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

Arthur Léonard

2021

Introduction

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. Si pour tout $f \in I$, il existe $g \in G$ tel que $\mathrm{LM}(g) \mid \mathrm{LM}(f)$, on dit que G est une base de Gröbner de I.*

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 $g_1, \ldots, g_m$, 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. 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.
- $g_3 s - tag_1 = taa - aas$, 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 qu'il est difficile de garantir la terminaison d'un algorithme à signature.

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

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

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

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

on notera :

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

— $\mathrm{LC}(\sigma) := \alpha_{\mathrm{LM}(\sigma)}$ le coefficient dominant de σ.

— $\mathrm{LT}(\sigma) := \mathrm{LC}(\sigma)\,\mathrm{LM}(\sigma)$ le terme dominant de σ.

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

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

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

Pour $p = (\sigma, f) \in \mathbb{K}[\mathcal{M} \times \{1, \ldots, m\} \times \mathcal{M}] \times \mathbb{A}$, 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 (σ, f) est réductible en tête par le sigpolynôme (σ', 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 $\sigma \in \mathbb{K}[\mathcal{M} \times \{1, \ldots, m\} \times \mathcal{M}]$ tel que $E(\sigma) = f$, d'où $(\sigma, f) \in M$. Choisissons un σ 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 (σ, f) est réductible en tête par (σ', 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), c'est qu'un algorithme qui calcule une base de Gröbner forte 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 σ 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 $\mathbb{K}[\mathcal{M} \times \{1, \ldots, m\} \times \mathcal{M}]$ engendré par les :*

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

On dira que la suite $(g_1, \ldots, g_m)$ 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 gérateur 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 dans une version simple, ce qui a permis d'observer qu'il terminait très rarement. En effet, dans le cas d'une suite régulière, un algorithme à signature déterminerait donc d'une manière ou d'une autre les monômes dominants des syzygies principales. Dans le cas commutatif, cette base est finie, et même très simple à caractériser : dans le cas incrémental, il s'agit des monômes qui sont divisibles par un des monômes dominants de la base de Gröbner G_0. 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 au moins traiter les syzygies principales de manière différente.

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 :

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

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

— $l\,\mathrm{LM}(g_i)r = l'\,\mathrm{LM}(g_j)r'$ 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 σ une syzygie non-nulle. On construit un graphe G_σ de la manière suivante :

— Les sommets de G_σ sont les

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

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

— Chaque sommet w est étiqueté

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

— Le fait que σ 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 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 σ 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 σ 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 σ 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 σ 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 LM_s l'ensemble des monômes dominants des syzygies, on cherche à déterminer 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 σ 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 σ 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).