Cryptanalyse

Cours 9 - Cryptanalyse Algébrique: Aspects Algorithmiques

Maxime Bombar

Mercredi 23 Octobre

Rappels d'hier : Systèmes Polynomiaux

Modélisation comme Système polynomial

- **Principe :** On détermine un système de m équations polynomiales

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases} \qquad f_i \in K[x_1, \dots, x_n]$$

- **Propriété :** Les solutions

$$\boxed{\mathcal{V}(f_1, \dots, f_m) = \left\{(x_1, \dots, x_n) \in \overline{K}^n \mid f_i(x_1, \dots, x_n) = 0 \quad \forall i \in \{1, \dots, m\}\right\}}$$

donnent de l'information sur le secret.

- Ici K est un corps. En pratique, $K = \mathbb{F}_2$ pour la cryptanalyse.

Idéal et Variété Algébrique

À un système polynomial $\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$ on associe l'**idéal** de $K[x_1, \ldots, x_n]$ défini par

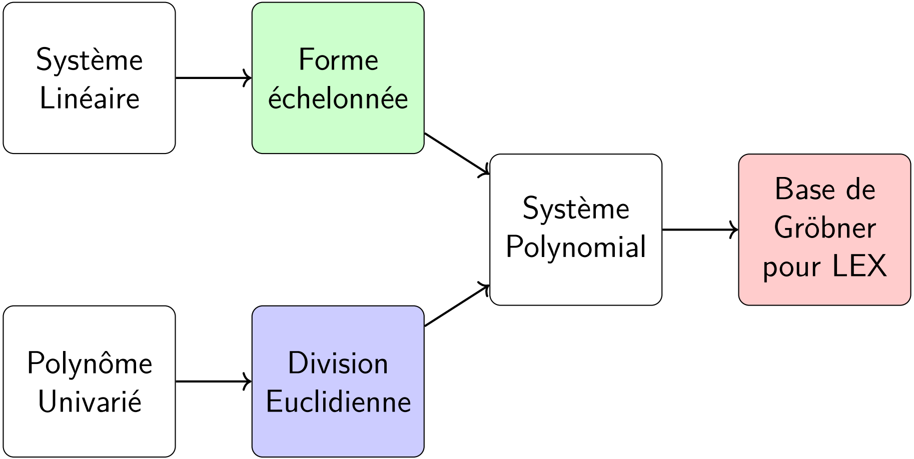
$$\mathcal{I} \stackrel{\text{def}}{=} \langle f_1, \ldots, f_m \rangle \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^{m} g_i f_i \mid g_i \in \mathbb{F}_2[x_1, \ldots, x_n] \right\}.$$

$$\mathcal{V}(\mathcal{I}) = \left\{ (x_1, \ldots, x_n) \in \overline{K}^n \mid f_i(x_1, \ldots, x_n) = 0 \quad \forall i \in \mathcal{I} \right\}$$

est appelé **variété algébrique** associée à $\mathcal{I}$.

Attention : Typo hier.

Objectif du Jour



Sur le nombre de solutions

- Soit $\begin{cases} f_1(x) = 0 \\ \vdots \\ f_m(x) = 0 \end{cases}$ un système de polynômes **univariés** de degrés d_i.

  Le nombre de solutions peut-il être infini ? Combien y en a-t-il **au maximum** ?
- Si les coefficients sont dans un corps fini, est-ce facile de trouver les solutions ?

Sur le nombre de solutions

- Soit $\begin{cases} f_1(x) = 0 \\ \quad \vdots \\ f_m(x) = 0 \end{cases}$ un système de polynômes **univariés** de degrés d_i.

  Le nombre de solutions peut-il être infini ? Combien y en a-t-il **au maximum** ?
- Si les coefficients sont dans un corps fini, est-ce facile de trouver les solutions ?

- Un polynôme à deux variables $f(x, y)$ a-t-il un nombre fini de racines (dans la cloture algébrique) ? (Pensez à $K = \mathbb{R}$ ou $\mathbb{C}$ et à la géométrie).

Sur le nombre de solutions

- Soit $\begin{cases} f_1(x) = 0 \\ \vdots \\ f_m(x) = 0 \end{cases}$ un système de polynômes **univariés** de degrés d_i.

  Le nombre de solutions peut-il être infini ? Combien y en a-t-il **au maximum** ?
- Si les coefficients sont dans un corps fini, est-ce facile de trouver les solutions ?

- Un polynôme à deux variables $f(x, y)$ a-t-il un nombre fini de racines (dans la cloture algébrique) ? (Pensez à $K = \mathbb{R}$ ou $\mathbb{C}$ et à la géométrie).
- Même pour si $f \in \mathbb{F}_2[x_1, x_2]$, f aura un nombre **infini** de racines dans $\overline{\mathbb{F}_2}^2$.
- Les équations de corps $x_i^2 - x_i = 0$ permettent de se ramener à $\mathbb{F}_2^2$, et donc à un ensemble **fini**.

Bases de Gröbner

Ordre Monomial

Un monomome dans $\mathbb{F}_q[x_1, \ldots, x_n]$ est un élément de la forme $\mu \stackrel{\text{def}}{=} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Ordre Monomial

Un ordre monomial $<$ sur $\mathbb{F}_q[x_1, \ldots, x_n]$ est une relation d'ordre sur l'ensemble des monômes tel que

- $<$ est un **ordre total** (on peut comparer tous les éléments)
- Pour tout triplets de monomes μ_1, μ_2, μ_3 alors

$$\mu_1 < \mu_2 \Rightarrow \mu_1 \cdot \mu_3 < \mu_2 \cdot \mu_3$$

- $<$ est un **bon ordre** : Toute partie non vide admet un **plus petit élément**.

Ordre Lexicographique

Ordre Lexicographique $x_1 > \cdots > x_n$

$x_1^{\alpha_1} \cdots x_n^{\alpha_n} <_{lex} x_1^{\beta_1} \cdots x_n^{\beta_n} \iff (\alpha_1, \ldots, \alpha_n) < (\beta_1, \ldots, \beta_n)$ *i.e.*,

$$\exists j \geqslant 1 \; (\alpha_i = \beta_i \, \forall i < j) \quad \text{et} \;\; \alpha_j < \beta_j.$$

i.e., la première coordonnée non nulle de $\boldsymbol{\alpha} - \boldsymbol{\beta}$ est **négative**.

Remarque : C'est l'ordre à choisir pour résoudre un système polynomial.
La base de Gröbner associée sera échelonnée.

Exemple

Ordre Lexicographique $x_1 > \cdots > x_n$

Dans $K[x_1, x_2, x_3]$, on a

- $x_1^2x_2x_3^{15} <_{lex} x_1^2x_2^2$ car $(2, 1, 15) - (2, 2, 0) = (0, -1, 15)$.
- $x_3^5 <_{lex} x_2^2x_3$ car $(0, 0, 5) - (0, 2, 1) = (0, -2, 4)$.
- $1 < x_3 < x_3^2 < \cdots < x_2 < x_2x_3 < x_2x_3^2 < \cdots < x_2^2 < x_2^2x_3 < \cdots < x_2^3 < \cdots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \cdots$

Base de Gröbner pour l'ordre LEX

Une base de Gröbner pour l'ordre LEX est de la forme

$$\begin{array}{r} g_{1,1}(x_1, x_2, \cdots, x_n) \\ \vdots \\ g_{1,r_1}(x_1, x_2, \cdots, x_n) \\ g_{2,1}(x_2, \cdots, x_n) \\ \vdots \\ g_{2,r_2}(x_2, \cdots, x_n) \\ \vdots \\ g_n(x_n) \end{array}$$

Pour résoudre un système polynomial, on calcule une base de Gröbner pour l'ordre LEX et on résoud par substitution !

Exemple : Base de Gröbner en Sage

```
sage: R.<x1, x2, x3> = PolynomialRing(GF(2), order='lex')
sage: f1 = x1^2 + x2*x3 + 1
....: f2 = x1*x2 + x3 + 1
....: f3 = x2^2 + x1*x3 + 1
sage: I = Ideal([f1, f2, f3])
sage: I.groebner_basis(); I
[x1 + x2*x3^2 + x2*x3 + x2 + x3, # x1, x2 et x3
x2^2 + x2*x3 + x3^3 + 1, # x3 et x2
x2*x3^3 + x2*x3^2 + x3^3 + x3^2, # x3 et x2
x3^4 + x3^3] # Que des x3
sage: J = Ideal([f1, f2, f3, x1^2-x1, x2^2-x2, x3^2-x3])
sage: J.groebner_basis()
[x1 + x2 + x3, x2^2 + x2, x2*x3 + x2 + x3 + 1, x3^2 + x3]
```

Exemple de résolution d'un système polynomial

$$\left\{\begin{array}{c} x_1^2 + x_2x_3 + 1 = 0 \\ x_1x_2 + x_3 + 1 = 0 \\ x_2^2 + x_1x_3 + 1 = 0 \end{array}\right. \xrightarrow[\text{Ordre LEX}]{\text{Base de Gröbner}} \left\{\begin{array}{c} x_1 + x_2x_3^2 + x_2x_3 + x_2 + x_3 = 0 \\ x_2^2 + x_2x_3 + x_3^3 + 1 = 0 \\ x_2x_3^3 + x_2x_3^2 + x_3^3 + x_3^2 = 0 \\ x_3^4 + x_3^3 = 0 \end{array}\right.$$

Systèmes équivalents

Exemple de résolution d'un système polynomial

$$\begin{cases} x_1^2 + x_2x_3 + 1 = 0 \\ x_1x_2 + x_3 + 1 = 0 \\ x_2^2 + x_1x_3 + 1 = 0 \end{cases} \xrightarrow[\text{avec } x_i^2 - x_i = 0]{\text{Base de Gröbner}} \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_2^2 + x_2 = 0 \\ x_2x_3 + x_2 + x_3 + 1 = 0 \\ x_3^2 + x_3 = 0 \end{cases}$$

Systèmes équivalents

Exemple de résolution d'un système polynomial

$$\left\{\begin{array}{l} x_1^2 + x_2x_3 + 1 = 0 \\ x_1x_2 + x_3 + 1 = 0 \\ x_2^2 + x_1x_3 + 1 = 0 \end{array}\right. \xrightarrow[\text{avec } x_i^2 - x_i = 0]{\text{Base de Gröbner}} \left\{\begin{array}{c} x_1 + x_2 + x_3 = 0 \\ x_2^2 + x_2 = 0 \\ x_2x_3 + x_2 + x_3 + 1 = 0 \\ x_3^2 + x_3 = 0 \end{array}\right.$$

Solutions (x_1, x_2, x_3) :

$$\Big\{(0,1,1),(1,0,1),(1,1,0)\Big\}$$

Graded Reverse Degree Lexicographic (GREVLEX ou DRL)

Ordre Degré-Lexicographique Inverse $x_1 > \cdots > x_n$

$x_1^{\alpha_1} \cdots x_n^{\alpha_n} <_{drl} x_1^{\beta_1} \cdots x_n^{\beta_n}$ si

- $\sum_i \alpha_i < \sum_i \beta_i$ OU
- $\sum_i \alpha_i = \sum_i \beta_i$ et la première coordonnée non nulle de $\boldsymbol{\alpha} - \boldsymbol{\beta}$ est **positive**.

Ordre moins intuitif, mais en pratique les algorithmes sont **plus rapides**.

Exemple

Dans $K[x_1, x_2, x_3]$, on a

- $x_1^2 x_2 x_3^{15} >_{drl} x_1^2 x_2^2$ car $2 + 1 + 15 = 18 > 4 = 2 + 2$
- $x_3^5 <_{lex} x_2^2 x_3$ car $(0, 0, 5) - (0, 2, 1) = (0, -2, 4)$.
- $1 < \underbrace{x_3 < x_2 < x_1}_{\text{Degré 1}} < \underbrace{x_3^2 < x_3 x_2 < x_2^2 < x_1 x_3 < x_1 x_2 < x_1^2}_{\text{Degré 2}} < x_3^3 < x_2 x_3^2 < x_2^2 x_3 < x_2^3 < \cdots$

Monôme de tête

À partir de maintenant, on se fixe un ordre monomial $<$ sur $K[x_1, \ldots, x_n]$.

Soit $f \stackrel{\text{def}}{=} \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} c_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}} \in K[x_1, \ldots, x_n]$.

- Le **monôme de tête** (*leading monomial*) de f est

$$LM_<(f) \stackrel{\text{def}}{=} \max_< \{\mathbf{x}^{\boldsymbol{\alpha}}\}.$$

- Le **coefficient de tête** (*leading coefficient*) de f est

$$LC_<(f) \stackrel{\text{def}}{=} c_{LM_<(f)}.$$

- Le **terme de tête** (*leading term*) de f est

$$LT_<(f) \stackrel{\text{def}}{=} LC_<(f) \cdot LM_<(f).$$

Exemple

On se place sur $\mathbb{F}_5[x, y, z]$:

$$\text{Soit } f \stackrel{\text{def}}{=} 2xy^2 - xz^2 + xyz + 2x^2 - yz^2.$$

- **Ordre Lex** avec $x > y > z$: $f = \underbrace{2}_{LC} \underbrace{x^2}_{LM} + 2xy^2 + xyz - xz^2 - yz^2$
- **Ordre Drl** avec $x > y > z$: $f = \underbrace{2}_{LC} \underbrace{xy^2}_{LM} + xyz - xz^2 - yz^2 + 2x^2$

Idéal monomial

Def. Soit $I = \langle f_1, \ldots, f_m \rangle \subset K[x_1, \ldots, x_n]$ un idéal et $<$ un ordre monomial. On lui associe l'idéal **monomial**

$$LM_<(\mathcal{I}) \stackrel{\text{def}}{=} \langle LM_<(f) \mid f \in \mathcal{I} \rangle.$$

On se place dans $\mathbb{F}_5[x, y, z]$ munit de $<_{lex}$ et on considère l'idéal $\mathcal{I} \stackrel{\text{def}}{=} \langle f_1, f_2 \rangle$ où

$$f_1 = x^2 y \qquad f_2 = xy^2 - z.$$

Remarquons que :

$$z^2 = y^3 \cdot f_1 - (xy^2 + z) \cdot f_2 \in \mathcal{I}$$

donc

$$z^2 \in LM_<(\mathcal{I}) \neq \langle x^2 y, xy^2 \rangle$$

Un critère utile

Lemme : Soit $\mathcal{J} = \langle \mathbf{x}^{\alpha(1)}, \ldots, \mathbf{x}^{\alpha(k)} \rangle$ un idéal **monomial**, et soit $\mathbf{x}^{\beta} \in K[x_1, \ldots, x_n]$ un monôme. Alors

$$\mathbf{x}^{\beta} \in \mathcal{J} \iff \exists \ell,\ \mathbf{x}^{\alpha(\ell)} \text{ divise } \mathbf{x}^{\beta}, \quad i.e., \boldsymbol{\beta} - \boldsymbol{\alpha}(\ell) \geqslant 0.$$

Preuve : Exercice.

Base de Gröbner

Def. Soit $I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{F}_q[x_1, \ldots, x_n]$ un idéal et $<$ un ordre monomial. Une **base de Gröbner** de $\mathcal{I}$, par rapport à $<$, est un sous-ensemble $\mathcal{G} \stackrel{\text{def}}{=} \{g_1, \ldots, g_s\} \subset \mathcal{I}$ tel que

$$LM_<(\mathcal{I}) = \langle LM_<(g_1), \ldots, LM_<(g_s) \rangle$$

On se place dans $\mathbb{F}_5[x, y, z]$ munit de $<_{lex}$ et on considère l'idéal $\mathcal{I} \stackrel{\text{def}}{=} \langle f_1, f_2 \rangle$ où

$$f_1 = x^2 y \qquad f_2 = xy^2 - z.$$

On verra que :

$$g_1 \stackrel{\text{def}}{=} x^2 y \quad g_2 \stackrel{\text{def}}{=} xy^2 - z \quad g_3 \stackrel{\text{def}}{=} xz \quad g_4 \stackrel{\text{def}}{=} z^2$$

est une base de Gröbner de $\mathcal{I}$.

Base de Gröbner : Existence et Unicité*

Soit $\mathcal{I} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ un idéal **non nul** et soit $<$ un ordre monomial.

Existence (Algorithme de Buchberger)

$\mathcal{I}$ admet une base de Gröbner.

Base de Gröbner réduite et Unicité

Une base de Gröbner $\mathcal{G}$ de $\mathcal{I}$ est **réduite** si pour tout $g \in \mathcal{G}$:

$$LC(g) = 1 \quad \text{et} \quad LM(g) \notin LT(\mathcal{G} \setminus \{g\}).$$

$\mathcal{I}$ admet une **unique** base de Gröbner réduite pour l'ordre monomial $<$.

Les bases de Gröbner dépendent **fortement** de l'ordre monomial choisi !

Algorithmes

Problème *Multivariate Quadratic* (MQ)

Donnée : Un système $f_1 = 0, \ldots, f_m = 0$ avec $f_i \in \mathbb{F}_q[x_1, \ldots, x_n]$ de degré 2.

Question : Le système admet-il une solution ?

MQ est NP-complet.

Un problème vraiment difficile

Problème *Ideal Membership* (IM)

Donnée : $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ idéal de $\mathcal{R} \stackrel{\text{def}}{=} K[x_1, \ldots, x_n]$ et $f \in \mathcal{R}$.

Question : $f \in \mathcal{I}$?

Calculer une base de Gröbner de $\mathcal{I}$ permet de résoudre le problème.

Mayr et Meyer, 1986

IM est EXP-SPACE complet.

Cas des fonctions booléennes

Gröbner basis in Boolean rings is not polynomial-space

Mark van Hoeij*
Florida State University
Tallahassee, Fl 32306-3027, USA

July 5, 2021

https://arxiv.org/pdf/1502.07220

Nombre fini de solutions

Lazard (1983) et Giusti (1984)

En général, calculer une base de Gröbner est doublement exponentiel. Lorsque le nombre de solutions est fini, il existe des algorithmes simplement exponentiels.

Division Euclidienne Généralisée

On se fixe un ordre monomial $<$ et $\mathcal{F} \stackrel{\text{def}}{=} \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_m]$ un ensemble fini.

Algorithme 1 : Réduction modulo $\mathcal{F}$

si $f = 0$ **alors**
  retourner 0
$r \leftarrow f$
tant que **Il existe** $h \in \mathcal{F}$ **tel que** $LT(h)$ **divise** $LT(r)$ **faire**
  $r \leftarrow r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(h)} h$
retourner r

On note $f \longrightarrow_{\mathcal{F}} r$

Exemple dans $\mathbb{F}_2[x, y]$

- On prend l'ordre lexicographique $x > y$
- $f = xy^2 + x$ et $\mathcal{F} \stackrel{\text{def}}{=} \{y^2 + 1, xy + 1\}$.

Non unicité de la réduction en général

- Si on prend $h = y^2 + 1$: $LT(h) = y^2$ divise $LT(f) = xy^2$ et

$$f - \frac{LT(f)}{LT(h)} h = xy^2 + x - \frac{xy^2}{y^2}\left(y^2 + 1\right) = 0$$

- Si on prend $h = xy + 1$: $LT(h) = xy$ divise $LT(f) = xy^2$ et

$$f - \frac{LT(f)}{LT(h)} h = xy^2 + x - \frac{xy^2}{xy}(xy + 1) = x + y$$

Forme Normale dans $K[x_1, \ldots, x_n]/\mathcal{I}$

Si $\mathcal{G} \stackrel{\text{def}}{=} \{g_1, \ldots, g_s\}$ est une base de Gröbner de l'idéal $\mathcal{I} \stackrel{\text{def}}{=} \langle f_1, \ldots, f_m \rangle$, alors pour tout élément $f \in K[x_1, \ldots, x_n]$ il existe $h_1, \ldots, h_s$ et $\rho \in K[x_1, \ldots, x_n]$ tels que

$$f = \sum_{i=1}^{s} g_i h_i + \rho,$$

et de telle sorte qu'aucun monôme de ρ ne soit divisible par les $LT(g_i)$.

ρ est unique et ne dépend que de $\mathcal{I}$ et de l'ordre monomial $<$ choisi (et pas du choix de $\mathcal{G}$). On l'appelle **Forme Normale** de f par rapport à l'idéal $\mathcal{I}$ et à $<$.

La forme normale s'obtient par réduction modulo $\mathcal{G}$. En particulier, celle-ci est bien définie pour une base de Gröbner.

Première Syzygy

S-Polynôme

Soit $f, g \in K[x_1, \ldots, x_n]$. On définit

$$S(f,g) \stackrel{\text{def}}{=} \frac{PPCM(LM(f), LM(g))}{LM(f)} \cdot f - \frac{PPCM(LM(f), LM(g))}{LM(g)} \cdot g$$

On se place dans $\mathbb{F}_5[x,y]$ et on note $f_1 \stackrel{\text{def}}{=} xy^2 + 1$ et $f_2 = xy^2 - 2$. Alors :

$$S(f1, f2) = y \cdot \left(x^2y + 1\right) - x \cdot \left(xy^2 - 2\right) = y + 2x.$$

Le Critère de Buchberger

Soit $\mathcal{I} \subset K[x_1, \ldots, x_n]$ un idéal, et $<$ un ordre monomial.

Soit $\mathcal{G} \stackrel{\text{def}}{=} \{g_1, \ldots, g_s\} \subset \mathcal{I}$. Alors $\mathcal{G}$ est une base de Gröbner de $\mathcal{I}$ si et seulement si pour tous $1 \leqslant i < j \leqslant s$,

$$S(g_i, g_j) \longrightarrow_{\mathcal{G}} 0$$

Algorithme de Buchberger

Données : Un ensemble fini $\mathcal{F} = \{f_1, f_2, \ldots, f_m\} \subset K[x_1, \ldots, x_m]$
Résultat : Une base de Gröbner $\mathcal{G}$ de $\langle \mathcal{F} \rangle$

$\mathcal{G} \leftarrow \mathcal{F}$ et $\mathcal{P} \leftarrow \{(f_i, f_j) \mid f_i, f_j \in \mathcal{F}, i \neq j\}$;
tant que $\mathcal{P} \neq \emptyset$ **faire**
    Choisir une paire $(f, g) \in \mathcal{P}$;
    Calculer $S(f, g)$ et réduire modulo $\mathcal{G}$: $S(f, g) \to_{\mathcal{G}} r$;
    si $r \neq 0$ **alors**
        $\mathcal{G} \leftarrow \mathcal{G} \cup \{r\}$;
        $\mathcal{P} \leftarrow \mathcal{P} \cup \{(r, h) \mid h \in \mathcal{G}, h \neq r\}$;
    fin
fin
retourner $\mathcal{G}$;

Exemple

On considère $\mathbb{F}_5[x, y, z]$ avec $x > y > z$, et $\mathcal{I} \stackrel{\text{def}}{=} \langle x^2y, xy^2 - z \rangle$. On note $\mathcal{G}$ une base de Gröbner de $\mathcal{I}$ pour l'ordre lexicographique.

Montrer que $\mathcal{G} = \{x^2y, xy^2 - z, xz, z^2\}$.

Critère de finitude

On considère un système polynomial.

$$(\mathcal{S}) \begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \qquad f_i \in K[x_1, \ldots, x_n]$$

et l'idéal $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ associé, muni d'une base de Gröbner $\mathcal{G}$ pour un certain ordre monomial $<$ fixé.

$(\mathcal{S})$ admet un nombre fini de solutions, si et seulement si pour toute variable x_i il existe un $g_i \in \mathcal{G}$ tel que $LM(g_i)$ est une puissance de x_i.

Vrai par exemple avec les équations de corps $x_i^q - x_i$.

Théorème d'Élimination

Soit $\mathcal{I}$ un idéal de $K[x_1, \ldots, x_n]$ et $t \in \{1, \ldots, n\}$. On note $\mathcal{I}^{(t)} \stackrel{\text{def}}{=} I \cap K[x_t, \ldots, x_n]$.

Soit $\mathcal{G}$ une base de Gröbner de $\mathcal{I}$ pour l'**ordre lexicographique**. Alors,

$$\mathcal{G}^{(t)} \stackrel{\text{def}}{=} \mathcal{G} \cap K[x_t, \ldots, x_n]$$

est une base de Gröbner pour $\mathcal{I}^{(t)}$.

En d'autre termes, le système associé à la base de Gröbner est **échelonné** !

Changement d'ordre monomial

Soit $\mathcal{I}$ un idéal de $K[x_1, \ldots, x_n]$ tel que $\mathcal{V}(\mathcal{I})$ soit fini.

Faugère, Giani, Lazard, Mora (FGLM), 1994

Il existe un algorithme qui étant donnée une base de Gröbner $\mathcal{G}$ de $\mathcal{I}$ pour un ordre monomial $<_1$ calcule une base de Gröbner $\mathcal{G}'$ relativement à un autre ordre monomial $<_2$ en temps

$$O(n \cdot \#\mathcal{V}(\mathcal{I})).$$

Pour résoudre un système polynomial en pratique, on calcule d'abord une base de Gröbner pour l'ordre DRL (plus rapide), et on la transforme en une base de Gröbner pour l'ordre LEX.

Rafinements de l'Algorithme de Buchberger

Inconvénients de Buchberger

L'algorithme de Buchberger réalise beaucoup d'opérations qui n'amènent pas plus proche de la base de Gröbner finale.

Algorithme F_4 (Faugère, 1999)

Améliore le calcul des bases de Gröbner à l'aide d'algèbre linéaire sur des **grosses** matrices appelées **Matrices de Macaulay**. C'est l'algorithme le plus utilisé pour calculer des bases de Gröbner (implanté dans Magma).

Algorithme F_5 (Faugère, 2002)

Améliore F_4 à l'aide de critères pour limiter les calculs inutiles.

Complexité

Déterminer la complexité du calcul de bases de Gröbner n'est pas chose aisée.

Sous des conditions relativement générales sur $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ idéal de $K[x_1, \ldots, x_n]$, alors on peut calculer une base de Gröbner pour $\mathcal{F}$ qui ne contient que des polynômes de degré D en temps

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right).$$

(**exponentiel** en D).

Les bases de Gröbner pour l'ordre DRL ont en général un degré plus faible.

Attention à la mémoire

Table 3. Memory ($\log_2$(#bytes)) needed to store the Macaulay matrix $M(Q)$ from Step 1 to be used in BW or Strassen's algorithm.

Scheme	BW Standard	BW Optimized	Strassen
GeMSS128	38.665	34.553	48.935
BlueGeMSS128	34.332	30.258	41.263
RedGeMSS128	27.645	23.729	29.873
GeMSS192	39.930	35.213	50.166
BlueGeMSS192	35.586	30.917	42.478
RedGeMSS192	28.897	24.410	31.073
GeMSS256	40.836	35.686	51.049
BlueGeMSS256	36.488	31.389	43.353
RedGeMSS256	29.800	24.905	31.940