Correspondances entre les algorithmes de Knuth-Bendix et de Buchberger

Benoît Robin

Rapport rédigé dans le cadre de l'Unité d'Enseignement TIPE
de l'Université Claude Bernard Lyon 1
et encadré par Philippe Malbos

Résumé

Ce rapport présente une analogie entre deux algorithmes issus de domaines distincts de l'algèbre. L'un concerne l'étude des polynômes à plusieurs indéterminées, tandis que l'autre concerne les systèmes de réécriture.

Table des matières

1 Introduction

Introduction. En algèbre appliquée, de nombreux problèmes de modélisation se formulent en terme d'équations polynomiales. L'étude des idéaux de polynômes à plusieurs indéterminées permet de résoudre des systèmes d'équations polynomiales à plusieurs inconnues, grâce à des méthodes algorithmiques.

Par ailleurs, la réécriture de mots est un modèle de calcul utilisé en algèbre et en informatique. Elle permet, en particulier, de résoudre le problème du mot. Il s'agit de la question de l'égalité de deux mots dans un monoïde. Bien que ce problème soit généralement indécidable, il existe aussi des méthodes algorithmiques qui décident le problème dans certains cas.

Le but de ce TIPE est d'étudier les correspondances existantes entre ces différents algorithmes issus de domaines distincts.

Le problème de l'appartenance à un idéal. L'ensemble des polynômes à plusieurs indéterminées forme un anneau commutatif, noté $\mathbb{K}[x_1, \ldots, x_n]$. Un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ est un sous-ensemble de cet anneau, stable pour l'addition et la multiplication. On peut définir des idéaux de $\mathbb{K}[x_1, \ldots, x_n]$ à partir d'une famille de polynômes, appelée *base de l'idéal*. L'idéal correspond alors à l'ensemble des combinaisons de polynômes de la base. Cette définition invite au problème suivant : comment savoir si un polynôme donné appartient à l'idéal engendré par une base donnée ? La division euclidienne peut répondre à cette question.

Exemple. Dans $\mathbb{R}[x]$, soient trois polynômes

$$f = x^2 - x,\ g = x - 1 \text{ et } h = x^3 - 1.$$

On cherche à savoir si le polynôme h appartient à l'idéal $I = \langle f, g \rangle$. On procède alors à la division de h par f.

$$\begin{array}{rr|l} x^3 & -1 & x^2 - x \\ \cline{3-3} x^3 - x^2 & & x + 1 \\ \cline{1-2} x^2 & -1 & \\ x^2 - x & & \\ \cline{1-2} x - 1 & & \end{array}$$

Puis on divise le reste par le polynôme g.

$$\begin{array}{r|l} x - 1 & x - 1 \\ \cline{2-2} x - 1 & 1 \\ \cline{1-1} 0 & \end{array}$$

Ainsi, le reste de la division euclidienne de h par f et g est nul. Donc h appartient à I.

Toutefois, cette méthode n'est pas toujours conluante.

Exemple. En effet, dans $\mathbb{R}[x]$, si

$$f = x^2 - 1,\ g = x^2 - x \text{ et } h = x - 1,$$

alors aucun des termes de h n'est divisible par le terme x^2, qui est le terme dominant de f et de g. Autrement dit, le reste de la division euclidienne de h par (f, g) est $h \neq 0$. Pourtant, $h = f - g$ appartient à l'idéal engendré par f et g.

Le problème est le même dans le cas de polynômes à plusieurs indéterminées. Mais avant de poser la division, il faut alors définir un ordre sur les monômes, appelé *ordre monomial*

Exemple. Dans $\mathbb{R}[x, y]$, soient trois polynômes

$$f = x^2y - x,\ g = xy^2 - y^2 \text{ et } h = xy^2 - xy.$$

On cherche à savoir si le polynôme h appartient à l'idéal $I = \langle f, g\rangle$. On essaye d'appliquer la méthode de la division euclidienne, en considérant l'odre lexicographique. Aucun des termes du polynôme h n'est divisible par le terme dominant de f qui est x^2y. Donc on divise le polynôme h par le second polynôme générateur g.

$$\begin{array}{rr|l} xy^2 - xy & & xy^2 - y^2 \\ \cline{3-3} xy^2 & - y^2 & 1 \\ \cline{1-2} & - xy + y^2 & \end{array}$$

On obtient le polynôme $-xy + y^2$ comme reste de la division. Ce reste n'est divisible ni par le terme dominant de f, ni par celui de g. Il s'agit donc du reste de la division de h par (f, g). Bien que ce reste soit non nul, le polynôme h appartient à I, puisque

$$h = yf - xg.$$

Donc la division euclidienne ne permet pas toujours de déterminer l'appartenance d'un polynôme à un idéal. Pour résoudre le problème de l'appartenance à un idéal, une méthode consiste à trouver, pour un idéal donné, une base qui respecte cette équivalence entre la nullité du reste de la division d'un polynôme par cette base et l'appartenance de ce polynôme à l'idéal. On appellera *bases de Gröbner* ces familles de polynômes aux propriétés nombreuses.

Le mathématicien Buchberger a créé un algorithme qui, pour tout idéal, calcule une base de Gröbner. Cet algorithme termine avec succès en un nombre fini d'étape.

Le problème du mot dans un monoïde. Par ailleurs, on s'intéresse aux présentations de monoïdes. Un *monoïde* est un ensemble muni d'une loi de composition interne associative et d'un élément neutre.

Soit X un ensemble fini, alors l'ensemble $X^* = \{a_1 \dots a_s \mid a_1, \dots, a_s \in X\}$ est le monoïde libre engendré par les éléments de X, alors appelés *générateurs*. Si $\mathcal{R} \subset X^* \times X^*$ est un ensemble de *relations* sur X^*, alors la *congruence* générée par $\mathcal{R}$, notée $\longleftrightarrow^*_{\mathcal{R}}$, est définie pour tous mots u et v de Σ^* par :

– $uxv \longleftrightarrow_{\mathcal{R}} uyv$, si u et v sont dans Σ^* et $\big((x, y) \in \mathcal{R}$ ou $(y, x) \in \mathcal{R}\big)$,

– $x \longleftrightarrow^*_{\mathcal{R}} y$, si $x \longleftrightarrow_{\mathcal{R}} \dots \longleftrightarrow_{\mathcal{R}} y$.

Une présentation d'un monoïde M est la donnée d'un ensemble Σ, appelé *alphabet*, et d'un ensemble $\mathcal{R}$ de relations sur Σ^*, de telle manière que le monoïde M soit isomorphe à l'ensemble de mots engendré par l'alphabet, quotienté par la relation de congruence :

$$M \cong {}^{\Sigma^*}\!/_{\longleftrightarrow^*_{\mathcal{R}}}.$$

La réécriture consiste à orienter les relations, qui deviennent alors des *règles*, formant un *système de réécriture*. Si $(\Sigma, \mathcal{R})$ est une présentation, et u et v sont deux mots de Σ^* tels que $u\mathcal{R}v$, alors on note $u \longrightarrow v$ la règle correpondante. Si x et y sont deux mots de Σ^*, alors on peut *réduire* le mot xuy ; on note $xuy \longrightarrow_{\mathcal{R}} xvy$. On dit qu'une présentation $(\Sigma, \mathcal{R})$ est *noethérienne* ou qu'elle *termine* si on ne peut pas réduire un mot une infitnité de fois. Elle est dite confluente si toutes les *réductions* d'un mot u mènent à un unique mot, appelé alors *forme normale* du mot u. Une présentation est dite *convergente* si elle est à la fois noethérienne et confluente. De telles présentations peuvent être utilisées pour décider du problème du mot : pour deux mots u et v de Σ^*, a-t-on $u = v$ dans M ? En effet, si une présentation possède à la fois les propriétés de terminaison et de confluence, alors il suffit d'appliquer l'algorithme de la forme normale pour résoudre le problème du mot. Cet algorithme consiste à réduire les deux mots u et v en leurs formes normales u' et v', qui existent, puisque la présentation termine, et qui sont uniques, puisque la présentation est confluente. Ensuite il suffit de vérifier si $u' = v'$, auquel cas on a bien $u = v$ dans M.

En revanche, si la présentation n'est pas convergente, l'algorithme de Knuth-Bendix permet de compléter l'ensemble de règles de la présentation, afin d'obtenir une nouvelle présentation convergente du monoïde. Toutefois l'algorithme de Knuth-Bendix ne réussit pas toujours.

Relations entre problème du mot et appartenance à un idéal. En fait, on peut voir le problème de l'appartenance à un idéal et le problème du mot comme un même problème. Pour cela, on associe à chaque polynôme f d'une base donnée la règle

$$LT(f) \xrightarrow{f} LT(f) - f.$$

Ainsi, la forme normale d'un polynôme correspond au reste de sa division par les polynômes de la base. On remarque alors que seule une base de Gröbner génère une relation de réduction convergente. Ces correspondances se synthétisent dans ce théorème fondamental :

Théorème. *Une base $G = \{g_1, \ldots, g_t\}$ d'un idéal I est une base de Gröbner de I si, et seulement si, la relation de réduction $\xrightarrow{G}$ est confluente.*

Ainsi, on peut calculer des bases de Gröbner grâce à une méthode plus simple et intuitive que le calcul des *S-polynômes* de Buchberger.

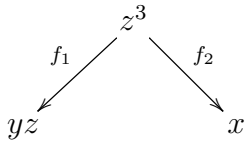
Exemple. Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{R}[x, y, z]$ avec

$$f_1 = y - z^2, \quad f_2 = x - z^3.$$

Considérons l'ordre lexicographique induit par l'ordre alphabétique $x < y < z$. On obtient alors deux règles

$$z^2 \xrightarrow{f_1} y \quad \text{et} \quad z^3 \xrightarrow{f_2} x.$$

On remarque que le monôme z^3 peut être réduit par les deux règles. On parle alors de *paire critique*.



Les polynômes yz et x sont irréductibles. Donc la paire critique n'est pas confluente, d'où (f_1, f_2) n'est pas une base de Gröbner de I pour cet ordre monomial.

Toutefois, si on considère l'ordre lexicographique induit par l'ordre lexicographique $z < y < x$, on a les règles

$$y \xrightarrow{f_1} z^2 \quad \text{et} \quad x \xrightarrow{f_2} z^3.$$

On remarque alors que les deux polynômes f_1 et f_2 ne forment pas de paires critiques, ainsi (f_1, f_2) est une base de Gröbner de I.

Cependant, l'analogie n'est pas totale. En effet, le problème de l'appartenance à un idéal est toujours décidable, contrairement au problème du mot. Cette divergence provient d'une propriété particulière de l'anneau des polynômes : la commutativité.

Organisation du document. Dans une première partie, nous étudierons l'anneau des polynômes à plusieurs indéterminées et l'algorithme de Buchberger permettant de résoudre le problème de l'appartenance à un idéal. Dans une seconde partie, nous définirons d'abord les systèmes de réécriture au sein de présentations que nous doterons des propriétés de terminaison et de confluence. Puis, nous étudierons la procédure de Knuth-Bendix, parfois utiles à la résolution du problème du mot. Il s'agira ensuite de développer les correspondances entre réécriture et bases de Gröbner.

2 L'algorithme de Buchberger

2.1 L'anneau des polynômes à plusieurs indéterminées

Dans cette partie, nous allons définir l'anneau des polynômes à plusieurs indéterminées Nous noterons $\mathbb{K}$ l'ensemble des scalaires sur lequel sont définis les anneaux de polynômes. Dans cette partie, on aura généralement $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. À l'image de ce que nous connaissons déjà pour l'anneau des polynômes à une indéterminée $\mathbb{K}[x]$, nous pouvons munir l'anneau des polynômes à plusieurs indéterminées d'une division euclidienne, nécessaire à la résolution algorithmique de problèmes liés à l'étude des idéaux. En approfondissant cette étude, nous constaterons les limites de cette division.

2.1.1 Les polynômes à plusieurs indéterminées

Définition 2.1. On appelle *monôme* en les indéterminées $x_1, \ldots, x_n$ tout produit de la forme

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n},$$

où $\alpha_1, \ldots, \alpha_n$ sont des entiers de $\mathbb{N}$. On appelle *degré total* de ce monôme la somme

$$\alpha_1 + \ldots + \alpha_n.$$

En notant $\alpha = (\alpha_1, \ldots, \alpha_n)$, on pose $x^\alpha = x_1^{\alpha_1} \ldots\ x_n^{\alpha_n}$. Par convention, $x^{(0,\ldots,0)} = 1$.

Définition 2.2. On appelle *polynôme* en les indéterminées $x_1, \ldots, x_n$ toute combinaison linéaire (finie) à coefficient dans $\mathbb{K}$ de monômes en les indéterminées $x_1, \ldots, x_n$. Un polynôme f s'écrit

$$f = \sum_\alpha a_\alpha x^\alpha,$$

où la somme est indexée par un nombre fini de n-uplets α et les a_α sont des scalaires de $\mathbb{K}$.

Proposition 2.1. *L'ensemble des polynômes en les indéterminées $x_1, \ldots, x_n$ muni de l'addition et la multiplication forme un anneau commutatif noté $\mathbb{K}[x_1, \ldots, x_n]$.*

Démonstration. Soient f, g et h trois polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. Alors on montre que
- $(f + g) + h = f + (g + h)$,
- $f + g = g + f$,
- $(fg)h = f(gh)$,
- $f(g + h) = fg + fh$,
- le polynôme 0 est l'élément neutre de l'addition,
- si $f = \sum_\alpha a_\alpha x^\alpha$, alors $-f = \sum_\alpha (-a_\alpha)\, x^\alpha$,
- le polynôme 1 est l'élément neutre de la multiplication,
- de plus, $fg = gf$.

□

Définition 2.3. Soit $f = \sum_\alpha a_\alpha x^\alpha$ un polynôme de $\mathbb{K}[x_1, \ldots, x_n]$,

– le scalaire a_α est appelé *coefficient* du monôme x^α,
– si $a_\alpha \neq 0$, alors on dit que $a_\alpha x^\alpha$ est un *terme* de f.

Exemple 2.1. Soit $f = 2x^2z + yz^3 - 1$ un polynôme de $\mathbb{R}[x, y, z]$, alors $2x^2z$ est un terme de f, x^2z est un monôme, de coefficient 2 et de degré total 3.

2.1.2 Idéaux de $\mathbb{K}[x_1, \ldots, x_n]$

Définition 2.4. On dit qu'un sous-ensemble I de $\mathbb{K}[x_1, \ldots, x_n]$ est un *idéal* si :
– 0 est élément de I,
– pour tous polynômes f et g de I, $f + g$ est un polynôme de I.
– pour tout polynôme f de I, pour tout polynôme g de $\mathbb{K}[x_1, \ldots, x_n]$, fg est un polynôme de I

Définition 2.5. Soient $f_1, \ldots, f_s$ des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, l'ensemble

$$\langle f_1, \ldots, f_s \rangle = \{\sum_{i=1}^{s} h_i f_i \mid 1 \leq i \leq s \text{ et } h_i \in \mathbb{K}[x_1, \ldots, x_n]\}$$

est appelé l'*idéal engendré* par les polynômes $f_1, \ldots, f_s$.

On remarque immédiatement que l'idéal engendré par une famille de polynômes est effectivement un idéal.

Définition 2.6. On dit qu'un idéal I de $\mathbb{K}[x_1, \ldots, x_n]$ est *finiment engendré* ou *de type fini*, s'il existe un ensemble fini $\{f_1, \ldots, f_s\}$ de polynômes de $\mathbb{K}[x_1, \ldots, x_n]$ tels que

$$I = \langle f_1, .., f_s \rangle .$$

Ces définitions amènent à se poser plusieurs questions. Nous allons nous intéresser en particulier au problème de l'appartenance à un idéal ; étant donné $I = \langle f_1, \ldots, f_s \rangle$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et un polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$, comment déterminer si f appartient à I ? Avant de rendre ce problème décidable, il nous faut introduire la notion de division euclidienne en plusieurs indéterminées.

Nous connaissons déjà la division euclidienne dans $\mathbb{K}[x]$. Etant donné deux polynômes f et g de $\mathbb{K}[x]$, il suffit en fait de diviser le terme de plus haut degré de f par celui de g puis de soustraire à f le résultat obtenu multiplié par g, puis de répéter ces instructions jusqu'à obtenir un polynôme, appelé *reste*, dont le degré est inférieur au degré de g ou qui est nul.

Dans le cas des polynômes à plusieurs indéterminées, il nous manque la notion de terme de plus haut degré. En effet, même si on regarde le degré total de chaque monôme d'un polynôme, on peut trouver deux monômes différents de même degré total. Par exemple, x^2y^3 et x^3y^2 ont pour degré total 5. Cette notion ne convient donc pas pour ordonner de manière totale tous les monômes d'un polynôme.

2.1.3 Ordres monomiaux

Par la suite, on notera

$$\mathcal{M}(x_1, \ldots, x_n) = \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$$

l'ensemble des monômes en les indéterminées $x_1, \ldots, x_n$.

Définition 2.7. Un *ordre monomial* sur $\mathcal{M}(x_1, \ldots, x_n)$ est une relation $<$ sur $\mathcal{M}(x_1, \ldots, x_n)$ telle que :

- $<$ est un ordre total,
- pour tous monômes $x^\alpha, x^\beta, x^\gamma$ de $\mathcal{M}(x_1, \ldots, x_n)$, si $x^\alpha < x^\beta$, alors $x^\alpha x^\gamma < x^\beta x^\gamma$,
- pour tout monôme x^α de $\mathcal{M}(x_1, \ldots, x_n)$ distinct de 1, $1 < x^\alpha$.

Exemple 2.2 (L'ordre lexicographique)**.** On définit d'abord un ordre sur l'ensemble des indéterminées, généralement l'ordre alphabétique défini par $x_n < \ldots < x_2 < x_1$. On définit l'ordre lexicographique en posant $x^\alpha <_{lex} x^\beta$, si le premier coefficient non nul du n-uplet $\beta - \alpha$ est positif.

Par exemple, dans $\mathcal{M}(x, y, z)$, $x^3y^4z <_{lex} x^3y^2z^4$ puisque $(3, 4, 1) - (3, 2, 4) = (0, 2, -3)$ et $2 > 0$.

On peut démontrer que l'ordre lexicographique est un ordre monomial.

Exemple 2.3 (L'ordre lexicographique par degré)**.** On le définit en posant $x^\alpha <_{grlex} x^\beta$ si

$$\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \text{ ou } \big(\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \text{ et } x^\alpha <_{lex} x^\beta\big).$$

Ainsi, dans $\mathcal{M}(x, y, z)$, $x^3y^4 <_{grlex} x^2y^3z^4$ puisque $3 + 4 + 0 < 2 + 3 + 4$.

L'ordre du degré lexicographique est aussi un ordre monomial.

Proposition 2.2. *Soit $<$ un ordre monomial sur $\mathcal{M}(x_1, \ldots, x_n)$. Soient x^α et x^β deux monômes de $\mathcal{M}(x_1, \ldots, x_n)$, on a*

$$\textit{si } x^\alpha \textit{ divise } x^\beta, \textit{ alors } x^\alpha < x^\beta$$

Démonstration. En effet, si x^α divise x^β, alors il existe un monôme x^γ de $\mathcal{M}(x_1, \ldots, x_n)$ tel que $x^\beta = x^\alpha x^\gamma$. Or, par définition, $1 < x^\gamma$ d'où $x^\alpha.1 < x^\alpha.x^\gamma$. Donc $x^\alpha < x^\beta$. □

Proposition 2.3. *Tout ordre monomial est un bon ordre.*

Définition 2.8. Soit $<$ un ordre monomial sur $\mathcal{M}(x_1, \ldots, x_n)$. Soit f un polynôme de $\mathbb{K}[x_1, \ldots, x_n]$. Le polynôme f peut s'écrire sous la forme

$$f = a_1x^{\alpha_1} + \ldots + a_rx^{\alpha_r}$$

où $a_1, \ldots, a_r$ sont des scalaires de $\mathbb{K}$ et $x^{\alpha_1}, \ldots, x^{\alpha_r}$ sont des monômes de $\mathcal{M}(x_1, \ldots, x_n)$, tels que $x^{\alpha_1} < \ldots < x^{\alpha_r}$. On dit que :

– le n-uplet α_1 est le *multidegré* de f, que nous noterons $mulitdeg(f)$,
– le coefficient a_1 est le *coefficient dominant* de f, que nous noterons $LC(f)$,
– le monôme x^{α_1} est le *monôme dominant* de f, que nous noterons $LM(f)$,
– le terme $a_1 x^{\alpha_1}$ est le *terme dominant* de f, que nous noterons $LT(f) = LC(f)LM(f)$.

Exemple 2.4. On considère l'ordre lexicographique, avec l'ordre alphabétique $z < y < x$. Le polynôme

$$f = x^2y^2z - x^2yz^3 + 2y^4z^4$$

a pour multidegré $(2, 2, 1)$, pour coefficient dominant 1, pour monôme dominant x^2y^2z et pour terme dominant x^2y^2z. Si on considère l'ordre lexicographique par degré, alors $multideg(f) = (0, 4, 4)$, $LC(f) = 2$, $LM(f) = y^4z^4$ et $LT(f) = 2y^4z^4$.

2.1.4 Algorithme de division en plusieurs indéterminées

Théorème 2.1. *Soient $<$ un ordre monomial sur $\mathcal{M}(x_1, \ldots, x_n)$ et $F = (f_1, \ldots, f_s)$ un s-uplet de polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. Alors tout polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$ peut s'écrire sous la forme*

$$f = a_1f_1 + \ldots + a_sf_s + r$$

où a_i et r sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$ et soit $r = 0$ soit aucun des monômes de r n'est divisible par $LT(f_1), \ldots, LT(f_s)$.

On dit alors que r est le reste *de la division de f par F et on écrit*

$$f \xrightarrow{F} r.$$

De plus, si $a_if_i \neq 0$, alors $multideg(f) \geq multideg(a_if_i)$.

Il existe un algorithme qui retourne, pour un polynôme donné f et une famille donnée F de polynômes, les polynômes a_i et r du théorème précédent. Cet algorithme termine en un nombre fini d'étapes. On dit alors qu'on effectue la division euclidienne du polynôme f par la famille de polynômes F.

Entrées : $f_1, \ldots, f_s, f$
Sorties : $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots; a_s := 0; r := 0;$
$p := f;$
tant que $p \neq 0$ **faire**
  $i := 1;$
  $div := faux;$
  tant que $i \leq s$ *ET* div=*faux* **faire**
    si $LT(f_i) | LT(p)$ **alors**
      $a_i := a_i + LT(p)/LT(f_i);$
      $p := p - (LT(p)/LT(f_i))f_i;$
      $div := vrai;$
    sinon
      $i := i + 1;$
  fin
  si $div = faux$ **alors**
    $r := r + LT(p);$
    $p := p - LT(p);$
fin

À présent, nous possédons un test de divisibilité des polynômes ; on dit qu'un polynôme f est divisible par une famille F de polynôme si le reste de la division de f par F est le polynôme nul. On en déduit immédiatement l'implication suivante :

$$\text{si } (f_1, \ldots, f_s) \text{ divise } f, \text{ alors } f \text{ est un polynôme de } \langle f_1, \ldots, f_s \rangle .$$

Toutefois, on ne peut toujours pas résoudre le problème de l'appartenance à un idéal. Il nous manque en effet la réciproque car le résultat de l'algorithme dépend de l'ordre des polynômes données dans F.

Exemple 2.5. Soit $F = (x^2y - 1, xy^2 + y)$ un couple de polynômes de $\mathbb{K}[x, y]$. On considère l'ordre lexicographique avec $y < x$. On souhaite effectuer la division euclidienne du polynôme $f = x^2y^2 + xy$ de $\mathbb{K}[x, y]$ par F.

$$\begin{array}{l|l} x^2y^2 + xy & x^2y - 1 \\ \cline{2-2} x^2y^2 - \ \ y & y \\ \cline{1-1} \qquad xy - y & \end{array}$$

Le polynôme $xy - y$ n'est pas divisible par $xy^2 + y$. Il s'agit donc du reste de la division de f par F. Par ailleurs, $f = x^2y^2 + xy = x(xy^2 + y)$, donc le reste de la division de f par $F' = (xy^2 + y, x^2y - 1)$ est nul. D'où, f est dans l'idéal $\langle x^2y - 1, xy^2 + y\rangle$.

2.2 Le problème de l'appartenance à un idéal

2.2.1 Idéaux monomiaux

Définition 2.9. Un idéal I de $\mathbb{K}[x_1, \ldots, x_n]$ est dit *monomial* s'il est engendré par une famille de monômes, autrement dit s'il existe une partie A de $\mathbb{N}^n$ telle que

$$I = \langle\, x^\alpha \mid \alpha \in A\rangle\,.$$

Proposition 2.4. *Soit I un idéal monomial de $\mathbb{K}[x_1, \ldots, x_n]$, soit f un polynôme de $\mathbb{K}[x_1, \ldots, x_n]$. Les assertions suivantes sont équivalentes :*

- *(i) le polynôme f appartient à I,*
- *(ii) tout terme du polynôme f est dans I,*
- *(iii) le polynôme f est une combinaison linéaire (à coefficients dans $\mathbb{K}$) de monômes de I.*

Démonstration. On montre $(iii) \Rightarrow (ii) \Rightarrow (i)$ de manière immédiate. Montrons $(i) \Rightarrow (iii)$. Supposons (i) et notons $I = \langle x^\alpha \mid \alpha \in A\rangle$, où A est une partie de $\mathbb{N}^n$. Alors

$$f = h_{\alpha_1} x^{\alpha_1} + \ldots + h_{\alpha_s} x^{\alpha_s}$$

où pour tout i de $\{1, \ldots, s\}$, h_{α_i} est un polynôme de $\mathbb{K}[x_1, \ldots, x_n]$ et α_i appartient à A. Il suffit à présent de décomposer chaque h_{α_i} en combinaison linéaire de monômes en $x_1, \ldots, x_n$ puis de développer l'expression de f. Ainsi f vérifie (iii). □

Proposition 2.5. *Soit $I = \langle x^\alpha \mid \alpha \in A\rangle$ un idéal monomial de $\mathbb{K}[x_1, \ldots, x_n]$, où A est une partie de $\mathbb{N}^n$. Alors, x^β est un monôme de I si, et seulement si, il existe α dans A, tel que x^α divise x^β.*

Théorème 2.2 (Le lemme de Dickson)**.** *Soit $I = \langle x^\alpha | \alpha \in A\rangle$ un idéal monomial de $\mathbb{K}[x_1, \ldots, x_n]$, où A est une partie de $\mathbb{N}^n$. Alors il existe des n-uplets $\alpha_1, \ldots, \alpha_s$ de A tels que $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s}\rangle$.*

Autrement dit, tout idéal monomial possède une base finie. Ce théorème est démontré dans [Cox 1997].

2.2.2 Le théorème de la base de Hilbert

Définition 2.10. Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$,

- on note $LT(I) := \{LT(f) \mid f \in I\}$,
- on note $\langle LT(I)\rangle$ l'*idéal engendré* par les éléments de $LT(I)$.

On remarque que si $I = \langle f_1, \ldots, f_s \rangle$ est un idéal de $\mathbb{K}[x_1, \ldots, x_n]$, alors

$$\langle LT(f_1), \ldots, LT(f_s) \rangle \subset \langle LT(I) \rangle .$$

Démonstration. Soit f un polynôme de l'idéal $\langle LT(f_1), \ldots, LT(f_s) \rangle$. Alors, il existe des polynômes $g_1, \ldots, g_s$ tels que

$$f = \sum_{i=1}^{s} g_i \, LT(f_i).$$

Or les termes $LT(f_1), \ldots, LT(f_s)$ appartiennent à $LT(I)$ donc à $\langle LT(I) \rangle$. D'où le polynôme f est dans $\langle LT(I) \rangle$. □

Cette inclusion est stricte en général

Exemple 2.6. Soient deux polynômes $f = xy-1$ et $g = xy+x$ de $\mathbb{K}[x, y]$. Soient $I = \langle f, g \rangle$ l'idéal de $\mathbb{K}[x, y]$ engendré par f et g. On a bien

$$\langle LT(f), LT(g) \rangle = \langle xy \rangle \subset \langle LT(I) \rangle .$$

A-t-on égalité entre les deux idéaux ? Le polynôme $x + 1 = g - f$ appartient à l'idéal à I. Ainsi, le monôme x est dans $LT(I)$, donc dans $\langle LT(I) \rangle$. Mais le monôme x n'appartient pas à $\langle xy \rangle$. Ainsi l'inclusion est stricte.

Proposition 2.6. *Soit $I = \langle x^\alpha \mid \alpha \in A \rangle$ un idéal monomial de $\mathbb{K}[x_1, \ldots, x_n]$, où A est une partie de $\mathbb{N}^n$, alors*

- *l'idéal $\langle LT(I) \rangle$ est monomial,*
- *il existe des polynômes $g_1, \ldots, g_t$ tels que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.*

Le théorème suivant est fondamental. Il est énoncé et montré dans [Cox 1997].

Théorème 2.3 (Théorème de la base de Hilbert)**.** *Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$. Alors il existe des polynômes $g_1, \ldots, g_t$ de I tels que*

$$I = \langle g_1, \ldots, g_t \rangle$$

.

Autrement dit, tout idéal de $\mathbb{K}[x_1, \ldots, x_n]$ possède un nombre fini de générateurs.

2.2.3 Les bases de Gröbner

Définition 2.11. Étant donné un ordre monomial fixé, un sous-ensemble $G = \{g_1, \ldots, g_t\}$ d'un idéal I de $\mathbb{K}[x_1, \ldots, x_n]$ est appelé *base de Gröbner* de I si

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle .$$

Proposition 2.7. *Étant donné un ordre monomial fixé, tout idéal non nul I de $\mathbb{K}[x_1, \ldots, x_n]$ possède une base de Gröbner. De plus, toute base de Gröbner de I est une base de I.*

Cette proposition est montré dans [ref...].

Proposition 2.8. *Soient I idéal de $\mathbb{K}[x_1, \ldots, x_n]$, $G = \{g_1, \ldots, g_t\}$ une base de Gröbner de I et f un polynôme de $\mathbb{K}[x_1, \ldots, x_n]$. Alors, il existe un unique polynôme r de $\mathbb{K}[x_1, \ldots, x_n]$ vérifiant :*

- *les termes de r ne sont pas divisibles par $LT(g_1), \ldots, LT(g_t)$,*
- *il existe un polynôme g de I tel que $f = g + r$.*

En particulier, r est le reste de la division de f par G, quelque soit l'ordre des éléments de G.

Proposition 2.9. *Soient I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et G une base de Gröbner de I. Un polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$ est un polynôme de I si, et seulement si, le reste de la division de f par G est nul.*

Ainsi, en connaissant une base de Gröbner d'un idéal de $\mathbb{K}[x_1, \ldots, x_n]$, on peut résoudre le problème de l'appartenance à un idéal. Il nous faut à présent trouver un moyen de la calculer pour tout idéal de $\mathbb{K}[x_1, \ldots, x_n]$.

2.2.4 L'algorithme de Buchberger

Définition 2.12. Soient deux polynômes f et g de $\mathbb{K}[x_1, \ldots, x_n]$. On note

$$(\alpha_1, \ldots, \alpha_n) = multideg(f) \text{ et } (\beta_1, \ldots, \beta_n) = multideg(g).$$

On pose $\gamma = (\gamma_1, \ldots, \gamma_n)$ où pour tout i dans $\{1, \ldots, n\}$,

$$\gamma_i = max(\alpha_i, \beta_i).$$

- Le monôme x^γ est appelé le *plus petit commun multiple* de $LM(f)$ et $LM(g)$. Nous le noterons $PPCM(LM(f), LM(g))$.
- On appelle *S-polynôme* de f et g le polynôme

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$$

Exemple 2.7. On considère l'anneau $\mathbb{K}[x, y]$ muni de l'ordre lexicographique, avec $y < x$. Soient $f = x^3y^2 - x^2y^3 + x$ et $g = 3x^4y + y^2$.

$$S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = x^4y^2 - x^3y^3 + x^2 - x^4y^2 - \frac{1}{3}y^3 = -x^3y^3 - \frac{1}{3}y^3 + x^2$$

On notera que

$$S(f, g) = -S(g, f)$$

Proposition 2.10. *Soient $f_1, \ldots, f_s$ des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$ et $c_1, \ldots, c_s$ des scalaires de $\mathbb{K}$. Notons $f = c_1 f_1 + \ldots + c_s f_s$. Supposons que pour tout i dans $\{1, \ldots, s\}$, $multideg(f_i) = \delta \in \mathbb{N}^n$. Si $multideg(f) < \delta$, alors :*

- *le polynôme f est une combinaison linéaire à coefficient dans $\mathbb{K}$ de $S(f_j, f_k)$, où j et k sont dans $\{1, \ldots, s\}$,*
- *de plus, pour tous j et k dans $\{1, \ldots, s\}$, $multideg(S(f_j, f_k)) < \delta$*

Cette proposition est montrée dans [Cox 1997].

Théorème 2.4 (Critère de Buchberger)**.** *Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$. Une base $G = \{g_1, \ldots, g_t\}$ de I est une base de Gröbner si, et seulement si, pour tous i et j de $\{1, \ldots, t\}$, on a*

$$S(g_i, g_j) \xrightarrow{G} 0.$$

Démonstration. Soit $G = \{g_1, \ldots, g_t\}$ une base d'un idéal I de $\mathbb{K}[x_1, \ldots, x_n]$. Si G est une base de Gröbner de I, alors tout S-polynôme $S(g_i, g_j)$ est dans I. D'où $S(g_i, g_j) \xrightarrow{G} 0$.

Montrons la réciproque. Supposons que pour tout couple (i, j), avec $i \neq j$, on ait $S(g_i, g_j) \xrightarrow{G} 0$. Il faut montrer à présent que G est une base de Gröbner de I, i.e.,

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle .$$

Soit f un polynôme de I. Il suffit de montrer que $LT(f)$ est dans l'idéal monomial $\langle LT(g_1), \ldots, LT(g_t) \rangle$. Il existe une décomposition $f = h_1 g_1 + \ldots + h_t g_t$, où les h_i sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. Posons $\delta = max\{multideg(h_1 g_1), \ldots, multideg(h_t g_t)\}$. On a $multideg(f) \leqslant \delta$.

Il existe plusieurs décomposition de f. Pour chaque décomposition, on a un δ de $\mathbb{N}^n$. On considère une décomposition de f telle que δ soit minimal, selon un ordre monomial.

Montrons par l'absurde que $multideg(f) = \delta$. Supposons $multideg(f) < \delta$. En posant $m(i) = multideg(h_i g_i)$, on a une décomposition

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i.$$

Les deux dernières sommes sont de degré strictement inférieur à δ. Comme par hypothèse $multideg(f) < \delta$, alors on a

$$multideg \Big(\sum_{m(i)=\delta} LT(h_i) g_i \Big) < \delta$$

En posant $LT(h_i) = c_i x^{\alpha(i)}$, avec c_i dans $\mathbb{K}$ et $\alpha(i)$ dans $\mathbb{N}^n$, on a

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i.$$

Comme pour tout i tel que $m(i) = \delta$, on a $multideg(LT(h_i)g_i) = \delta$, la somme $\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ satisfait aux hypothèses de la proposition 2.10. Cette somme se décompose alors en combinaison linéaire à coefficients dans $\mathbb{K}$ de S-polynômes $S(x^{\alpha(i)}g_i, x^{\alpha(k)}g_k)$:

$$\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{jk} S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$$

où $c_{jk} \in \mathbb{K}$. Or

$$S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k) = \frac{x^\delta}{x^{\alpha(j)} LT(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(k)} LT(g_k)} x^{\alpha(k)} g_k$$

$$= \frac{x^\delta}{PPCM(LM(g_j), LM(g_k))} S(g_j, g_k).$$

On obtient ainsi une décomposition

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{j,k} c_{jk} \frac{x^\delta}{PPCM(LM(g_j), LM(g_k))} S(g_j, g_k).$$

Or, par hypothèse, pour tous j, k,

$$S(g_i, g_j) \xrightarrow{G} 0.$$

Ainsi, le S-polynôme $S(g_j, g_k)$ peut s'écrire sous la forme

$$S(g_j, g_k) = \sum_{i=1}^{t} k_{ijk} g_i,$$

où les k_{ijk} sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$ qui satisfont pour tous i, j et k à

$$multideg(k_{ijk} g_i) \geq multideg(S(g_j, g_k)).$$

On a alors

$$\frac{x^\delta}{PPCM(LM(g_j), LM(g_k))} S(g_j, g_k) = \sum_{i=1}^{t} l_{ijk} g_i,$$

avec $l_{ijk} = \frac{x^\delta}{PPCM(LM(g_j), LM(g_k))} k_{ijk}$. On a donc

$$multideg(l_{ijk} g_i) \leq multideg\Big(\frac{x^\delta}{PPCM(LM(g_j), LM(g_k))} S(g_j, g_k) \Big) < \delta.$$

D'où,

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{j,k} c_{jk} \Big(\sum_{i=1}^{t} l_{ijk} g_i \Big) = \sum_{i=1}^{t} h'_i \, g_i.$$

Les polynômes h'_i vérifient

$$multideg(h'_i\, g_i) < \delta.$$

Ainsi le multidegré de $\sum_{m(i)=\delta} LT(h_i)g_i$ est strictement inférieur à δ, par suite dans la décomposition, tous les termes ont un multidegré strictement inférieur à δ. Ceci contredit l'hypothèse sur la minimalité de δ, par suite, $multideg(f) = \delta$. Donc, il existe un i dans $\{1, \ldots, t\}$, tel que $multideg(f) = multideg(h_i g_i)$. D'où, $LT(f)$ est divisible par $LT(g_i)$. Donc, $LT(f)$ appartient à l'idéal $\langle LT(g_1), \ldots, LT(g_t)\rangle$. □

Grâce à ce théorème, le mathématicien Buchberger a pu définir un algorithme qui complète une base de Gröbner avec de nouveaux générateurs, de manière à ce que chaque S-polynôme se réduise en 0, et sans modifier l'idéal engendré par la base. Il s'agit donc d'une boucle qui pour chaque S-polynôme, ajoute un générateur si nécessaire. Cet algorithme est publié dans [Buchberger 1965].

Algorithme de Buchberger

Entrées : $F = \{f_1, \ldots, f_s, \}$ base d'un idéal $I \subset \mathbb{K}[x_1, \ldots, x_n]$
Sorties : G base de Gröbner de I telle que $F \subset G$
$G := F$;
répéter
  $G' := G$;
  pour chaque *paire* $\{p, q\} \subset G$ **faire**
    $S(p, q) \xrightarrow{G'} S$;
    si $S \neq 0$ **alors** $G := G \cup \{S\}$
  fin
jusqu'à $G = G'$;

Cet algorithme termine toujours avec succès. Il permet donc de résoudre le problème de l'appartenance à un idéal.

3 Les systèmes de réécriture

3.1 Réductions et règles de réécriture

3.1.1 Présentations de monoïdes

Définition 3.1. Soit Σ un ensemble. Le *monoïde libre* Σ^* engendré par l'ensemble Σ est l'ensemble des mots formés avec les éléments de Σ, muni de la concaténation $u, v \mapsto uv$. L'ensemble Σ est alors appelé *alphabet*. Le monoïde libre $\Sigma^* = \{\alpha_1\alpha_2 \ldots \alpha_n \mid \alpha_1, \ldots, \alpha_n \in \Sigma\}$ a pour unité le mot vide, que nous noterons 1.

Soit $\mathcal{R} \subset \Sigma^* \times \Sigma^*$ une relation binaire sur Σ^*. La *congruence* $\longleftrightarrow^*_{\mathcal{R}}$ engendrée par $\mathcal{R}$ est définie par :

- $uxv \longleftrightarrow_{\mathcal{R}} uyv$, si u et v sont dans Σ^* et $\big((x,y) \in \mathcal{R}$ ou $(y,x) \in \mathcal{R}\big)$,
- $x \longleftrightarrow^*_{\mathcal{R}} y$, si $x \longleftrightarrow_{\mathcal{R}} \ldots \longleftrightarrow_{\mathcal{R}} y$.

Une *présentation* (par générateurs et relations) d'un monoïde M est la donnée d'un alphabet Σ et d'une relation binaire $\mathcal{R}$ sur Σ^* tels que M soit isomorphe au quotient de Σ^* par la congruence $\longleftrightarrow^*_{\mathcal{R}}$:

$$M \cong {\Sigma^*}/{\longleftrightarrow^*_{\mathcal{R}}}$$

Exemple 3.1. On cherche une présentation par générateurs et relations du monoïde $\mathbb{N}^2$. Ce monoïde est le monoïde abélien libre à deux générateurs.

Prenons $\Sigma = \{a, b\}$ et $\mathcal{R} = \{(ba, ab)\}$, alors $\mathbb{N}^2 \cong {\Sigma^*}/{\longleftrightarrow^*_{\mathcal{R}}}$. En effet,

$$ {\Sigma^*}/{\longleftrightarrow^*_{\mathcal{R}}} = \{a^n b^m | (n,m) \in \mathbb{N}^2\},$$

car si w est un mot de Σ^*, alors il existe deux entiers n et m de $\mathbb{N}$ tels que $w \longleftrightarrow^*_{\mathcal{R}} a^n b^m$. Les entiers n et m sont en fait respectivement le nombre d'occurences de a et de b dans le mot w.

De plus, l'application $\rho : \mathbb{N}^2 \longrightarrow {\Sigma^*}/{\longleftrightarrow^*_{\mathcal{R}}},\ (n,m) \longmapsto a^n b^m$ est un isomorphisme de monoïde.

Exemple 3.2. Soient un alphabet $\Sigma = \{a\}$ et une relation $\mathcal{R} = \{(aa, a)\}$. Alors

$$ {\Sigma^*}/{\longleftrightarrow^*_{\mathcal{R}}} = \{1, a\}.$$

On a donc une présentation d'un monoïde à deux éléments.

3.1.2 Les systèmes de réécriture

Définition 3.2. La donnée $(\Sigma, \mathcal{R})$, où Σ est un ensemble et $\mathcal{R}$ est un sous-ensemble de $\Sigma^* \times \Sigma^*$ est appelé un *système de réécriture*.

- Si $\rho = (x, y) \in \mathcal{R}$, on dit que $x \xrightarrow{\rho} y$ est une *règle de réécriture*, avec x pour *source* et y pour *cible*.
- Une *réduction élémentaire* est une réécriture de la forme $uxv \xrightarrow{u\rho v} uyv$, où u et v sont des mots de Σ^* et $x \xrightarrow{\rho} y$ est une règle. On note alors

$$uxv \longrightarrow_{\mathcal{R}} uyv.$$

- Une *réduction* $x \xrightarrow{r} y$ est une suite finie $x = x_0 \xrightarrow{r_1} x_1 \xrightarrow{r_2} \ldots \xrightarrow{r_n} x_n = y$ de réductions élémentaires r_i. On note alors

$$x \longrightarrow^*_{\mathcal{R}} y.$$

On a ainsi défini deux relations sur Σ^* engendrées par $\mathcal{R}$: une relation de réduction élémentaire $\longrightarrow_{\mathcal{R}}$ et une relation de réduction composée $\longrightarrow_{\mathcal{R}}^*$ qui est la *clôture réflexive et transitive* de $\longrightarrow_{\mathcal{R}}$.

Si $x \xrightarrow{r} y$ et $y \xrightarrow{s} z$ sont des réductions, on note $x \xrightarrow{r*s} z$ la réduction composée $x \xrightarrow{r} y \xrightarrow{s} z$.

Il existe aussi une réduction vide $x \xrightarrow{x} x$, pour tout mot x.

De plus, pour toute réduction $x \xrightarrow{r} y$, pour tout mot u, on peut définir deux réductions $ux \xrightarrow{ur} uy$ et $xu \xrightarrow{ru} yu$.

Exemple 3.3. Soient l'alphabet $\Sigma = \{a, b, c\}$ et la règle $ab \xrightarrow{\rho} ca$. On a alors par exemple $aabbc \xrightarrow{a\rho bc} acabc \xrightarrow{ac\rho c} accac$. D'où $acabc \longrightarrow_{\mathcal{R}}^* accac$.

Un système de réécriture est un ensemble de règles.

Définition 3.3. Soit $(\Sigma, \mathcal{R})$ un système de réécriture. On dit qu'un mot x de Σ^* est *réductible* s'il existe un mot y de Σ^* tel que $x \longrightarrow_{\mathcal{R}} y$. Dans le cas contraire, on dit que x est *irréductible*, *réduit* ou *en forme normale*. Si $x \longrightarrow_{\mathcal{R}} y$ et y est irréductible, alors on dit que y est une forme normale de x.

3.2 Les propriétés de terminaison et de confluence

3.2.1 Les systèmes de réécriture noethériens

Définition 3.4. On dit qu'un système de réécriture $(\Sigma, \mathcal{R})$ est *noethérien* si on a la propriété de *terminaison* : il n'existe aucune réduction infinie

$$u_0 \to_{\mathcal{R}} u_1 \to_{\mathcal{R}} \ldots \to_{\mathcal{R}} u_n \to_{\mathcal{R}} \ldots$$

Dans les exemples suivants, on prend pour alphabet $\Sigma = \{a, b\}$.

Exemple 3.4. Le système formé de l'unique règle $a \to ab$ n'est pas noetherien, car il existe une chaîne infinie $a \to ab \to abb \to \ldots$

Exemple 3.5. Le système formé des deux règles $a \to b$ et $b \to a$ n'est pas noetherien, car il existe une chaîne infinie $a \to b \to a \to b \to \ldots$

Exemple 3.6. Le système formé de l'unique règle $ab \to a$ est noetherien, car la longueur d'un mot diminue à chaque étape de réécriture.

Exemple 3.7. Le système formé de l'unique règle $ab \to caa$ est noetherien, car le nombre d'occurences de b diminue à chaque étape.

Définition 3.5. Soit $(\Sigma, \mathcal{R})$ un système de réécriture. On dit qu'une propriété P est *$\mathcal{R}$-héréditaire* si :

$$\forall x \in \Sigma^* \left(\forall y \in \Sigma^*, x \longrightarrow_{\mathcal{R}} y \Longrightarrow P(y)\right) \Longrightarrow P(x).$$

En particulier, une telle propriété s'applique à tous les mots réduits.

Proposition 3.1. *Soit $(\Sigma, \mathcal{R})$ un système de réécriture. Les assertions suivantes sont équivalentes :*

- *(i) Terminaison : il n'existe pas de réduction infinie*

$$u_0 \to_{\mathcal{R}} u_1 \to_{\mathcal{R}} \ldots \to_{\mathcal{R}} u_n \to_{\mathcal{R}} \ldots,$$

- *(ii) Ordre de terminaison : il existe un bon ordre $>$ (appelé ordre de terminaison) compatible avec le produit sur Σ^*, tel que pour tous mots x et y de Σ^*,*

$$x \longrightarrow_{\mathcal{R}} y \text{ implique } x > y,$$

- *(iii) Principe de récurence noethérienne : toute propriété $\mathcal{R}$-héréditaire s'applique à tout mot de Σ^*.*

On trouve la preuve de ce théorème dans []

Ainsi, la propriété de terminaison se démontre de manière générale en construisant un ordre de terminaison. En effet, dans l'exemple 3.6, on a implicitement construit un ordre de terminaison de la manière suivante : $x > y$ si le mot x est plus long que le mot y. Dans l'exemple 3.7 on peut définir un ordre de terminaison de la manière suivante : $x > y$ si le nombre d'occurences de b dans le mot x est strictement supérieur au nombre d'occurences de b dans le mot y.

Le principe de récurrence noethérienne sera nécessaire dans la partie suivante.

3.2.2 Systèmes de réécriture convergents

Définition 3.6. On dit qu'un système de réécriture $(\Sigma, \mathcal{R})$ est *confluent*, si pour tous mots x, y et z de Σ^*, lorsqu'on suppose

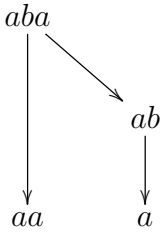
$$x \to_{\mathcal{R}}^* y \text{ et } x \to_{\mathcal{R}}^* z,$$

alors, il existe un mot t de Σ^* tel que

$$y \to_{\mathcal{R}}^* t \text{ et } z \to_{\mathcal{R}}^* t.$$

Dans les exemples suivants, on prend pour alphabet $\Sigma = \{a, b\}$.

Exemple 3.8. Le système formé des deux règles $ab \to a$ et $ba \to b$ n'est pas confluent, car on a :



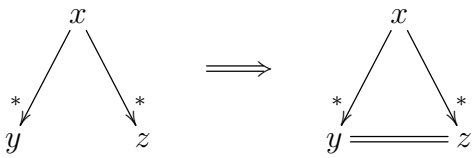
or aa et a sont en forme normale.

Exemple 3.9. Le système formé des deux règles $ab \to 1$ et $ba \to 1$ est confluent. Pour le démontrer, nous allons utiliser la proposition suivante.

Proposition 3.2. *Soit $(\Sigma, \mathcal{R})$ un système de réécriture noethérien, alors les propositions suivantes sont équivalentes :*

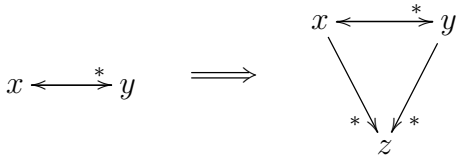
- *(i) Unicité de la forme réduite :*

$$(x \longrightarrow_{\mathcal{R}}^{*} y \text{ et } x \longrightarrow_{\mathcal{R}}^{*} z, \text{ tels que } y \text{ et } z \text{ sont réduits }) \Longrightarrow (y = z)$$



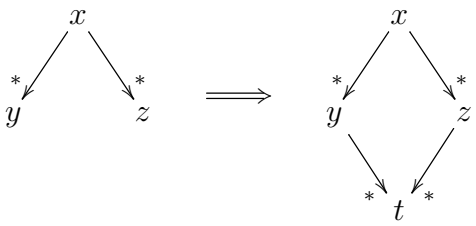
- *(ii) Propriété de Church-Rosser :*

$$(x \longleftrightarrow_{\mathcal{R}}^{*} y) \Longrightarrow (\text{il existe un mot } z \text{ de } \Sigma^{*} \text{ tel que } x \longrightarrow_{\mathcal{R}}^{*} z \text{ et } y \longrightarrow_{\mathcal{R}}^{*} z)$$



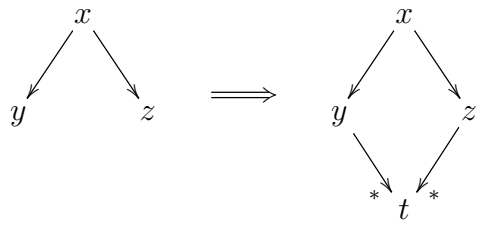
- *(iii) Confluence :*

$$(x \longrightarrow_{\mathcal{R}}^{*} y \text{ et } x \longrightarrow_{\mathcal{R}}^{*} z) \Longrightarrow (\text{il existe un mot } t \text{ de } \Sigma^{*} \text{ tel que } y \longrightarrow_{\mathcal{R}}^{*} t \text{ et } z \longrightarrow_{\mathcal{R}}^{*} t)$$



– *(iv) Confluence locale :*

$$(x \longrightarrow_{\mathcal{R}} y \text{ et } x \longrightarrow_{\mathcal{R}} z) \Longrightarrow (\text{il existe un mot } t \text{ de } \Sigma^* \text{ tel que } y \longrightarrow_{\mathcal{R}}^* t \text{ et } z \longrightarrow_{\mathcal{R}}^* t)$$



En particulier, l'implication $(iv) \Rightarrow (iii)$ dans le cas noetherien est connue sous le nom de *lemme de Newman* ou *lemme du diamant*.

Théorème 3.1 (Lemme de Newman)**.** *Si un système de réécriture est noethérien et localement confluent, alors il est confluent.*

Démonstration. Soit un système de réécriture noethérien $(\Sigma, \mathcal{R})$.

Pour tout mot x de Σ^*, notons $C(x)$ la propriété de confluence en x et $Cl(x)$ la propriété de confluence locale en x :

$C(x)$: $\ll$ Pour tous mots y et z de Σ^*,

$(x \longrightarrow_{\mathcal{R}}^* y \text{ et } x \longrightarrow_{\mathcal{R}}^* z) \Longrightarrow (\text{il existe un mot } t \text{ de } \Sigma^* \text{ tel que } y \longrightarrow_{\mathcal{R}}^* t \text{ et } z \longrightarrow_{\mathcal{R}}^* t)$ $\gg$

$Cl(x)$: $\ll$ Pour tous mots y et z de Σ^*,

$(x \longrightarrow_{\mathcal{R}} y \text{ et } x \longrightarrow_{\mathcal{R}} z) \Longrightarrow (\text{il existe un mot } t \text{ de } \Sigma^* \text{ tel que } y \longrightarrow_{\mathcal{R}}^* t \text{ et } z \longrightarrow_{\mathcal{R}}^* t)$ $\gg$

Supposons que l'on ait $Cl(x)$, pour tout mot x de Σ^*. Puisque le système de réécriture est noethérien, il suffit, grâce au principe de récurrence noethérienne, de montrer que la propriété C est $\mathcal{R}$-héréditaire.

Soit x un mot de Σ^*, supposons, pour tout mot y de Σ^*, l'implication

$$x \longrightarrow_{\mathcal{R}} y \Longrightarrow C(y).$$

Soient y et z deux mots de Σ^*, chacun distinct de x, tels que

$$x \longrightarrow_{\mathcal{R}}^* y \text{ et } x \longrightarrow_{\mathcal{R}}^* z.$$

Il existe des mots y_0 et z_0 de Σ^* tels que

$$x \longrightarrow_{\mathcal{R}} y_0 \longrightarrow_{\mathcal{R}}^* y \text{ et } x \longrightarrow_{\mathcal{R}} z_0 \longrightarrow_{\mathcal{R}} z.$$

Or, on a $Cl(x)$, donc il existe un mot t_0 de Σ^* tel que

$$y_0 \longrightarrow_{\mathcal{R}}^* t_0 \text{ et } z_0 \longrightarrow_{\mathcal{R}}^* t_0.$$

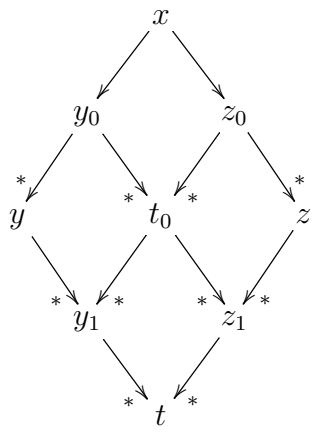
Par hypothèse, on a $C(y_0)$ et $C(z_0)$. Ainsi il existe des mots y_1 et z_1 de Σ^* tels que

$$y \longrightarrow_{\mathcal{R}}^* y_1,\ t_0 \longrightarrow_{\mathcal{R}}^* y_1,\ t_0 \longrightarrow_{\mathcal{R}}^* z_1 \text{ et } z \longrightarrow_{\mathcal{R}}^* z_1.$$

De la même manière, puisque $x \longrightarrow_{\mathcal{R}}^* t_0$, on a $C(t_0)$, d'où il existe un mot t de Σ^* tel que

$$y_1 \longrightarrow_{\mathcal{R}}^* t \text{ et } z_1 \longrightarrow_{\mathcal{R}}^* t.$$

On remarque alors que $y \longrightarrow_{\mathcal{R}}^* t$ et $z \longrightarrow_{\mathcal{R}}^* t$, d'où la propriété $C(x)$. Ainsi, la propriété de confluence est $\mathcal{R}$-héréditaire si on suppose la confluence locale pour tout mot. Et comme la présentation est noethérienne, on a $C(x)$, pour tout mot x de Σ^*, d'après le principe de récurrence noethérienne.



□

Si $(\Sigma, \mathcal{R})$ est un système de réécriture convergent, on note $\hat{x}$ la forme normale de x, qui est l'unique mot irréductible tel que $x \longrightarrow_{\mathcal{R}}^* \hat{x}$.

Par la propriété de Church-Rosser et par l'unicité de la forme normale, on a

$$(x \longleftrightarrow_{\mathcal{R}}^* y) \Longleftrightarrow (\hat{x} = \hat{y})$$

Proposition 3.3. *Si un système de réécriture $(\Sigma, \mathcal{R})$ est fini et convergent, alors la congruence $\longleftrightarrow_{\mathcal{R}}^*$ est une relation décidable.*

Démonstration. En effet, dans le cas d'un système de réécriture convergent, pour trouver la forme réduite d'un mot, il suffit de lui appliquer des réductions jusqu'à arriver à une forme normale.

Puisque la présentation est noethérienne, le nombre de réduction que l'on peut appliquer à un mot est toujours finie, et puisque la présentation est confluente, cette forme normale est unique. De plus, l'hypothèse finie permet de dire qu'un mot est en forme normale. Ainsi, la relation $x \longleftrightarrow_{\mathcal{R}}^* y$ est équivalente à l'égalité des formes normales de x et de y. □

Si $\longleftrightarrow^*_{\mathcal{R}}$ est une relation décidable et si $(\Sigma, \mathcal{R})$ est une présentation du monoïde M, on dit que M a un problème du mot décidable.

La méthode vue dans la preuve pour décider du problème du mot est appelée *algorithme de la forme normale*.

3.3 Le problème du mot

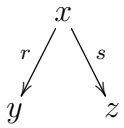
Un problème de décision est une question mathématiquement définie demandant une réponse par oui ou non. Un problème de décision est dit décidable, s'il existe un algorithme qui termine en un nombre fini d'étapes et qui le décide, c'est-à-dire qui réponde par oui ou par non à la question posée. S'il n'existe pas de tels algorithmes, le problème est dit indécidable.

En particulier, le problème du mot est un problème de décision. La question posée par le problème du mot dans une présentation $(\Sigma, \mathcal{R})$ d'un monoïde M est : étant donnés deux mots u et v de Σ^*, a-t-on $u = v$ dans le monoïde M ?

Dans le cas général, le problème est indécidable. Toutefois nous savons à présent qu'il est décidable dans le cas d'une présentation convergente finie. Comment savoir si un système de réécriture fini noethérien est convergent ? La notion de paire critique nous permettra de répondre à cette question.

3.3.1 Paires critiques

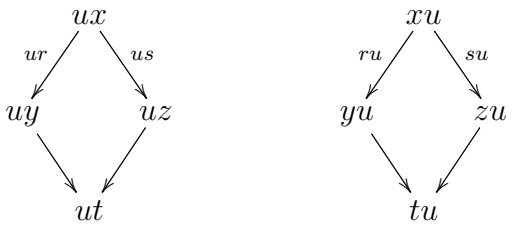
Une *paire* de source x est une paire $p = (r, s)$ de réductions élémentaires dont x est la source commune.



On dit qu'une telle paire est *confluente*, s'il existe un mot t de Σ^* tel que

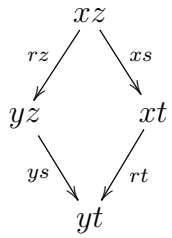
$$y \longrightarrow^*_{\mathcal{R}} t \text{ et } z \longrightarrow^*_{\mathcal{R}} t.$$

– Si u est un mot est $p = (r, s)$ une paire confluente, alors les paires $up = (ur, us)$ et $pu = (ru, su)$ le sont aussi.



– Si $x \xrightarrow{r} y$ est une réduction élémentaire, alors $p = (r, r)$ est une paire confluente.

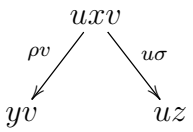
– Si $x \xrightarrow{r} y$ et $z \xrightarrow{s} t$ sont des réductions élémentaires, alors $p = (rz, xs)$ est confluente :



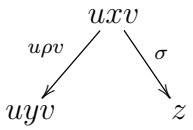
On dit alors que les réductions rz et xs sont disjointes.

Définition 3.7. Une paire est *critique* si elle n'est pas de la forme up ou pu (où p est une paire et u est un mot non vide) et ses réductions ne sont ni égales ni disjointes.

Donc une paire critique est nécessairement d'une de ces deux formes :
– Un *chevauchement* $(\rho v, u\sigma)$ où $ux \xrightarrow{\rho} y$ et $xv \xrightarrow{\sigma} z$ sont des règles et $u, x, v \neq 1$.



– Une *inclusion* $(u\rho v, \sigma)$ où $x \xrightarrow{\rho} y$ et $uxv \xrightarrow{\sigma} z$ sont des règles et $ux, xv \neq 1$



Proposition 3.4. *Si toutes les paires critiques d'un système de réécriture sont confluentes, alors toutes les paires le sont.*

Démonstration. Soit $(\Sigma, \mathcal{R})$ un système de réécriture dont toutes les paires critiques sont confluentes. Soit $p = (r, s)$ une paire.

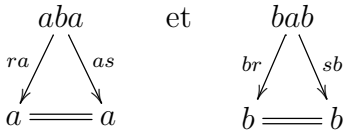
D'après la définition 3.7, la paire p entre forcément dans un des cas de figure suivants :
– Si la paire p est critique, alors, par hypothèse, elle est confluente.
– Si les réductions r et s sont égales, on a vu que la paire $p = (r, r)$ est confluente.
– Si les réductions r et s sont disjointes, on a vu que la paire $p = (r, s)$ est confluente.
– Si p est de la forme up' ou $p'u$, où p' est une paire et u un mot différent de 1, on peut supposer que la paire p' n'est pas de la forme vp'' ou $p''v$, où p'' est une paire et v un mot non vide. Donc la paire p' entre forcément dans un des cas de figure vu précédemment. Ainsi, la paire p' est confluente. Alors, on a vu que les paires up' et $p'u$ sont confluentes aussi. Donc, la paire p est confluente.

Ainsi, la paire p est confluente. Donc, toutes les paires du système de réécriture $(\Sigma, \mathcal{R})$ sont confluentes. □

Corollaire 3.1. *Si un système de réécriture est noethérien et si toutes ses paires critiques sont confluentes, alors elle est convergente.*

Démonstration. En effet, si toutes les paires critiques d'un système de réécriture noethérien sont confluentes, alors, d'après la proposition 3.4, toutes les paires le sont. Ainsi, le système est confluent, donc, convergent. □

Revenons à l'exemple 3.9. On a les deux règles $ab \xrightarrow{r} 1$ et $ba \xrightarrow{s} 1$. On a donc deux paires critiques :



Ces paires critiques sont localement confluentes. Comme le système est noethérien, elles sont confluentes, donc le système de réécriture est confluent.

3.3.2 L'algorithme de Knuth-Bendix

Proposition 3.5. *La convergence est une propriété décidable pour tout système de réécriture noethérien fini.*

Démonstration. En effet, d'après le corollaire 3.1, il suffit de vérifier la confluence de toutes les paires critiques, qui sont forcément en nombre fini dans ce cas. □

L'algorithme de Knuth-Bendix consiste à transformer un système de réécriture noethérien en un système de réécriture convergent. Il s'agit d'une procédure de complétion, qui pour chaque paire critique, regarde si elle conflue, et dans le cas où elle ne conflue pas, rajoute une règle permettant la confluence.

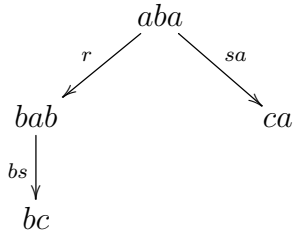
Cet algorithme est publié dans [Knuth-Bendix 1970].

Si $\mathcal{R}$ est un ensemble de règles, on notera $PC(\mathcal{R})$ l'ensemble des paires critiques formées à partir des règles de $\mathcal{R}$.

ALGORITHME DE KNUTH-BENDIX

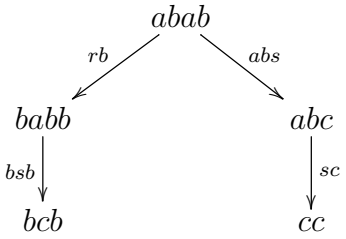
Entrées : Une présentation noethérienne $(\Sigma, \mathcal{R})$ d'un monoïde M et un ordre de terminaison $<$.
Sorties : Une présentation convergente $(\Sigma, \mathcal{R}')$ du même monoïde M, si la procédure termine avec succès, « *Échec* » si la procédure échoue.
Initialisation :
si *il existe un couple* $(u, v) \in \mathcal{R}$ *tel que* $u \neq v$, $u \not< v$ *et* $v \not< u$ **alors** terminer et retourner « *Échec* »,
sinon $i := 0$ et $\mathcal{R}_0 := \{u \to v \mid (u, v) \in \mathcal{R} \text{ et } v < u\}$;
répéter
  $\mathcal{R}_{i+1} := \mathcal{R}_i$;
  pour chaque *paire* $\{x \to y, x \to z\} \in PC(\mathcal{R})$ **faire**
    – Réduire y et z à des formes normales $\hat{y}$ et $\hat{z}$;
    – **si** $\hat{y} \neq \hat{z}$, $\hat{y} \not< \hat{z}$ *et* $\hat{z} \not< \hat{y}$ **alors** terminer et retourner « *Échec* »;
    – **si** $\hat{z} < \hat{y}$ **alors** $\mathcal{R}_{i+1} := \mathcal{R}_{i+1} \cup \{\hat{y} \to \hat{z}\}$;
    – **si** $\hat{y} < \hat{z}$ **alors** $\mathcal{R}_{i+1} := \mathcal{R}_{i+1} \cup \{\hat{z} \to \hat{y}\}$;
    $i := i + 1$;
  fin
jusqu'à $\mathcal{R}_i = \mathcal{R}_{i-1}$;
Retourner $\mathcal{R}_i$;

Exemple 3.10. Soit un monoïde M avec pour présentation l'alphabet $\Sigma = \{a, b, c\}$ et les règles $aba \xrightarrow{r} bab$ et $ab \xrightarrow{s} c$. Cette présentation est noethérienne mais elle n'est pas confluente. Nous allons tenter grâce à l'algorithme de Knuth-Bendix de trouver une présentation convergente pour M. Nous avons une première paire critique :

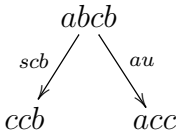


On rajoute donc la règle $ca \xrightarrow{t} bc$ au système de réécriture. Nous avons une autre paire

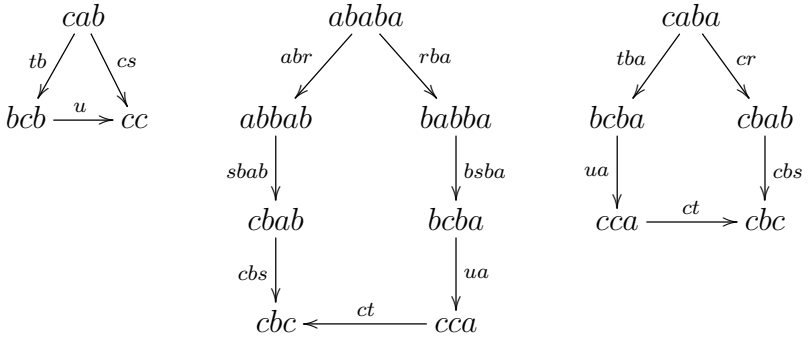
critique :

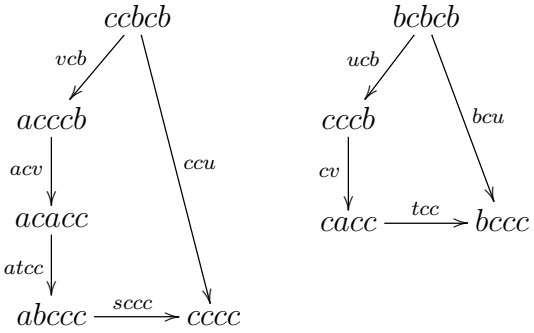


On rajoute alors la règle $bcb \xrightarrow{u} cc$. Cette nouvelle règle forme une nouvelle paire critique non confluente :



Il faut rajouter la règle $ccb \xrightarrow{v} acc$. Vérifions à présent si les paires critiques restantes sont confluents :





On obtient une nouvelle présentation, convergente, du même monoïde. On peut donc résoudre le problème du mot dans ce monoïde.

4 Lien entre réécriture et bases de Gröbner

4.1 Étude des idéaux de polynômes en terme de réécriture

Le but de cette partie est d'aborder une étude des polynômes à plusieurs indéterminées sous un autre angle, celui de la réécriture. Cette nouvelle approche permettra de créer des liens entre ces deux domaines de l'algèbre et d'avoir une nouvelle approche des bases de Gröbner et notamment de leur construction algorithmique.

4.1.1 Système de réécriture dans $\mathbb{K}[x_1, \ldots, x_n]$

Soit un ordre monomial fixé et soit f un polynôme de $\mathbb{K}[x_1, \ldots, x_n]$. On associe à f la règle de réécriture

$$LT(f) \xrightarrow{f} LT(f) - f.$$

Pourquoi ce choix ? Il permet en fait de procéder à la division euclidienne d'un polynôme f par une famille de polynômes $(f_1, \ldots, f_n)$ de $\mathbb{K}[x_1, \ldots, x_n]$. En effet si on réduit f grâce à une réduction élémentaire, après avoir défini les règles $f_1, \ldots, f_n$, cela revient à exécuter une étape de division de l'algorithme de division vu dans le premier chapitre.

Exemple 4.1. On se place dans $\mathbb{K}[x, y]$ et on considère l'ordre lexicographique. Soient trois polynômes $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ et $f_2 = y^2 - 1$ de $\mathbb{K}[x, y]$. On cherche à calculer le reste de la division de f par (f_1, f_2).

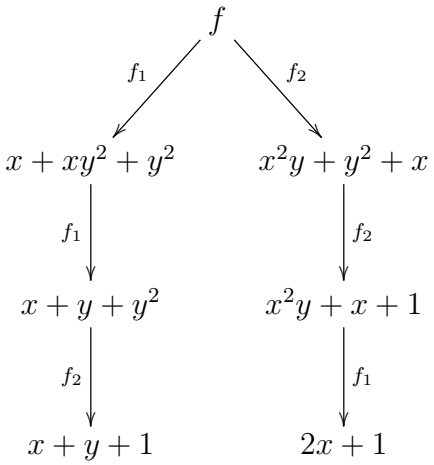
On dispose des deux règles $xy \xrightarrow{f_1} 1$ et $y^2 \xrightarrow{f_1} 1$. On remarque que le terme $LT(f_1) = xy$ divise $LT(f) = x^2y$, donc on peut appliquer la réduction générée par f_1 à $LT(f)$:

$$x^2y \xrightarrow{xf_1} x.$$

On peut même l'appliquer directement à f :

$$f \xrightarrow{xf_1+xy^2+y^2} x + xy^2 + y^2.$$

Pour simplifier les notations, on écrit $f \xrightarrow{f_1} x + xy^2 + y^2$. Puis on continue jusqu'à obtenir un polynôme « en forme normale », c'est-à-dire sur lequel on ne peut appliquer ni la règle $\xrightarrow{f_1}$ ni la règle $\xrightarrow{f_2}$. Cela signifie qu'aucun des termes de ce polynômes n'est divisible par f_1, f_2, ce qui est bien la définition d'un reste. Voici les deux résultats obtenus selon l'ordre des polynômes f_1 et f_2 dans la division :



Pour trois polynômes $f, g, h \in \mathbb{K}[x_1, \ldots, x_n]$, on dit que g se réduit en h, par la réduction élémentaire f, si $LM(f)$ divise un terme non nul X de f et que $h = f - \frac{X}{LT(g)}g$. On note alors

$$g \xrightarrow{f} h.$$

Exemple 4.2. Dans $\mathbb{K}[x, y, z]$, avec l'ordre lexicographique, soient $f = x^3y^2z^3 - x^2z + 2y^3$ et $g = x^4z^4 - 3x^3y^4z^5 + x$ deux polynômes. On obtient la règle

$$x^3y^2z^3 \xrightarrow{f} x^2z - 2y^3.$$

Puis, comme le terme $x^3y^2z^3$ divise le terme $x^3y^4z^5$, on a la réduction

$$g \xrightarrow{f} x^4z^4 - 3y^2z^2(x^2z - 2y^3) + x = x^4z^4 - 3x^2y^2z^3 + 6y^5z^2 + x$$

.

Ainsi, à chaque idéal $I = \langle f_1, \ldots, f_t \rangle$ de $\mathbb{K}[x_1, \ldots, x_n]$, on peut associer un système de réécriture fini $(\Sigma, \mathcal{R})$ où

$$\Sigma = \{x_1, \ldots, x_n\} \text{ et } \mathcal{R} = \{(LT(f_1), LT(f_1) - f_1), \ldots, (LT(f_t), LT(f_t) - f_t)\}.$$

Toutefois, on ne travaille pas sur l'ensemble des mots commutatifs $\Sigma^* = \mathcal{M}(x_1, \ldots, x_n)$ mais sur l'ensemble des polynômes $\mathbb{K}[x_1, \ldots, x_n]$, qui est muni en plus d'une structure additive.

4.1.2 Équivalence entre les bases de Gröbner et les relations de réductions

Théorème 4.1. *Une base $G = \{g_1, \ldots, g_t\}$ d'un idéal I est une base de Gröbner de I si, et seulement si, la relation de réduction $\xrightarrow{G}$ est confluente.*

Démonstration. Soient f et g deux polynômes distincts de G. On note

$$x^\gamma = PPCM(LM(f), LM(g)).$$

Alors, il existe deux monômes u et v de $\mathcal{M}(x_1, \ldots, x_n)$, tels que

$$x^\gamma = uLT(f) = LT(g)v.$$

Si $x^\gamma \neq LT(f)LT(g)$, alors (f, g) est une paire critique dont x^γ est la source, et on a

$$\begin{array}{ccc} & \overset{f}{\swarrow} \; x^\gamma \; \overset{g}{\searrow} & \\ u(LT(f) - f) & & (LT(g) - g)v \\ \| & & \| \\ \frac{x^\gamma}{LT(f)}(LT(f) - f) & & (LT(g) - g)\frac{x^\gamma}{LT(g)} \\ \| & & \| \\ x^\gamma - \frac{x^\gamma}{LT(f)}f & & x^\gamma - \frac{x^\gamma}{LT(g)}g \end{array}$$

La paire est confluente si, et seulement si, on a

$$x^\gamma - \frac{x^\gamma}{LT(g)}g \xrightarrow{G} x^\gamma - \frac{x^\gamma}{LT(f)}$$

$$\text{i.e., } \frac{x^\gamma}{LT(f)}f - \frac{x^\gamma}{LT(g)}g \xrightarrow{G} 0$$

$$\text{i.e., } S(f, g) \xrightarrow{G} 0$$

Or $\xrightarrow{G}$ est confluente si, et seulement si, toutes les paires critiques confluents. On a démontré que c'est vrai si, et seulement si, pour tous polynômes distincts f et g de G, $S(f, g) \xrightarrow{G} 0$, ce qui, d'après le critère de Buchberger, signifie que la base G est une base de Gröbner. □

Cette preuve met en évidence que les paires critiques d'une famille de règles engendrées par des polynômes, correspondent aux plus petits « chevauchements » des paires de monômes de plus haut degré non disjoints, qui sont en fait ce qu'on appelle les plus petits communs multiples. On a donc un lien évident entre la notion de paires critiques et de PPCM. C'est pourquoi les S-polynômes, qui correspondent à la différence entre deux réductions d'une paire critique, se réduisent en 0 si, et seulement si, la paire est confluente.

Ce théorème fondamental est le plus important de ce mémoire, car il est la justification de ce travail de rapprochement des deux domaines. Il synthétise beaucoup de connections possibles entre l'anneau des polynômes et les systèmes de réécriture.

Ainsi l'algorithme de Knuth-Bendix, appliqué à une base d'un idéal de $\mathbb{K}[x_1, \ldots, x_n]$, est similaire à l'algorithme de Buchberger, dans le sens où il procède aux mêmes calculs, aux mêmes complétions.

4.2 Le problème de l'égalité de deux idéaux

Lorsque l'on construit une base de Gröbner ou une présentation convergente, on remarque qu'elle n'est pas unique et qu'elle peut contenir des générateurs ou des règles inutiles. Existe-t-il des bases de Gröbner plus « intéressantes » que d'autres pour un idéal donné ? Quelles sont leurs équivalents en terme de systèmes de réécriture ? On verra que la réponse à ces questions résout le problème de l'égalité de deux idéaux qui est de savoir si deux bases données génèrent le même idéal.

4.2.1 Bases de Gröbner réduites

Définition 4.1. Une *base de Gröbner minimale* d'un idéal I est une base de Gröbner G de I, telle que, pour tout polynôme p de G,
- $LC(p) = 1$,
- $LT(p)$ n'appartient pas à $\langle LT(G - \{p\})\rangle$.

Lemme 4.1. *Soit G une base de Gröbner d'un idéal I. Soit p un polynôme de G tel que $LT(p)$ est dans $\langle LT(G - \{p\})\rangle$. Alors $G - \{p\}$ est aussi une base de Gröbner de I.*

Démonstration. Si $LT(p) \in \langle LT(G - \{p\})\rangle$, alors

$$\langle LT(G - \{p\})\rangle = \langle LT(G)\rangle = \langle LT(I)\rangle .$$

Donc $G - \{p\}$ est aussi une base de Gröbner de I. □

On peut donc construire une base de Gröbner minimale d'un idéal donné I à partir d'une base de Gröbner de I en éliminant tous les générateurs « inutiles », puis en multipliant chaque générateur restant de manière à ce que son coefficient dominant soit égal à 1.

Exemple 4.3. Soient cinq polynômes de $\mathbb{K}[x, y]$

$$f_1 = x^3 - 2xy,$$
$$f_2 = x^2y - 2y^2 + x,$$
$$f_3 = -x^2,$$
$$f_4 = -2xy$$
$$f_5 = -2y^2 + x.$$

Si on considère l'ordre lexicographique par degré, on montre que les polynômes forment une base de Gröbner de l'idéal $I = \langle f_1, f_2, f_3, f_4, f_5\rangle$ qu'ils engendrent.

On remarque que $LT(f_1) = x^3 = -xLT(f_3)$ et $LT(f_2) = x^2y = -(1/2)xLT(f_4)$. Donc d'après le lemme 4.1, on peut éliminer f_1 et f_2. Ce sont les seuls générateurs dont le terme dominant est divisible par le terme dominant d'un autre générateur. À présent, on multiplie par un scalaire les polynômes restants afin que leurs coefficients dominants valent 1. Ainsi on obtient une base de Gröbner minimale pour I :

$$f'_3 = x^2, \quad f'_4 = xy, \quad f'_5 = y^2 - (1/2)x.$$

Il est facile de vérifier que pour tout scalaire a de $\mathbb{K}$, les polynômes

$$\hat{f_3} = x^2 + axy, \quad f'_4 = xy, \quad f'_5 = y^2 - (1/2)x$$

forment aussi une base de Gröbner minimale pour I.

Comme vient de le montrer cet exemple, une base de Gröbner minimal pour un idéal n'est pas unique. On ne peut peut donc pas encore décider le problème de l'égalité de deux idéaux.

Définition 4.2. Une *base de Gröbner réduite* d'un idéal I est une base de Gröbner G de I telle que pour tout polynôme p dans G :
- $LC(p) = 1$;
- aucun monôme de p n'appartient à $\langle LT(G - \{p\})\rangle$.

On construit une base de Gröbner réduite d'un idéal I à partir d'une base de Gröbner minimale de I. À chaque générateur de cette base de Gröbner minimal, on enlève les termes qui sont divisibles par le terme dominant d'un autre générateur. La base modifiée reste une base de Gröbner puisque la modification n'influe pas sur l'égalité $\langle LT(G)\rangle = \langle LT(I)\rangle$.

Exemple 4.4. Revenons à l'exemple 4.3. Parmi les bases de Gröbner minimales

$$\{x^2 + axy, xy, y^2 - (1/2)x),$$

pour a dans $\mathbb{K}$, seule celle avec $a = 0$ est réduite.

Proposition 4.1. *Soit $I \neq \{0\}$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$. Alors, pour un ordre monomial donné, I possède une unique base de Gröbner réduite.*

On retrouvera cette proposition avec sa démonstration dans [Cox 1997].

Grâce à sa propriété d'unicité, cette notion de base de Gröbner réduite rend décidable le problème de l'égalité de deux idéaux. Il suffit en effet de comparer leur base de Gröbner réduite.

4.2.2 Présentations convergentes réduites

Définition 4.3. On dit qu'un système de réécriture convergent $(\Sigma, \mathcal{R})$ est *réduit*, si tout générateur α de Σ est réduit et si pour toute règle $x \xrightarrow{\rho} y$, la source x est réductible uniquement par ρ et la cible y est réduite.

On peut alors identifier toute règle à sa source. De plus, toutes les paires critiques sont alors des chevauchements et sont déterminées par leur source. On peut donc aussi les identifier à leurs sources.

Au-delà des commodités syntaxiques, cette notion de présentation réduite présente l'avantage de son existence, puisque pour toute présentation convergente, il en existe un réduite, sans symbole ni règle supplémentaire. Calculer une base de Gröbner réduite revient à supprimer pour chaque paire critique sous la forme d'une inclusion $(u\rho v, \sigma)$ la règle σ.

On se pose à présent la question du lien entre la notion de base de Gröbner réduite et de présentation convergente réduite. Soit $G = \{f_1, \ldots, f_t\}$ une base de Gröbner d'un idéal I et $(\Sigma, \mathcal{R})$ le système de réécriture associé. Comme G est une base de Gröbner, la présentation est convergente. Supposons G réduite et montrons que la présentation l'est aussi.

Soit f un polynôme de G. La règle f a pour source $LT(f)$. Supposons par l'absurde qu'il existe un générateur g dans G tel que $LT(f)$ soit réductible par la règle g. Alors par définition $LT(f)$ est divisible par $LT(g)$, d'où $LT(f)$ appartient à $\langle LT(G - \{f\})\rangle$, ce qui contredit l'hypothèse de minimalité de G. Donc pour toute règle f de $\mathcal{R}$, la source est réductible uniquement par f. Par définition, $(\Sigma, \mathcal{R})$ est réduite.

À présent, si nous supposons le système de réécriture $(\Sigma, \mathcal{R})$ réduit, on peut aisément démontrer que G est alors minimale. En fait, une base de Gröbner est minimale (et non réduite), si, et seulement si, le système de réécriture associé est réduit. En effet une présentation réduite n'est pas unique.

5 En guise de conclusion

On a étudié les présentations convergentes finies et constaté qu'elles rendaient le problème du mot décidable grâce à l'algorithme de la forme normale. On peut donc se demander s'il existe une présentation convergente finie pour chaque monoïde de type finie. La réponse à cette question a été donnée par le mathématicien Squier en 1987 à travers le théorème suivant démontré dans [Squier 1987].

Théorème 5.1. *Il existe des monoïdes de type fini et décidables (i.e., qui ont un problème du mot décidable) qui ne possèdent pas de présentations convergentes finies.*

Par conséquent, dans de tels monoïde, on ne peut pas décider le problème du mot avec l'algorithme de la forme normale.

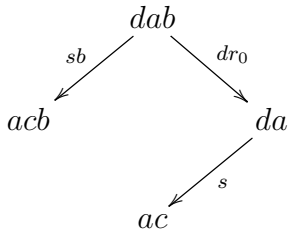
Pourtant, tout idéal de $\mathbb{K}[x_1, \ldots, x_n]$ possède une base de Gröbner. En effet, l'algorithme de Buchberger termine toujours avec succès. Mais, en ce qui concerne les systèmes de réécriture, si M est un monoïde, il ne possède pas toujours de présentation convergente finie. En effet l'algorithme de Knuth-Bendix ne termine pas toujours sur une présentation convergente finie.

Exemple 5.1. On considère le système de réécriture $(\Sigma, \mathcal{R})$, où

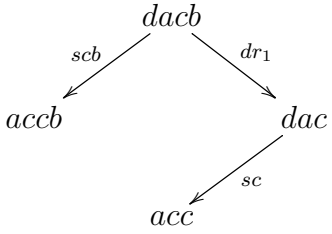
$$\Sigma = \{a, b, c, d\} \text{ et } \mathcal{R} = \{ab \xrightarrow{r_0} a, da \xrightarrow{s} ac\}$$

Le système est noethérien puisque le nombre d'occurrences de b et de d diminue à chaque

réduction. Il existe une paire critique :



Donc, on ajoute la règle $acb \xrightarrow{r_1} ac$. Le système est toujours noethérien, mais on a une nouvelle paire critique :



Donc, on ajoute la règle $accb \xrightarrow{r_2} acc$, ce qui créé une nouvelle paire critique, et ainsi de suite. En continuant ainsi, on obtient en fait une présentation convergente *infinie* :

$$\mathcal{R} = \{ac^n b \xrightarrow{r_n} ac^n \mid n \in \mathbb{N}\} \cup \{da \xrightarrow{s} ac\}$$

De plus, l'algorithme de Knuth-Bendix ne garantit pas la conservation de la propriété de terminaison du système et peut donc échouer.

Pourquoi l'algorithme de Buchberger termine-t-il toujours tandis que son homologue dans les système de réécriture, l'algorithme de Knuth-Bendix, ne réussit pas toujours ?

Si, pour une présentation $(\Sigma, \mathcal{R})$ d'un monoïde M, l'algorithme de Knuth-Bendix échoue, cela ne signifie pas qu'il n'existe pas de présentation convergente finie pour le monoïde M. En effet, Diekert a prouvé, dans [Diekert 1986], le théorème suivant :

Théorème 5.2. *Tout monoïde commutatif de type fini possède une présentation convergente finie.*

Démonstration. Nous allons démontrer ce théorème en utilisant les liens que nous connaissons avec l'anneau de polynômes à plusieurs indéterminées. Soit $(\Sigma, \mathcal{R})$ une présentation d'un monoïde commutatif fini.

$$\Sigma = \{x_1, \ldots, x_n\} \text{ et } \mathcal{R} = \{f_k = g_k \mid k \in \{1, \ldots, t\},\ f_k, g_k \in \Sigma^*\}.$$

Comme M est commutatif, on a, pour tous i et j de $\{1, \ldots, n\}$, $x_i x_j = x_j x_i$. On remarque alors que $\Sigma^* = \mathcal{M}(x_1, \ldots, x_n)$. Considérons à présent l'idéal $I = \langle f_k - g_k \mid k \in \{1, \ldots, t\}\rangle$. Pour tout k dans $\{1, \ldots, t\}$, $f_k - g_k$ est bien un polynôme de $\mathbb{K}[x_1, \ldots, x_n]$, donc les $f_k - g_k$ forment bien une base d'un idéal. On peut donc appliquer l'algorithme de Buchberger afin de trouver une base de Gröbner G de I. On peut montrer que les polynômes de la

base de Gröbner trouvée possèdent tous deux termes et que leurs coefficients sont égaux à 1. On obtient une nouvelle présentation $(\Sigma, \mathcal{R}')$ où les règles de $\mathcal{R}'$ s'obtiennent à partir des générateurs de G. La présentation est noethérienne puisqu'il suffit de prendre l'ordre monomial utilisé dans l'algorithme de Buchberger, comme ordre de terminaison. De plus, d'après le théorème 4.1, la présentation est confluente. Donc $(\Sigma, \mathcal{R}')$ est une présentation convergente du monoïde M. □

Ainsi nous avons redémontré un théorème de réécriture grâce aux bases de Gröbner. Cette preuve repose notamment sur le fait que si G est une base de Gröbner d'un idéal I, alors la relation de réduction $\xrightarrow{G}$ est toujours noethérienne. En effet, dans $\mathbb{K}[x_1, \ldots, x_n]$, on peut poser un ordre $<$ défini par $f < g$ si $multideg(f) <_0 multideg(g)$, où $<_0$ est l'ordre monomial préalablement fixé. Donc, par définition, pour tout polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$,

$$f - LT(f) < LT(f).$$

Or on montre facilement que $<$ est un bon ordre. De plus, si G est une base d'un idéal I, pour toute réduction $x \xrightarrow{G} y$, on a $y < x$. Donc la relation de réduction $\xrightarrow{G}$ termine, i.e., la présentation $(\Sigma, \mathcal{R})$ associée est noethérienne.

Ainsi, l'analogie des bases de Gröbner avec les présentation convergentes finies se situe dans le cas particulier des monoïdes commutatifs.

Références

[Cox 1997] D. Cox, J.Little et D.O'Shea, *Ideals, Varieties, and Algorithms*, 2nd edition, Springer-Verlag, New York, (1997).

[Buchberger 1965] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal)*, PhD Thesis, Mathematical Institute, University of Innsbruck, Austria, (1965). (English translation to appear in Journal of Symbolic Computation, 2004)

[Knuth-Bendix 1970] D. Knuth et P. Bendix, Simple word problems in universal algebras. In . Leech, edito, *Computational Problems in Abstract Algebra*, pages 263-297. Pergamon Press, New York, (1970).

[Lafont 1991] Yves Lafont, Prouté, *Alain Church-Rosser property and homology of monoids*, Math. Structures Comput. Sci. 1 (1991), no. 3, 297–326.

[Baader-Nipkow 1998] Franz Baader, Tobias Nipkow, *Term rewriting and all that*, Cambridge University Press, Cambridge, (1998). xii+301 pp.

[Squier 1987] Craig C. Squier, *Word problems and a homological finiteness condition for monoids*, Journal of Pure and Applied Algebra, 49, 201–217, (1987).

[Diekert 1986] Volker Diekert, *Commutative monoids have complete presentations by free (non-commutative) monoids*, Theoretical Computer Science, 46, pages 319-327, North-Holland, (1986).