de $M$, il existe $(\sigma', f') \in G_f$ tel que $(\sigma, f)$ est réductible en tête par $(\sigma', f')$. Si $f' = 0$, alors il existe $l, r \in \mathcal{M}$ tel que $\mathrm{LM}(\sigma) = l\,\mathrm{LM}(\sigma')r$, et alors :

$$(\sigma - \mathrm{LC}(\sigma) l\,\mathrm{LM}(\sigma')r, f) \in M,$$

ce qui contredit la minimalité de $\mathrm{LM}(\sigma)$.

Si $f' \neq 0$, alors il existe $l, r \in \mathcal{M}$ tel que $\mathrm{LM}(f) = l\,\mathrm{LM}(f')r$, d'où $\mathrm{LM}(f') \mid \mathrm{LM}(f)$ et $\pi_2(G_f)$ est bien une base de Gröbner de $I$. □

L'avantage (mais aussi l'inconvénient) d'un algorithme qui calcule une base de Gröbner forte est qu'il calcule aussi une base de Gröbner des syzygies.

**Définition** (Base de Gröbner des syzygies)**.** *On dit qu'un sous-ensemble $G_s$ des syzygies est une base de Gröbner des syzygies, si pour chaque syzygie $\sigma$ non-nulle, il existe $\sigma' \in G_s$ et $l, r \in \mathcal{M}$ tels que $\mathrm{LM}(\sigma) = l\,\mathrm{LM}(\sigma')r$.*

**Fait.** *Lorsque l'on considère les premières composantes des sigpolynômes de seconde composante nulle d'une base de Gröbner forte, on obtient une base de Gröbner des syzygies.*

Il se trouve que l'on connaît déjà de nombreuses syzygies :

**Définition** (Syzygies principales)**.** *On appelle syzygie principale une syzygie qui est dans le sous-*$\mathbb{A}$*-bimodule de* $\mathbb{K}[\mathcal{M} \times \{1, \dots, m\} \times \mathcal{M}]$ *engendré par les :*

$$g_i(X, j, 1) - (1, i, X)g_j, X \in \mathcal{M}, (i, j) \in \{1, \dots, m\}^2$$

*On dira que la suite* $(g_1, \dots, g_m)$ *est régulière s'il n'y a pas d'autres syzygies que les syzygies principales.*

Par exemple, prenons $g_1 = ba - ab, g_2 = b^3$, avec pour ordres deglex et poslexdeglex. Les générateurs des syzygies principales sont de la forme :

$$\begin{aligned}
&(1, 2, Xba) - (1, 2, Xab) - (b^3X, 1, 1)\\
&(baX, 2, 1) - (abX, 2, 1) - (1, 1, Xb^3)\\
&(b^3X, 2, 1) - (1, 2, Xb^3)\\
&(baX, 1, 1) - (abX, 1, 1) - (1, 1, Xba) + (1, 1, Xab)
\end{aligned}$$

pour n'importe quel $X \in \mathcal{M}$.

Remarquons que l'on peut construire d'autres syzygies principales à partir des ces générateurs : par exemple, si on multiplie le deuxième générateur par $b^2$ à gauche et qu'on fait le remplacement $X \to aX$ dans la troisième relation, on obtient :

$$(b^2abX, 2, 1) - (1, 2, aXb^3) + (b^2, 1, Xb^3)$$

En simplifiant par la deuxième relation, on obtient :

$$(bab^2X, 2, 1) - (1, 2, aXb^3) + (b^2, 1, Xb^3) + (b, 1, bXb^3)$$

Et en resimplifiant par la deuxième relation, on obtient :

$$(ab^3X, 2, 1) - (1, 2, aXb^3) + (b^2, 1, Xb^3) + (b, 1, bXb^3) + (1, 1, b^2Xb^3)$$

On peut alors simplifier par la troisième relation, on obtient :

$$(a, 2, Xb^3) - (1, 2, aXb^3) + (b^2, 1, Xb^3) + (b, 1, bXb^3) + (1, 1, b^2Xb^3)$$

Qui donne un nouveau type de monôme dominant. Cette approche peut-être systématisée en un algorithme à la Knuth-Bendix.

Un algorithme à signature "naïf" ferait exactement la même chose que GVW dans le nouveau langage : il commence avec les paires $\{((1, i, 1), g_i) \mid 1 \leq i \leq m\}$, puis à chaque étape choisit la paire critique de plus petite signature, la réduit régulièrement par les paires déjà ajoutées, puis l'ajoute aux paires existantes, en

ignorant éventuellement des paires dont la signature est un monôme dominant de syzygie principale. Ce dernier algorithme a été implémenté par moi-même dans une version simple, ce qui a permis d'observer qu'il terminait très rarement. En effet, un algorithme à signature déterminerait donc d'une manière ou d'une autre les monômes dominants des syzygies. Dans le cas commutatif, cette base est finie ; c'est une conséquence du lemme de Dickson. En revanche, dans le cas non-commutatif, les syzygies ne sont pas forcément de type fini, ce qui nous empêche de faire cet algorithme naïf. Pour que notre algorithme ait une chance de terminer, il faut réussir à traiter les syzygies de manière différente, ou au moins les syzygies princiales si on veut qu'il termine dans le cas d'une suite régulière.

# Exemples de calcul de syzygies

### Ordre TOP

Considérons l'exemple $g_1 = b^2, g_2 = ba - ab$, avec pour ordre deglex d'un côté, et avec pour ordres deglex et l'ordre de concaténation, où nous avons $(l, i, r) \leq (l', j, r')$ si l'une des conditions ci-desous est vérifiée :

— $l \operatorname{LM}(g_i) r < l' \operatorname{LM}(g_j) r'$

— $l \operatorname{LM}(g_i) r = l' \operatorname{LM}(g_j) r'$ et $\deg l \leq \deg l'$

— $l \operatorname{LM}(g_i) r = l' \operatorname{LM}(g_j) r'$ et $\deg l = \deg l'$ et $i \leq j$.

Nous cherchons à déterminer les monômes dominants des syzygies.

**Fait.** *Les monômes dominants des syzygies sont les paires $(l, i, r)$ dont $l$ contient au moins un $b$.*

*Démonstration.* Commençons par montrer que tous les monômes dominants des syzygies contiennent un $b$ à gauche.

Soit $\sigma$ une syzygie non-nulle. On construit un graphe $G_\sigma$ de la manière suivante :

— Les sommets de $G_\sigma$ sont les

$$\{l(ba)r \mid (l,2,r) \in \operatorname{supp}(\sigma)\} \cup \{l(ab)r \mid (l,2,r) \in \operatorname{supp}(\sigma)\} \cup \{l(bb)r \mid (l,1,r) \in \operatorname{supp}(\sigma)\}$$

— Pour chaque terme $\alpha(l, 2, r)$ de $\sigma$, on ajoute un arc entre $l(ba)r$ et $l(ab)r$ de pondération $\alpha$.

— Chaque sommet $w$ est étiqueté

$$\sum_{\alpha(l,1,r) \text{ terme de } \sigma, w = l(b^2)r} \alpha$$

— Le fait que $\sigma$ est une syzygie implique que pour chaque sommet $v$, la somme de la pondération de $v$, de la pondération des arcs qui sortent de $v$, moins la pondération des arcs qui entre dans $v$ est nulle. Appellons cette propriété "équation d'équilibre" en $v$.

Soit $s$ le sommet de $G_\sigma$ le plus grand pour l'ordre monomial, par propriétés de l'ordre de concaténation, il n'y a pas d'arc qui entre dans $s$.

Distinguons deux cas :

— Le monôme dominant de $\sigma$ est de la forme $(l, 1, r)$. Dans ce cas, puisqu'on a choisit l'ordre de concaténation, on a $s = l(b^2)r$. Par équation d'équilibre en $s$, on obtient qu'il existe un monôme $(l', j, r')$ de $\sigma$ tel que $l' \operatorname{LM}(g_j) r' = l(b^2)r$. Si $j = 1$, alors $l'(b^2)r' = l(b^2)r$, et comme $\deg l' < \deg l$, on obtient que $l$ doit contenir un $b$. Si $j = 2$, alors $l'(ba)r' = l(b^2)r$, et comme $\deg l' \leq \deg l$, on obtient que $l$ doit contenir un $b$.

— Le monôme dominant de $\sigma$ est de la forme $(l, 2, r)$. Dans ce cas, puisqu'on a choisit l'ordre de concaténation, on a $s = l(ba)r$. Par équation d'équilibre en $s$, on obtient qu'il existe un monôme $(l', j, r')$ de $\sigma$ tel que $l' \operatorname{LM}(g_j) r' = l(ba)r$. Si $j = 1$, alors $l'(b^2)r' = l(ba)r$, et comme $\deg l' \leq \deg l$, on obtient que $l$ doit contenir un $b$. Si $j = 2$, alors $l'(ba)r' = l(ba)r$, et comme $\deg l' < \deg l$, on obtient que $l$ doit contenir un $b$.

Réciproquement, montrons que tous les monômes contenant un $b$ à gauche sont des monômes dominants de syzygies. Par compatibilité à la multiplication à gauche et à droite, il suffit de montrer que :

$$(ba^n, 1, 1) \text{ et } (ba^n, 2, 1)$$

sont des monômes dominants des syzygies, ce qui est le cas car :

$$(ba^n, 1, 1) - (1, 2, a^{n-1}b^2) - (aba^{n-1}, 1, 1)$$

est une syzygie de monôme dominant $(ba^n, 1, 1)$ et

$$(ba^n, 2, 1) + \sum_{k=0}^{n} (a^k, 2, a^{n-k}b) + (a^{n+1}, 1, 1) - \sum_{k=0}^{n-1} (a^k, 2, a^{n-1-k}ba) - (a^n, 1, a)$$

est une syzygie de monôme dominant $(ba^n, 2, 1)$. □

Ce fait implique qu'il n'y a pas de base de Gröbner forte finie de $(g_1, g_2)$.

**Ordre POT**

Considérons maintenant l'exemple $g_1 = a^2, g_2 = ba - ab$, avec pour ordre deglex d'un côté, et avec pour ordres deglex et l'ordre POT, où nous avons $(l, i, r) \leq (l', j, r')$ si l'une des conditions ci-desous est vérifiée :

— $i < j$

— $i = j$ et $\deg l \leq \deg l'$

— $i = j$ et $\deg l = \deg l'$ et $l \operatorname{LM}(g_i) r < l' \operatorname{LM}(g_j) r'$

Soit $\operatorname{LM}_s$ l'ensemble des monômes dominants des syzygies, on cherche à déterminer $\operatorname{LM}_s$.

**Fait.** *On a :*

$$\operatorname{LM}_s \cap \{(l, 2, 1) \mid l \in \mathcal{M}\} = \{(l, 2, 1) \mid l \in \mathcal{M}, l \textit{ contient un } a\}$$

*Démonstration.* Soit $\sigma$ une syzygie non-nulle, dont le monôme dominant est $(l, 2, 1)$. Par équation d'équilibre en $l(ba)$, on obtient qu'il doit exister un monôme $(l', j, r')$ de $\sigma$ qui doit vérifier l'une des conditions suivantes :

— $j = 2$ et $l'(ba)r' = l(ba)$, comme $\deg l' < \deg l$, on obtient que $l$ doit contenir un $a$.

— $j = 2$ et $l'(ab)r' = l(ba)$, comme $\deg l' < \deg l$, on obtient que $l$ doit contenir un $a$.

— $j = 1$ et $l'(aa)r' = l(ba)$, dans ce cas, il est clair que $l$ doit contenir au moins un $a$.

Montrons maitenant que tout élément de la forme $(l, 2, 1)$ avec $l$ contenant au moins un $a$ est un monôme dominant de syzygie. Par compatibilité à la multiplication à gauche et à droite, il suffit de montrer que les :

$$(ab^n, 2, 1)$$

sont des monômes dominants des syzygies, ce qui est le cas car :

$$(b^{n+1}, 1, 1) - \sum_{k=0}^{n} (b^{n-k}, 2, b^k a) - \sum_{k=0}^{n} (ab^{n-k}, 2, b^k) - (1, 1, b^{n+1})$$

est une syzygie de monôme dominant $(ab^n, 2, 1)$. □

Ce fait implique qu'il n'y a pas de base de Gröbner forte finie de $(g_1, g_2)$.

## Langage régulier ?

Au vu de la forme des syzygies principales, et de l'algorithme pour en calculer de nouvelles, on peut se demander si un automate peut reconnaître les monômes dominants des syzygies, lorsque la base de Gröbner est finie. Nous allons démontrer que ce n'est pas le cas, en utilisant le fait que le langage $\{a^n b^n \mid n \in \mathbb{N}\}$ n'est pas régulier. Considérons, pour l'alphabet

$$\{a, b, c, d, e, s, t, x, y, z, \infty\}$$

les polynômes :

$$\begin{aligned}
g_1 &:= sa - tcx \\
g_2 &:= xa - ax \\
g_3 &:= xd - dx \\
g_4 &:= ya - ay \\
g_5 &:= yd - dy \\
g_6 &:= xbb - dyb \\
g_7 &:= cya - ccx \\
g_8 &:= xbe - dze \\
g_9 &:= dz - zb \\
g_{10} &:= cz - za \\
g_{11} &:= tz - s
\end{aligned}$$

avec pour ordre $m_1 < m_2$ si :

— Il y a moins de symboles $\infty$ dans $m_1$ que dans $m_2$.

— Il y a autant de symboles $\infty$ dans $m_1$ que dans $m_2$, mais il y a moins de symboles $s$ dans $m_1$ que dans $m_2$.

— Il y a autant de symboles $\infty$ et de symboles $s$ dans $m_1$ que dans $m_2$, mais $m_1 <_{deglex} m_2$ où $a < b < c < d < x < y < z < e < t < s < \infty$.

Nous avons $(l, i, r) \leq (l', j, r')$ si l'une des conditions ci-desous est vérifiée :

— $l \operatorname{LM}(g_i) r < l' \operatorname{LM}(g_j) r'$

— $l \operatorname{LM}(g_i) r = l' \operatorname{LM}(g_j) r'$ et $i < j$

— $l \operatorname{LM}(g_i) r = l' \operatorname{LM}(g_j) r'$ et $i = j$ et $\deg l < \deg l'$.

L'idée est que les deux symboles $s, t, e$ sont présents aux extrémités du mot pour pouvoir faire des opérations sur le premier $a$ ou sur le dernier $b$. Le premier $a$ va se transformer en $c$ en générant un $x$, les autres $a$ vont absorber un $y$, et générer un $x$ en se tranformant en $c$. Le dernier $b$ va absorber un $x$, générer un $z$ et se transformer en $d$, les autres $b$ vont absorber un $x$, et générer un $y$ en se transformant en $d$. Les $x$ et les $y$ sont des "messages" qui commutent avec les $a$ et les $d$. Un $x$ "dit" à la frontière entre les $b$ et les $d$ qu'un $a$ s'est transformé en $c$, alors qu'un $y$ "dit" à la frontière entre les $a$ et les $c$ qu'un $b$ s'est transformé en $d$, l'objectif étant que pour comparer le nombre de $a$ et de $b$, il y ait autant de transformations de chaque type. Le $z$ est le message qui permet de retransformer les $d$ en $b$ et les $c$ en $a$ à la fin du processus. On reparlera du rôle de $\infty$ plus tard.

Pour mieux comprendre, prenons $n = 2$. Le monôme $(1, 11, a^2b^2e)$ est un

monôme dominant de syzygie car on a les réécritures suivantes :

$$\begin{aligned} saabbe &=_1 tcxabbe =_2 tcaxbbe =_6 tcadybe \\ &=_5 tcaydbe =_4 tcyadbe =_7 tccxdbe \\ &=_3 tccdxbe =_8 tccddze =_9 tccdzbe \\ &=_9 tcczbbe =_{10} tczabbe =_{10} tzaabbe \\ &=_{11} saabbe \end{aligned}$$

**Fait.** *Les monômes dominants des syzygies de la suite de polynômes précédente ne forment pas un langage régulier.*

*Démonstration.* Nous allons montrer que l'ensemble des monômes dominants des syzygies de la forme $(1, 11, a^n b^m e)$ vérifient $n = m$. Cela conclura, puisque si l'on note $X$ l'ensemble des monômes dominants des syzygies, si $X$ était régulier, alors son intersection avec le langage régulier $\{(1, 11, a^n b^m e) \mid n, m \geq 1\}$ devrait être régulier, or cette intersection est le langage $\{(1, 11, a^n b^n e) \mid n \geq 1\}$, qui n'est clairement pas régulier par le lemme de pompage.

Soit $n \geq 1$, commençons par montrer $(1, 11, a^n b^n e)$ est un monôme dominant de syzygie. On vérifie que :

$$
\begin{aligned}
(1,1,a^{n-1}b^ne) &+ \sum_{k=2}^{n}(tc^{k-2},7,a^{n-k}d^{k-1}b^{n-k+1}e)\\
&+ \sum_{k=1}^{n-1}(tc^ka^{n-k}d^{k-1},6,b^{n-k-1}e)\\
&+ (c^nd^{n-1},8,1)\\
&+ (1,11,a^nb^ne)\\
&+ \sum_{k=1}^{n}(tc^nd^{n-k},9,b^{k-1}e)\\
&+ \sum_{k=1}^{n}(tc^{n-k},10,a^{k-1}b^ne)\\
&+ \sum_{k=1}^{n}\sum_{l=0}^{n-k-1}(tc^ka^l,2,a^{n-l-k-1}d^{k-1}b^{n-k+1}e)\\
&+ \sum_{k=1}^{n}\sum_{l=0}^{k-2}(tc^ka^{n-k}d^l,3,d^{k-2-l}b^{n-k-1}e)\\
&+ \sum_{k=1}^{n-1}\sum_{l=0}^{k-1}(tc^ka^{n-k}d^l,5,d^{k-1-l}b^{n-k-2}e)\\
&+ \sum_{k=1}^{n-1}\sum_{l=0}^{n-k-1}(tc^ka^l,4,a^{n-l-k-1}d^kb^{n-k}e)
\end{aligned}
$$

est une syzygie de monôme dominant $(1,11,a^nb^ne)$.

Soit $\sigma$ une syzygie de monôme dominant $(1,11,a^nb^me)$, et essayons de montrer que $n=m$. Soit $G$ le graphe dont les sommets sont les éléments de $M$, et pour chaque $\alpha(l,i,r)$ terme de $\sigma$, si $g_i$ s'écrit $X-Y$, on crée un arc entre $lXr$ et $lYr$. Alors, soit $W$ l'ensemble des sommets d'une des formes suivantes :

$$
\begin{aligned}
&sa^nb^ne,\\
&tc^pa^qxa^rd^nb^me,\\
&tc^pa^qd^rxd^nb^me,\\
&tc^pa^qya^rd^nb^me,\\
&tc^pa^qd^ryd^nb^me,\\
&tc^pza^qb^re,\\
&tc^pd^qzb^re
\end{aligned}
$$

Chaque sommet de $W$ ne peut être relié qu'à des sommets de $W$, et chaque sommet de $W$ est relié à au plus deux sommets. Ainsi, la composante connexe

de $sa^n b^n e$ dans $\sigma$ est une chaîne ou un cycle. Comme $\sigma$ est une syzygie, il doit s'agir d'un cycle, ce qui impose $n = m$.

□

On pourrait remarquer que la suite de polynômes n'admet pas forcément de base de Gröbner finie. Cependant, grâce à l'astuce suivante, on peut transformer l'exemple précédent pour qu'il ait une base de Gröbner finie : on ajoute $\infty$ à la suite des polynômes, et pour toute lettre $\alpha$, on ajoute $\infty - \alpha$ à la suite des polynômes.

La nouvelle suite de polynômes ainsi contruite a une base de Gröbner finie ; elle contient pour tout symbole $\alpha$ le polynôme $\alpha$. Soit $X$ l'ensemble des monômes dominants des syzygies avant la transformation, $Y$ l'ensemble des monômes dominants des syzygies après la transformation, et $Z$ le langage :

$$\{(l, i, r) \in \mathcal{M} \times \mathbb{N} \times \mathcal{M} \mid l \operatorname{LM}(g_i) r \text{ ne contient pas } \infty\}$$

On a :

$$X = Y \cap Z$$

Comme $Z$ est un langage régulier, si $Y$ était un langage régulier, alors $X$ le serait aussi. Le langage $Y$ n'est donc pas régulier.

On a donc construit une suite de polynômes qui admet une base de Gröbner finie, mais dont l'ensemble des monômes dominants des syzygies n'est pas un langage régulier.

De plus, on peut rendre l'ordre isomorphe à $\mathbb{N}$ en choisissant deglex et en remplaçant le symbole $\infty$ par $\infty^{10}$ et $s$ par $s^5$, car les degrés varient d'au plus une constante lors des réécritures contenues dans une syzygie.

## Langage algébrique ?

La question naturelle suivante est de se demander s'il existe un automate à pile qui reconnaît les monômes dominants des syzygies. Il se trouve que la technique de la section précédente se généralise : on utilise le même genre de construction, en utilisant que le langage $\{a^n b^n c^n \mid n \in \mathbb{N}\}$ n'est pas algébrique. On en déduit que les monômes dominants de syzygies ne sont pas toujours reconnaissables par un automate à pile. Comme dans le cas du langage régulier, on peut modifier l'exemple pour que l'ordre soit isomorphe à $\mathbb{N}$, car les degrés varient d'au plus une constante lors des réécritures contenues dans une syzygie.

## Langage décidable

Si l'ordre monomial est isomorphe pour les ordres à $\mathbb{N}$, il existe bien un algorithme pour décider si un triplet $(l, i, r)$ est un monôme dominant de syzygie, mais il s'avère qu'il est très peu efficace : on considère l'espace vectoriel $V$ engendré par les triplets plus petits que $(l, i, r)$, qui est de dimension finie. Décider si $(l, i, r)$ est un monôme dominant de syzygie revient à décider s'il

existe des éléments $\sigma$ de $V$ tel que le coefficient de $(l, i, r)$ dans $\sigma$ est 1, et tel que $E(\sigma) = 0$, ce qui revient à décider si un système linéaire avec un nombre fini d'équations admet des solutions, ce qui est bien enten du décidable.

En revanche, si l'ordre monomial n'est pas isomorphe à $\mathbb{N}$, alors il n'existe pas forcément d'algorithme pour décider si un triplet $(l, i, r)$ est un monôme dominant de syzygie. Nous avons en effet trouvé une construction qui ramène ce problème au problème de l'arrêt.

Soit $m_1, \ldots, m_n$ les différents états d'une machine de Turing, son ruban de travail est constitué des symboles 0 et 1. On suppose que la machine de Turing termine si et seulement si elle atteint l'état $m_n$.

Considérons :

$$\Sigma := \{l_1, \ldots, l_n, l'_1, \ldots, l'_n, r_1, \ldots, r_n, r'_1, \ldots, r'_n, 0, 1, 0', 1', s, e, u^r_1, \ldots, u^r_n, u^l_1, \ldots, u^l_n, \infty\}$$

Avec $u^r_n = r_n$ et $u^l_n = l_n$ .

Les règles d'exécution de la machine de Turing déterministe sont de la forme $(m_i, a) \to (m_j, b, d)$ où $a, b \in \{0, 1\}$ et $d$ est un déplacement à gauche ou à droite.

Pour une telle règle, on rajoute donc :

— Si le déplacement est à droite :

$$\begin{aligned} r_i a &- r'_i a' b r_j \\ a l_i &- l'_i a' b r_j \\ u^r_i a &- r'_i a' b u^r_j \\ a u^l_i &- l'_i a' b u^r_j \end{aligned}$$

— Si le déplacement est à gauche :

$$\begin{aligned} r_i a &- r'_i a' l_j b \\ a l_i &- l'_i a' l_j b \\ u^r_i a &- r'_i a' u^l_j b \\ a u^l_i &- l'_i a' u^l_j b \end{aligned}$$

Les $l_i, r_i, u^l_i, u^r_i$ commutent avec les $l'_i, r'_i, 0', 1'$.

On rajoute de plus les règles :

$$\begin{aligned} r_i e &- r_i 0 e \\ u^r_i e &- u^r_i 0 e \\ s r_1 e &- s \infty e \\ s u^r_1 e &- s \infty e \end{aligned}$$

Ainsi, une suite de réécriture à partir de $sr_1e$ peut-être vu comme une exécution de la machine de Turing avec historique sur le ruban vide. Décider si une telle machine de Turing s'arête est bien sur indécidable.

Ainsi, $s\infty e$ correspond à un monôme dominant de syzygie si et seulement si la machine de Turing s'arrête sur le ruban vide.

# Conclusion

La motivation de départ, qui était d'adapter l'algorithme GVW au cadre non-commutatif, s'est révélé être un problème plus hardu que prévu ; après avoir posé des définitions qui découlaient naturellement du cadre commutatif, nous nous sommes rendus compte que le point central de l'algorithme, c'est à dire le calcul de la base de Gröbner forte, ne terminait pas. Nous avons alors essayé de démontrer des obstructions à la terminaison d'un algorithme naïf à signature, objectif que nous avons partiellement réussi.

# Références


[1] Buchberger B. "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal." Thèse de doct. Leopold-Franzens University, 1965.

[2] Faugère J. C. "A new efficient algorithm for computing Gröbner bases (F4)". In : *Journal of Pure and Applied Algebra* 139.1 - 3 (1999), p. 61-88.

[3] Faugère J. C. "A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)". In : *ISSAC '02 : Proceedings of the 2002 international symposium on Symbolic and Algebraic Computation* (2002), p. 75-83.

[4] Hofstadler C. et Verron T. "Signature Gröbner bases, bases of syzygies and cofactor reconstruction in the free algebra". In : *arXiv :2107.14675* ().

[5] Vaccon T. Caruso X. et Verron T. "Signature-based algorithms for Gröbner bases over Tate algebras". In : *ISSAC'20 : Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation* (2020), p. 70-77.

[6] Kapur D. et Narendran P. "A finite Thue system with decidable word problem and without equivalent finite canonical system". In : *Theoretical Computer science* 35.2 – 3 (1985), p. 337-344.

[7] Guan Y. Gao S. et Volny IV F. "A new incremental algorithm for computing Gröbner bases". In : *ISSAC'10 : Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation* (2010), p. 13-19.

[8] Wang M. Gao S. et Volny IV F. "A new framework for computing Gröbner bases". In : *Mathematics of computation* 85.297 (2016), p. 449-465.

[9] Hu Y. Pan S. et Wang B. "The Termination of Algorithms for Computing Gröbner Bases". In : *arXiv :1202.3524* (2012).

[10] Mora T. "An introduction to commutative and noncommutative Gröbner bases". In : *Theoretical Computer Science* 134.1 (1994), p. 131-173.

# Annexe

Considérons un exemple supplémentaire sur les lettres $t, x, a, b$. Sur les monômes, nous utiliserons l'ordre deglex pour $a < b < t < x$ (qui est isomorphe à $\mathbb{N}$).

Prenons :

$$g_1 := xt - ta$$
$$g_2 := xt - tb$$
$$g_3 := b - a$$

Il n'y a aucune paire critique, il s'agit donc bien d'une base de Gröbner.

Maintenant, sur $\mathcal{M} \times \{1, 2, 3\} \times \mathcal{M}$, nous définissons un ordre (qui est isomorphe à $\mathbb{N}$), où nous avons $(l, i, r) \leq (l', j, r')$ si l'une des conditions ci-desous est vérifiée :

- $\deg l \operatorname{LM}(g_i)r < \deg l' \operatorname{LM}(g_j)r'$
- $\deg l \operatorname{LM}(g_i)r = \deg l' \operatorname{LM}(g_j)r'$ et $i < j$.
- $\deg l \operatorname{LM}(g_i)r = \deg l' \operatorname{LM}(g_j)r'$ et $i = j$ et $\deg r < \deg r'$.
- $\deg l \operatorname{LM}(g_i)r = \deg l' \operatorname{LM}(g_j)r'$ et $i = j$ et $\deg r = \deg r'$ et $l \operatorname{LM}(g_i)r \geq l' \operatorname{LM}(g_j)r'$.

On définit le degré d'un chemin de réduction comme le degré maximal d'un de ses termes, où le degré d'un terme est défini par :

$$\deg (l, i, r) = \deg l \operatorname{LM}(g_i)r$$

**Lemme.** *Dans cet exemple, $M$ n'admet pas de base de Gröbner forte.*

*Démonstration.* Supposons par l'absurde que $M$ admette une base de Gröbner forte $G_f$. On peut réduire chaque élément de monôme dominant non-nul de $G_f$ par les syzygies de $G_f$, et ainsi, on peut supposer sans perte de généralité qu'ils sont tous irréductibles (et pas seulement en tête !) par les syzygies.

**Fait.** *Dans cet exemple, pour tout sigpolynôme $(\sigma, f)$ de $G_f$, $\deg \operatorname{LM}(f) = \deg \operatorname{LM}(\sigma)$.*

*Démonstration.* Nous sommes dans un cas homogène : dans le cas contraire, les termes de degré $\deg \operatorname{LM}(\sigma)$ dans $\sigma$ formeraient une syzygie, ce qui contredit l'hypothèse que $(\sigma, f)$ est irréductible par les syzygies. □

Pour tout $n \in \mathbb{N}$,

$$\left( -(x^n, 2, 1) - \sum_{i=0}^{n-1} (x^i, 1, a^{n-1-i}b) + \sum_{i=0}^{n} (x^i, 1, a^{n-i}), ta^n b - ta^{n+1} \right)$$

est dans $M$ donc doit être réductible en tête par un élément $(\sigma_n, f_n)$ de $G_f$, il existe donc $l, r \in \mathcal{M}$ tels que :

$$l \operatorname{LM}(f_n)r = ta^n b$$
$$l \operatorname{LM}(\sigma_n)r \leq (x^n, 2, 1)$$

On choisit maintenant $n$ tel que le degré de $ta^n b$ est strictement plus grand que le plus grand degré d'un monôme dominant d'un élément de $G_f$. Dans ce cas, $\mathrm{LM}(f_n)$ est d'une des formes : $a^k$, $a^k b\ ta^k$.

— Cas où $\mathrm{LM}(f_n)$ ne contient pas de $t$. Dans ce cas, le terme $\mathrm{LM}(f_n)$ peut seulement apparaître grâce à un terme de la forme $(u, 3, v)$ dans $\sigma_n$, avec $\deg(u, 3, v) = \deg \mathrm{LM}(f_n)$, ce qui une contradiction car :

$$(lu, 3, vr) \leq l\,\mathrm{LM}(\sigma_n)r \leq (x^n, 2, 1)$$

Avec $\deg(lu, 3, vr) = \deg(x^n, 2, 1)$.

— Cas $\mathrm{LM}(f_n) = ta^k$. Ce cas est impossible : le terme $ta^k$ ne peut être réécrit qu'en des termes de même degré lexicographiquement plus grands par les règles données.

Les deux cas mènent donc à une contradiction. □

Définissons une syzygie particulière :

$$\sigma := (t, 3, 1) + (1, 2, 1) - (1, 1, 1)$$

**Lemme.** *L'union de $\{\sigma\}$ et des syzygies principales est une base de Gröbner des syzygies.*

*Démonstration.* Nous voulons montrer que toute syzygie non-nulle est réductible en tête par $\sigma$ ou par l'une des syzygies principales. Pour cela, comme l'ordre est isomorphe à $\mathbb{N}$, il suffit de montrer que toute syzygie non-nulle est réductible (pas forcément en tête), car en répétant les réductions, on finira par réduire le monôme dominant, ce qui nous donnera une réduction en tête.

Considérons une syzygie non-nulle $s$, dont on veut montrer qu'elle est réductible par $\sigma$ ou par l'une des syzygies principales.

Chaque règle étant de la forme $\alpha_i - \beta_i$, on peut poser

$$m := \min_{(l,i,r)} \min_{\text{monôme de } s} l\beta_i r$$

Comme $E(s) = 0$, il existe au moins deux monômes distincts de $s$, $(l_1, i_1, r_1)$ et $(l_2, i_2, r_2)$, tels que $l_1\beta_{i_1} r_1 = l_2\beta_{i_2} r_2 = m$. On ne peut pas avoir $l_1 = l_2$ et $r_1 = r_2$, car dans ce cas, on doit avoir $\beta_{i_1} = \beta_{i_2}$, d'où $i_1 = i_2$ ce qui est impossible.

Si $\deg l_1 \geq \deg l_2\beta_{i_2}$ ou $\deg l_2 \geq \deg l_1\beta_{i_1}$, on peut supposer par symétrie que $m$ s'écrive :

$$m_1\beta_{i_1} m_2 \beta_{i_2} m_3$$

On a alors :

$$(l_1, i_1, r_1) = (m_1, i_1, m_2\beta_{i_2} m_3)$$
$$(l_2, i_2, r_2) = (m_1\beta_{i_1} m_2, i_2, m_3)$$

On voit alors que $s$ est réductible par la syzygie principale :

$$m_1(g_{i_1}(m_2, i_2, 1) - (1, i_1, m_2)g_{i_2})m_3$$

Sinon, les deux occurences, de $\beta_{i_1}$ et $\beta_{i_2}$, choisies dans $m$ ont une intersection non-vide mais ne coincident pas. Cela n'est possible que si $\{i_1, i_2\} = \{1, 3\}$. Supposons par symétrie $i_1 = 1$ et $i_2 = 3$, dans ce cas, $m$ s'écrit :

$$m_1 t a m_2$$

On a alors :

$$(l_1, i_1, r_1) = (m_1, 1, m_2)$$
$$(l_2, i_2, r_2) = (m_1 t, 3, m_2)$$

On voit alors que $s$ est réductible par la syzygie :

$$m_1 \sigma m_2$$

N'importe quelle syzygie non-nulle est donc réductible. □

Cela répond par la négative à une conjecture ouverte.